Hewlett Packard
Enterprise

HPE Network Node Manager i Software

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

HPE Network Node Manager i Software–HPE Network Automation Integration Guide

Document Release Date: May 2017
Software Release Date: November 2016

Legal Notices

Warranty

Restricted Rights Legend

Oracle Technology — Notice of Restricted Rights

Copyright Notice

Trademark Notices

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.hpe.com/group/softwaresupport/search-result?keyword=.

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

Support

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

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

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

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

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

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

Contents

Integrate NNMi with NA

HPE Network Node Manager i Software (NNMi) provides smart network fault and availability monitoring using common network protocols such as SNMP and ICMP to help you maintain a healthy network across your organization. NNMi can discover network nodes (such as switches and routers) on an automatic and continuing basis, providing an up-to-date representation of the network topology (Layers 2 and 3).

NNMi uses an accurate picture of the network to pinpoint network problems by using topology-based root cause analysis (RCA). Together, RCA, advanced correlation features, and a *management by exception* incident management model provide a dynamic fault management solution for an ever changing network environment.

NNMi also monitors device health indicators such as CPU and memory utilization along with interface performance metrics such as utilization and interface errors. Real-time performance indicators can be monitored at intervals as fine as one second through live performance graphs.

Network Automation software (NA) is an enterprise-class network device change and configuration management tool. It eliminates human error in device configuration changes while also maintaining compliance standards through a policy-based change management model. NA maintains a complete audit trail of all device changes, including a key stroke log of command line changes made through the NA telnet proxy.

NA supports thousands of network device model and operating system combinations from the major vendors. NA minimizes MTTR using configuration archiving and deployment and tracks the following information:

- Changes made to network devices.
- Initiator of each change.
- Current device configurations.
- Device configuration compliance with organizational standards.

> **NOTE:** The policy compliance related features require the NA Ultimate license.

For information about purchasing NNMi or NA, contact your HPE sales representative.

This chapter describes the HPE NNMi–HPE NA integration and supported integration deployment architectures. It includes the following topics:

- "Integration Overview" below
- "Integration Architecture" on page 10

Integration Overview

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

The integration provides the following functionality:

- Synchronizes the NNMi and NA topologies for lower ownership cost and better management coverage of provisioned devices.
- Automatically runs NA device diagnostics when certain NNMi incidents occur.

- Shows NA node configuration and compliance information in the NNMi Analysis Pane for synchronized nodes with active configuration policies.

  NOTE: Compliance information requires the NA Ultimate license.

- Shows NA interface configuration information in the NNMi Analysis Pane for interfaces on synchronized nodes.
- Prevents unnecessary alarming in NNMi while devices are out of service as NA applies device configuration updates.
- Updates the NNMi configuration with information for accessing managed devices.

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

The HPE NNMi–HPE NA integration adds menu items to the NNMi console for opening connections to the NA console in the context of the NNMi view and for viewing configuration information on devices managed by 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.

  NOTE: Compliance information requires the NA Ultimate license.

- Run NA diagnostics and command scripts from NNMi nodes.
- Detect connections with mismatched speed or duplex configurations

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

NOTE: The HPE NNMi–HPE 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.

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

Value

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

- Alarm integration—The HPE NNMi–HPE NA integration communicates NA configuration change information to the NNMi console, enabling you to quickly identify whether configuration changes might have caused network problems. From within the NNMi console, you can quickly access 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.
- Content integration—The HPE NNMi–HPE NA integration adds tabs in the analysis pane of the NNMi console for synchronized nodes. These tabs display the current device or interface configuration, device configuration history, and the current status of compliance with NA configuration policies. From within the NNMi console, you can quickly access the NA console in the context of the current view to continue researching a specific issue.

  NOTE: Compliance information requires the NA Ultimate license.
- 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:

- NNMi
- NA

The products can be licensed at the same or different levels. License levels do impact the features available in each product. For more information, contact your HPE sales representative.

TIP: For the list of supported versions, see the NNMi Support Matrix or the *NA Support Matrix*.

Integration Configuration Details

For information about supported integration architectures, see "Integration Architecture" on the next page.

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

TIP: It is recommended that NA and NNMi each run on a dedicated server.

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

The HPE NNMi–HPE NA integration is not operating system dependent.

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 HPE NNMi–HPE NA integration.

Integration Architecture

The HPE NNMi–HPE NA integration can be deployed in any of the following integration architectures:

- **One NNMi Management Server to One NA Core**

  One standalone NNMi management server connected to one NA core that is either standalone or participating in a Horizontal Scalability environment. See "Figure 1 Example Deployment Architectures: One NNMi Management Server to One NA Core".

- **NNMi Global Network Management to Multiple Standalone NA Cores**

  Each NNMi regional management server in a Global Network Management environment integrated with a different standalone NA core. See "Figure 2 Example Deployment Architecture: NNMi Global Network Management to Multiple Standalone NA Cores".

- **NNMi Global Network Management to a Standalone NA Core or NA Horizontal Scalability**

  NNMi in a Global Network Management environment integrated with a standalone NA core or with one or more NA cores running in a Horizontal Scalability environment. Any or all of the NNMi regional servers and, optionally, the NNMi global server can connect to any of the NA cores. For example:

  - All of the NNMi management servers might connect to one NA core. In this case, all NA console pages launched from NNMi run on that NA core. Consider reserving this NA core for user interaction so that it is fully devoted to responding to user requests. For more information, see the *NA Horizontal Scalability Guide*.

  - Each NNMi management server might connect to a different NA core.

  See "Figure 3 Example Deployment Architecture: NNMi Global Network Management to NA Horizontal Scalability".

  For this architecture, note the following:

  - NA receives inventory from each integrated NNMi management server. For complete inventory synchronization, integrate each NNMi regional manager with an NA core. If the NNMi global manager manages nodes locally, also integrate the NNMi global manager with an NA core.

  - For nodes that the NNMi global manager does not manage locally, integrating the NNMi global manager with an NA core provides NA data in the analysis pane and the ability to launch NA console pages from the NNMi console.

  - Inventory synchronization is from NNMi to NA only. If NA manages devices that do not appear in the inventory of any NNMi management servers, consider manually adding those devices to the NNMi inventory.

  - Because each NNMi management server connects to only one NA core (as specified on the **HPE NNMi–HPE NA Integration Configuration** form), each NNMi management server initiates communication to only the one integrated NA core. Examples of communication from NNMi to NA include:

  - Initiating an NA diagnostic in response to an NNMi incident
  - Opening NA console pages

- Because all NA cores connect to a single NA database, each NA core can initiate communication to any integrated NNMi management server. That NNMi management server can respond to the initiating NA core. Examples of communication from NA to NNMi include:
  - Sending SNMP traps
  - Updating SNMP community strings for a device

NNMi multi-tenancy environments

Regardless of architecture, when NNMi runs in a multi-tenancy environment, note the following:

- In an NNMi multi-tenancy environment, inventory synchronization is from NNMi to NA only.
- The HPE NNMi–HPE NA integration cannot distinguish among duplicate IP addresses. For this reason, all nodes synchronized from the NNMi management servers to connected NA cores must have unique IP addresses.

"Table 1 Integration Features" below lists the available features in the HPE NNMi–HPE NA integration and notes special considerations as applicable to the supported integration architectures.

Table 1 Integration Features

Integration Feature	Initiating Server	Notes	See Also
Synchronize the NNMi inventory into the NA inventory	NNMi	• On an NNMi global manager, synchronizes the locally managed nodes only.	"Inventory Synchronization Between NNMi and NA" on page 28
Synchronize the NA inventory into the NNMi inventory	NA	• Not available with the *NNMi Global Network Management to NA Horizontal Scalability* architecture. • Not available in an NNMi multi-tenancy environment.	
Deleting a node in NNMi unmanages that device in NA	NNMi	• When no NNMi management server is managing that node.	
Deleting a device in NA deletes that node in NNMi	NA	• On all NNMi management servers that manage that node.	
Launch NA console pages from the NNMi console	NNMi	• Available on all integrated NNMi management servers. • Opens NA console pages on the integrated NA core.	"Launching NA Console Pages from the NNMi Console" on page 31
Trigger NA diagnostics from NNMi	NNMi	• Diagnostics run on the integrated NA core.	"Triggering NA Diagnostics from NNMi" on page 32

Table 1 Integration Features, continued

Integration Feature	Initiating Server	Notes	See Also
Identify layer 2 connections with mismatched states	NNMi	• The NA inventory must include the MAC addresses for both interfaces that form a layer 2 connection.	"Identifying Layer 2 Connections with Mismatched States"
View NA data in the NNMi analysis pane (with permission)	NNMi	• Available on all integrated NNMi management servers.	"NA Information Displayed in the NNMi Analysis Pane" on page 34
Launch NNMi console pages from the NA console	NA	• Available on all NA cores in the Horizontal Scalability environment. • Opens NNMi console pages on the NNMi management server associated with the link.	"Launching NNMi Console Pages from the NA Console" on page 38
Send notifications of NA device events to NNMi	NA	• NA communicates with each NNMi management server that manages the node locally. • For any nodes that are managed by an NNMi regional management server, this functionality is not available on the NNMi global management server.	"Sending SNMP Traps to NNMi" on page 38
Trigger NNMi node configuration polls after certain NA tasks	NA		"Triggering NNMi Node Config Polls from NA" on page 39
Disable network management during device configuration	NA		"Disabling Network Management During Device Configuration" on page 40
Propagate device community string changes	NA		"Propagating Device Community String Changes to NA" on page 41
Use an SSL connection from NNMi to NA	NNMi	• Exchange certificates among all integrated NNMi management servers and all NA cores. • For NA in a Horizontal Scalability environment, install the NNMi certificate on all NA cores regardless of how the integration is configured.	"Configuring SSL Communication Between NNMi and NA" on page 19
Use an SSL connection from NA to NNMi	NA		
Single sign-on from NNMi to NA	NNMi	• Use the same initialization string on all NNMi management servers and all	"Configuring Single Sign-On Between NNMi and NA" on

Table 1 Integration Features, continued

Integration Feature	Initiating Server	Notes	See Also
		NA cores. • For NA in a Horizontal Scalability environment, configure single sign-on on all NA cores regardless of how the integration is configured.	page 24
Single sign-on from NA to NNMi	NA		

Figure 1 Example Deployment Architectures: One NNMi Management Server to One NA Core

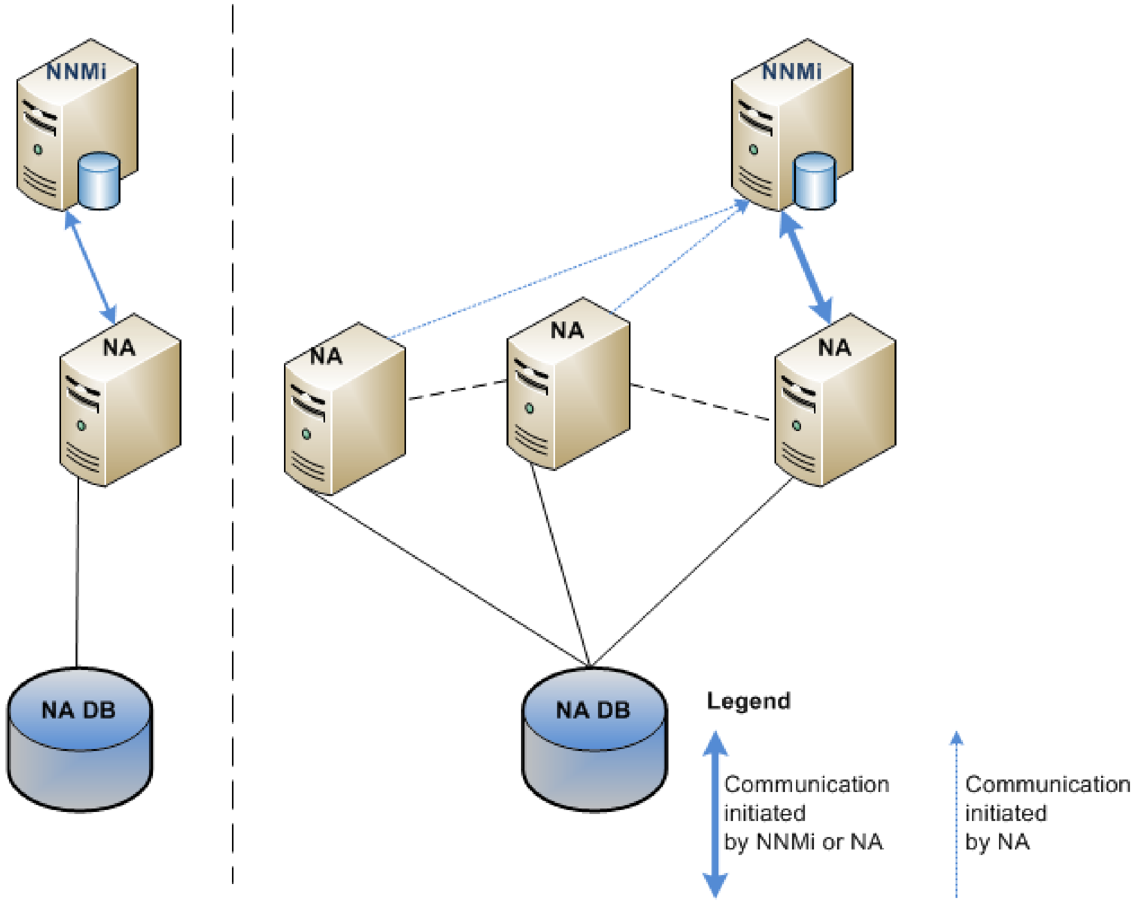

NNMi
NA
NA DB
NNMi
NA
NA
NA
NA DB
Legend
Communication initiated by NNMi or NA
Communication initiated by NA

Figure 2 Example Deployment Architecture: NNMi Global Network Management to Multiple Standalone NA Cores

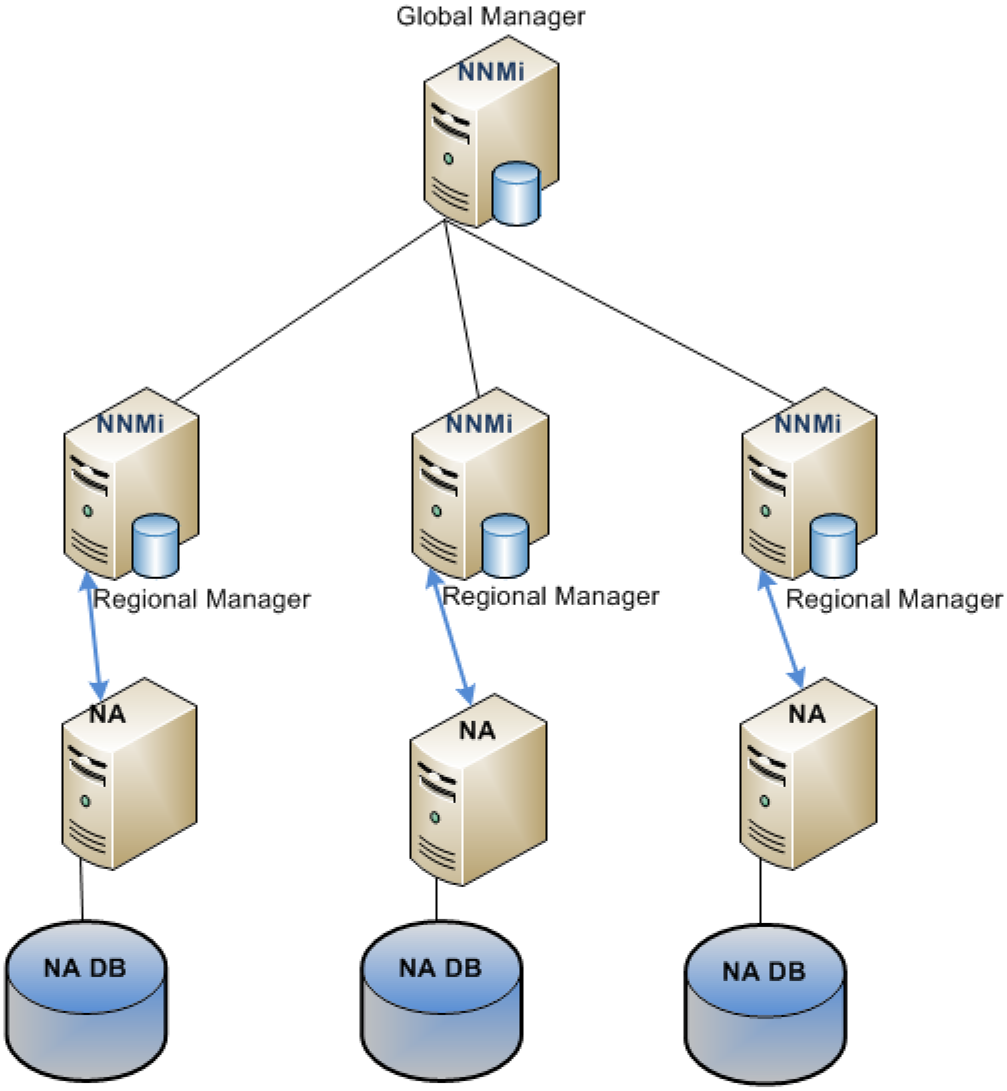
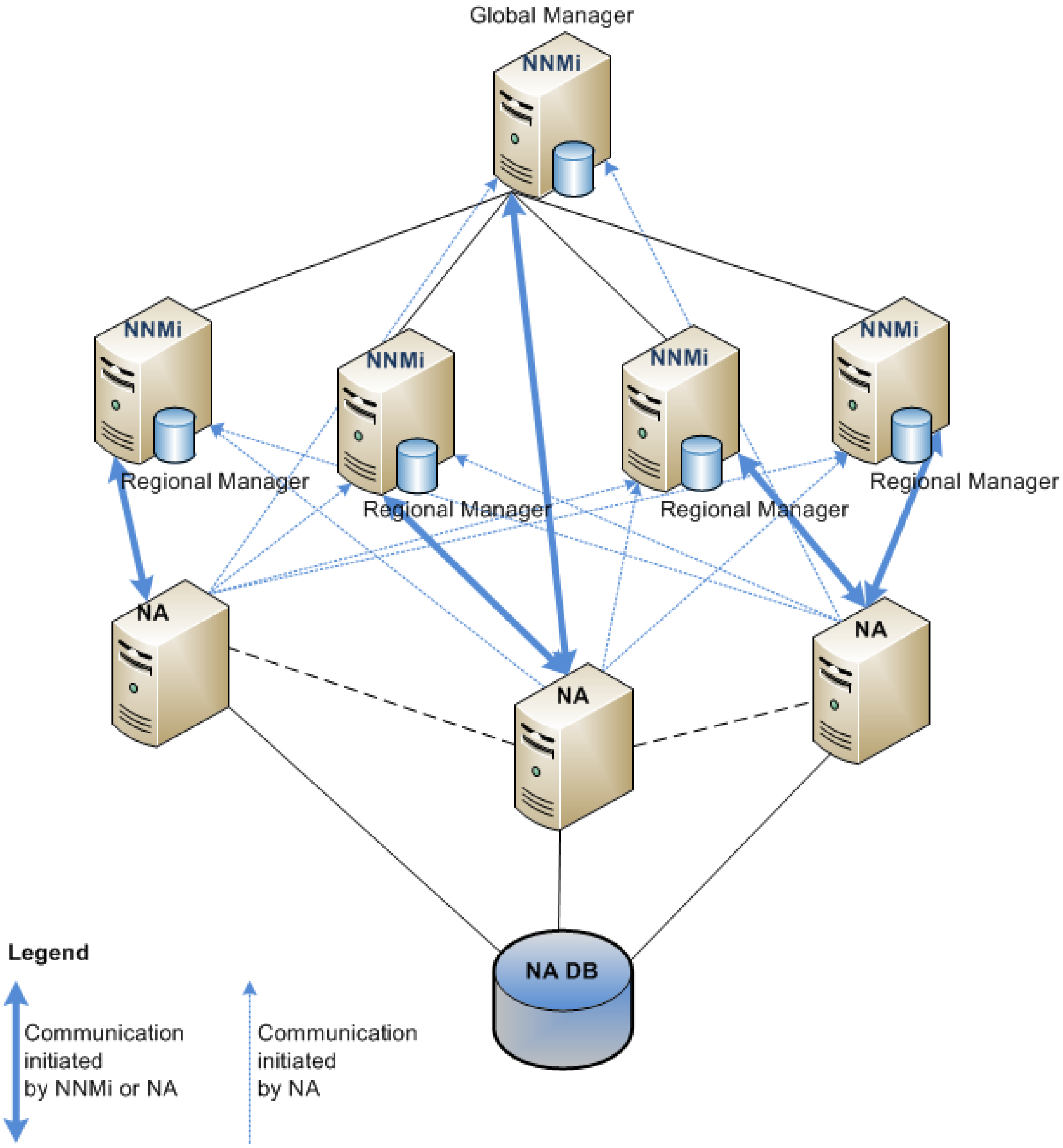


Figure 3 Example Deployment Architecture: NNMi Global Network Management to NA Horizontal Scalability



Enabling the HPE NNMi-HPE NA Integration

Enabling the HPE NNMi–HPE NA integration initiates inventory synchronization between NNMi and NA. The integration always synchronizes the NNMi inventory to NA. When only one NNMi management server is integrated with NA, the integration can also synchronize the NA inventory to NNMi.

This section describes the following procedures:

- "Preparation" below
- "New Integration Configuration" below
- "Integration Configuration Upgraded from NNMi 10.10 to NNMi 10.21" on page 18
- "Configuring SSL Communication Between NNMi and NA" on page 19
- "Configuring Single Sign-On Between NNMi and NA" on page 24

Preparation

For each NNMi management server, decide which nodes to synchronize to NA. If you will not synchronize the complete NNMi inventory for an NNMi management server, create one node group containing the nodes to synchronize with the NA inventory.

The integration can synchronize NNMi security groups to NA partitions. Before enabling this feature, do all of the following:

- In conjunction with the NNMi and NA administrators, prepare a user security plan and evaluate the user security implications of enabling the mapping of NNMi security groups to NA partitions.
- Ensure that each NNMi node is in the correct security group.
- In NA, configure which NA users can see which of the NA partitions that map to the NNMi security groups.
- In an NNMi multi-tenancy environment, ensure that each NNMi node is assigned to the correct tenant.

New Integration Configuration

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

1. Complete the processes described in "Preparation" above.
2. *Optional*. To use SSL communication with the NNMi or NA web services, exchange certificates among the NNMi and NA servers as described in "Configuring SSL Communication Between NNMi and NA" on page 19.
3. Create NA device password rules for the nodes in the NNMi inventory. In the NA console, follow these steps:
   a. Open the **Device Password Rule** page (**Devices > Device Tools > Device Password Rules**).
   b. Create one or more device password rules that specify how to communicate with the nodes in the NNMi inventory.
4. Note the number of devices in the NA inventory.
5. In the NNMi console, configure the connection from NNMi to NA:
   a. Open the **HPE NNMi–HPE NA Integration Configuration** form (**Integration Module Configuration > HPE 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. Verify that you exchanged certificates in step 2 before selecting either of these check boxes.

d. Enter the information for connecting to this NNMi management server. For information about these fields, see "NNMi Management Server Connection" on page 69.

e. Enter the information for connecting to an NA core. For information about these fields, see "NA Core Server Connection" on page 70.

f. Enter values for the remaining fields.

   - In an NNMi multi-tenancy environment, clear the **Topology Filter Node Group** field and select the **Map NNMi Security Groups to NA Partitions** check box.
   - In other environments, set these field according to your needs.

   For information about these fields, see "Integration Behavior" on page 71.

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 core server, click **Return**, and then adjust the values for connecting to the NA core server as suggested by the text of the error message.

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

7. *Optional*. Wait for initial inventory synchronization to complete.

   Compare the number of nodes in the NNMi inventory with the number of devices in the NA inventory. The number of devices in the NA inventory should increase relative to the number of nodes in the NNMi inventory (or in the NNMi topology filter node group) that were not already in the NA inventory before integration.

   Waiting for the initial inventory synchronization to the NA core to complete ensures that synchronization does not impact NA performance.

8. For each additional NNMi management server to integrate with NA, repeat step 4 through step 7.

9. *Optional for the One NNMi Management Server to One NA Core architecture and the NNMi Global Network Management to Multiple Standalone NA Cores architecture only*. If the management environment does not include NNMi multi-tenancy, enable synchronization of the NNMi device inventory into the NA inventory as follows:

   a. In the NNMi console, open the **Discovery Configuration** form (**Configuration > Discovery > Discovery Configuration**) to the **Auto-Discovery Rules** tab.

   b. Create one or more auto-discovery rules that specify how to communicate with the devices in the NNMi inventory.

   > **CAUTION:** If a device in the NNMi inventory is *not* included in an NNMi auto-discovery rule at this time, the integration will never synchronize that device into the NA inventory.

   c. In the NA console, enable the *NA/NNMi Topology Synchronization for Device Addition* event rule by setting the **Rule Status** to **Active**. For more information, see "Enable an NA Event Rule" on page 43.

   d. Re-enable the integration:

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

  - Clear the **Enable Integration** check box, and then click **Submit** at the bottom of the form.
  - Select the **Enable Integration** check box, and then click **Submit** at the bottom of the form.

10. *Optional*. In the NA console, alter the default settings of the NA functionality provided by the integration:
    a. Open the **Administrative Settings - NA/NNMi Integration** page (**Admin > Administrative Settings > NA/NNMi Integration**).
    b. Change the selections for any of the following fields:
       - **Tasks that Place Device Out-of-Service**
       - **If the device task fails**
       - **If device compliance check fails** (if available)
       - **Out Of Service Completion Delay**
       - **Tasks that Request NNMi Config Poll**

       For information about these fields, see "Configuration Parameters in the NA Console" on page 74.
    c. Click **Save** at the bottom of the page.
11. *Optional*. If you want the integration to detect connections with mismatched speed or duplex configurations for some devices, ensure that NA discovers drivers for those devices. Use one of the following methods:
    - If you configured the integration to discover drivers, the integration has already completed this step.
    - In the NA console, on the **New Task - Discover Driver** page (**Devices > Device Tasks > Discover Driver**), discover the drivers for the devices imported from the NNMi inventory.
12. *Optional*. Configure single sign-on among all integrated NNMi management servers and all NA cores as described in "Configuring Single Sign-On Between NNMi and NA" on page 24.

    TIP: Use the same initialization string on all NNMi management servers and all NA cores. For NA in a Horizontal Scalability environment, configure single sign-on on all NA cores regardless of how the integration is configured.

Integration Configuration Upgraded from NNMi 10.10 to NNMi 10.21

If you plan to upgrade either NNMi 10.0x or NA 10.1x to version 10.2x, you must upgrade both applications to the required versions for the integration to work correctly. To upgrade and enable the HPE NNMi–HPE NA integration to use NNMi 10.21 and NA 10.21, follow these steps:

1. In the NNMi console of each integration NNMi management server, disable the HPE NNMi–HPE NA integration. See "Disabling the HPE NNMi–HPE NA Integration" on page 65.
2. Upgrade all deployed NNMi management servers and all deployed NA cores to version 10.2x. Upgrade these applications in either order, as the upgrade sequence does not matter.

   NOTE: If NNMi and NA are installed on the same server, you might see a port conflict warning from the NA installer while upgrading NA. Assuming that NNMi is using the ports shown in the warning, ignore these warnings. For more information, see the NNMi *nnm.ports* reference page, or the Linux manpage.

> **NOTE:** Do not attempt to enable the HPE NNMi–HPE NA integration until you finish upgrading both NNMi and NA to the required versions.

3. Configure the HPE NNMi–HPE NA integration as described in "New Integration Configuration" on page 16. Note the following:
   - The **HPE NNMi–HPE NA Integration Configuration** form contains the values from the previous integration configuration. The new fields on this form are set to their default values.
   - NNMi 10.00 adds the **Minimum Object Access Privilege for Analysis Pane Data** field, which interacts with the **Minimum NNMi Role for Analysis Pane Data** field. Upgrading NNMi brings forward the value of the **Minimum NNMi Role for Analysis Pane Data** field and sets the **Minimum Object Access Privilege for Analysis Pane Data** field to `Object Guest`. This configuration maintains the access level as configured before the upgrade. You can refine the access level by changing the value of the **Minimum Object Access Privilege for Analysis Pane Data** field. For more information, see "Configuring NNMi User Access to NA Information in the NNMi Analysis Pane" on page 73.
   - Prior to NA 10.00, the integration provided command script examples for a single NNMi server integration. NA 10.00, no longer includes these scripts. Upgrading the integration to NA 10.00 removes the command scripts from the NNMi management server to be removed. The NA system variables used by the command scripts are no longer valid.
   - If you are upgrading from an older version of NA, the **NNMi-NA Integration Level** field is mapped as follows:
     - The value **Complete** enables the *NA/NNMi Topology Synchronization for Device Addition* event rule in NA 10.00 or later.
     - The values **Partial** and **One way from NNMi** disable the *NA/NNMi Topology Synchronization for Device Addition* event rule in NA 10.00 or later.

Configuring SSL Communication Between NNMi and NA

Before enabling the integration with SSL communication, complete the following steps to exchange certificates among the NNMi and NA servers.

> **TIP:** Exchange certificates among all NNMi management servers and NA cores involved in the integration. For NA in a Horizontal Scalability environment, install the NNMi certificate on all NA cores regardless of how the integration is configured.

> **Note:** In this procedure, the instructions assume you plan to export the default NA self-signed certificate from the `truecontrol.keystore` file. The `-alias sentinel` part of the referenced commands might be different based on the type of certificate contained in the `truecontrol.keystore` file. See *Using Certificates with NA* in the *NA Administration Guide* for more information.
>
> Prior to the version 10.20, NNMi used to provide a Java KeyStore (JKS) repository to store certificates. NNMi 10.20 introduces a Public Key Cryptography Standards (PKCS) #12 repository to store

certificates. The new PKCS #12 file-based certificate management technique is available for use as soon as you install a new instance of NNMi 10.20 on a system.

However, when you upgrade an older version of NNMi to the version 10.2x, the PKCS #12 file-based certificate management does not immediately come into effect and NNMi continues to use the JKS repository for certificate management.

With additional configuration tasks, you can configure the upgraded NNMi management server to use the new technique of PKCS #12 file-based certificate management.

1. The SSL certificates for systems integrated with NNMi must contain the fully qualified domain name (FQDN) of the integrated server, not the domain name server (DNS) short name or the name `localhost`. If necessary, re-generate the certificates for any NA core servers that integrate with NNMi. During certificate generation, specify the server's FQDN as the common name (CN) value.
2. On one NA core server, export the NA certificates from the `truecontrol.keystore` file by running the following command:
   - *Windows*:
     ```
     <NA_HOME>\jre\bin\keytool.exe -export -alias sentinel
     -file C:\temp\na.cer -keystore <NA_HOME>\server\ext\jboss\
     server\default\conf\truecontrol.keystore
     -storepass sentinel
     ```
   - *Linux*:
     ```
     <NA_HOME>/jre/bin/keytool -export -alias sentinel
     -file na.cer -keystore <NA_HOME>/server/ext/jboss/server/
     default/conf/truecontrol.keystore -storepass sentinel
     ```
3. Verify that you see the `Certificate stored in file <directory>:\na.cer` message.
4. Copy the NA certificate file (`na.cer`) that you created in step 2 to each NNMi management server.
5. On each NNMi management server, import the NA certificate into the NNMitruststore, by running the following command:
   - On a system with JKS repository:
     - *Windows*:
       ```
       %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -import
       -alias sentinel -file "<certificate file directory>\na.cer"
       -keystore %NnmDataDir%\shared\nnm\certificates\
       nnm.truststore -storepass ovpass
       ```
     - *Linux*:
       ```
       $NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -import
       -alias sentinel -file <certificate file directory>/na.cer
       -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore
       -storepass ovpass
       ```
   - On a system with PKCS#12 repository:
     - *Windows*:
       ```
       %NnmInstallDir%\bin\nnmkeytool.ovpl -import
       -alias sentinel -file "<certificate file directory>\na.cer"
       -keystore %NnmDataDir%\shared\nnm\certificates\nnm-trust.p12
       ```

```
-storetype PKCS12 -storepass ovpass
```

- *Linux*:

```
$NnmInstallDir/bin/nnmkeytool.ovpl -import
-alias sentinel -file <certificate file directory>/na.cer
-keystore $NnmDataDir/shared/nnm/certificates/nnm-trust.p12
-storetype PKCS12 -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
```

6. On one NNMi management server, determine the NNMi certificate alias name using the following command.

   - On a system with JKS repository:
     - *Windows*:

```
%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -v -list
-keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore
-storepass nnmkeypass
```

     - *Linux*:

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

   - On a system with PKCS#12 repository:
     - *Windows*:

```
%NnmInstallDir%\bin\nnmkeytool.ovpl -v -list
-keystore %NnmDataDir%\shared\nnm\certificates\nnm-key.p12
-storetype PKCS12 -storepass nnmkeypass
```

     - *Linux*:

```
<NnmInstallDir>/bin/nnmkeytool.ovpl -v -list -keystore
<NnmDataDir>/OV/shared/nnm/certificates/nnm-key.p12 -storetype PKCS12 -
storepass nnmkeypass
```

7. Export the NNMi certificate to a file using the following command. For `<alias>`, use the value from the output of the command in "On one NNMi management server, determine the NNMi certificate alias name using the following command." above.

   - On a system with JKS repository:
     - *Windows*:

```
%NnmInstallDir%\nonOV\hpsw\bin\keytool -export
-alias <alias> -file <directory>\nnm.cer
```

```
-keystore %NNMDataDir%\shared\nnm\certificates\nnm.keystore
-storepass nnmkeypass
```

    - *Linux*:
      ```
      <NnmInstallDir>/nonOV/jdk/hpsw/bin/keytool -export
      -alias <alias> -file <directory>/nnm.cer
      -keystore <NnmDataDir>/shared/nnm/certificates/nnm.keystore
      -storepass nnmkeypass
      ```

  - On a system with PKCS#12 repository:
    - *Windows*:
      ```
      %NnmInstallDir%\bin\nnmkeytool.ovpl -export
      -alias <alias> -file <directory>\nnm.cer
      -keystore %NNMDataDir%\shared\nnm\certificates\nnm-key.p12
      -storetype PKCS12 -storepass nnmkeypass
      ```
    - *Linux*:
      ```
      <NnmInstallDir>/bin/nnmkeytool.ovpl -export
      -alias <alias> -file <directory>/nnm.cer
      -keystore <NnmDataDir>/shared/nnm/certificates/nnm-key.p12
      -storetype PKCS12 -storepass nnmkeypass
      ```

8. Copy the NNMi certificate file (`nnm.cer`) to each NA core server.
9. On each NA core server, import the NNMi certificate to the NA `truecontrol.truststore` file by running the following command. For `<alias>`, use the value from the output of the command in step 6.
   - *Windows*:
     ```
     <NA_HOME>\jre\bin\keytool.exe -import -alias <alias>
     -file <Directory>\nnm.cer -keystore <NA_HOME>\server\ext\
     jboss\server\default\conf\truecontrol.truststore
     -storepass sentinel
     ```

   - *Linux*:
     ```
     <NA_HOME>/jre/bin/keytool -import -alias <alias>
     -file <Directory>/nnm.cer -keystore <NA_HOME>/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
   ```
10. On each NA core server, restart the NA services:

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:

  TrueControl ManagementEngine

  TrueControl FTP Server

  TrueControl SWIM Server

  TrueControl Syslog Server

  TrueControl TFTP Server

- *Linux*: Run the following command:

  ```
  /etc/init.d/truecontrol restart
  ```

11. Run the following command sequence on each NNMi management server:

    - `ovstop`
    - `ovstart`

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

    - NNMi management server (Windows):

      Server with the JKS repository

      ```
      %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool -v -list
      -keystore %NnmDataDir%\shared\nnm\certificates\
      nnm.truststore -storepass ovpass
      ```

      Server with the PKCS#12 repository

      ```
      %NnmInstallDir%\bin\nnmkeytool.ovpl -v -list
      -keystore %NnmDataDir%\shared\nnm\certificates\
      nnm-trust.p12 -storetype PKCS12 -storepass ovpass
      ```

    - *NNMi management server (Linux)*:

      Server with the JKS repository

      ```
      <NnmInstallDir>/nonOV/jdk/hpsw/bin/keytool -v -list
      -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore
      -storepass ovpass
      ```

      Server with the PKCS#12 repository

      ```
      <NnmInstallDir>/bin/nnmkeytool.ovpl -v -list
      -keystore $NnmDataDir/shared/nnm/certificates/nnm-trust.p12
      -storetype PKCS12 -storepass ovpass
      ```

    - *NA core server (Windows)*:

      ```
      <NA_HOME>\jre\bin\keytool.exe -v -list -keystore <NA_HOME>\
      server\ext\jboss\server\default\conf\truecontrol.truststore
      -storepass sentinel
      ```

    - *NA core server (Linux)*:

      ```
      <NA_HOME>/jre/bin/keytool -v -list -keystore
      /opt/NA/server/ext/jboss/server/default/conf/truecontrol.truststore -storepass
      sentinel
      ```

Configuring Single Sign-On Between NNMi and NA

NOTE: When Security Assertion Markup Language (SAML) is enabled, NA does not support the NNMi SSO (also known as LWSSO (Light-weight Single Sign-on)) feature between NNMi and NA.

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

If the NNMi and NA user names are exactly the same for a particular individual, that person can log on to the NNMi console and view NA pages without logging on to the NA console. Likewise, that person can log on to the NA console and view NNMi pages without logging on to the NNMi console.

This single sign-on feature maps user names, but not passwords, between the two products. The passwords for logging on to NNMi and 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 NNMi and administrator privileges in NA.

For single sign-on access between NNMi and NA, ensure 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.

TIP: Use the same initialization string on all NNMi management servers and all NA cores. For NA in a Horizontal Scalability environment, configure single sign-on on all NA cores regardless of how the integration is configured.

To configure single sign-on between NNMi and NA, complete both of the following tasks:

- "Task 1: Configure NNMi for Single Sign-On" below
- "Task 2: Configure NA for Single Sign-On" on the next page

Task 1: Configure NNMi for Single Sign-On

On each NNMi management server, complete the following steps:

1. Open the following file in a text editor:
   - *Windows*: `%NNM_PROPS%\nms-ui.properties`
   - *Linux*: `$NNM_PROPS/nms-ui.properties`
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
   ```
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. Ensure that the value of the `initString` parameter is the same for all NNMi management servers.
5. Run the following command:

   `nnmsso.ovpl -reload`

   See the *nnmsso.ovpl* reference page, or the Linux man page, for more information.

Task 2: Configure NA for Single Sign-On

On each NA core server, complete the following steps:

1. Open the following file in a text editor:
   - *Windows*:
     `<NA_HOME>\server\ext\jboss\server\default\conf\lwssofmconf.xml`
   - *Linux*:
     `<NA_HOME>/server/ext/jboss/server/default/conf/lwssofmconf.xml`

   The default value of `<NA_HOME>` is as follows:
   - *Windows*: `C:\na`
   - *Linux*: `/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 core server. For example, if the hostname of the NA core server is na.location.example.com, set `<domain>location.example.com</domain>`.

     NOTE: This step assumes that the NNMi management server is in the same domain as the NA core 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, verify or set the `initString` attribute to the value of the `initString` property in the NNMi `nms-ui.properties` file.

   NOTE: 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:

   ```
   <multiDomain>

   <trustedHosts>

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

```
</trustedHosts>

</multiDomain>
```

6. The actions in the above step assume that the NNMi management server is in the same domain as the NA core server. If the NA core server is in a different domain than the NNMi management server, remove the **`<!--`** and **`-->`** characters shown in the following example, and then add `DNSDomain` entries for both domains:

   ```
   <multiDomain>
       <trustedHosts>
           <!--
           <DNSDomain>gmx.com</DNSDomain>
           <DNSDomain>companydomain2.com</DNSDomain>
           <NetBiosName>myserver</NetBiosName>
           <IP>192.168.12.13</IP>
           <FQDN>myserver.companydomain.com</FQDN>
           -->
       </trustedHosts>
   </multiDomain>
   ```

7. 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 system time, after conversion to GMT, should be the same.
8. Restart the NA jboss server:
   - *Windows*: In the NA console, on the **Admin > Start/Stop Services** page, restart the Management Engine.
   - *Linux*: Run the following command:

     `/etc/init.d/truecontrol restart`

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

   > **NOTE:** If NNMi or NA automatically logs you out of its user interface, or if you manually log out of either NNMi or NA, you will be logged out of both the NNMi console and the NA console.

   Do the following to set identical NNMi and NA timeout values:

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

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

      - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf\lwssofmconf.xml`
      - *Linux*: `<NA_HOME>/server/ext/jboss/server/default/conf/lwssofmconf.xml`

      The default value of `<NA_HOME>` is as follows:

      - *Windows*: `C:\na`
      - *Linux*: `/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 the NA services.

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

   - *Windows*: `%NNM_PROPS%\nms-ui.properties`
   - *Linux*: `$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, and 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 Linux man page, for more information.

Using the HPE NNMi-HPE NA Integration

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

- "Inventory Synchronization Between NNMi and NA" below
- "NNMi Functionality Provided by the Integration" on page 31
- "NA Functionality Provided by the Integration" on page 37

Inventory Synchronization Between NNMi and NA

The HPE NNMi–HPE NA integration dynamically synchronizes the NNMi inventory with the devices in the NA inventory. The integration matches NNMi nodes with NA devices by comparing IP addresses. The integration adds the NA device ID to each synchronized NNMi node and the NNMi node UUID to each synchronized NA device.

When is the NNMi inventory synchronized?

Enabling the HPE NNMi–HPE NA integration enables synchronization of the NNMi inventory into the NA inventory. Synchronization of the NNMi inventory into the NA inventory occurs continuously while the integration remains enabled.

Which NNMi nodes?

The HPE NNMi–HPE NA integration synchronizes some or all of the nodes in the NNMi inventory as determined by the **Topology Filter Node Group** parameter on the HPE NNMi–HPE NA **Integration Configuration** form.

- If a node group is specified, only the nodes in that group are synchronized with the NA inventory.
- To synchronize the entire NNMi inventory to the NA inventory, clear the **Topology Filter Node Group** field.

Where do NNMi nodes go in the NA inventory?

The NA partition for inventory synchronization depends on whether the **Map NNMi Security Groups to NA Partitions** check box is selected on the **HPE NNMi–HPE NA Integration Configuration** form.

- If the **Map NNMi Security Groups to NA Partitions** check box is selected, a device synchronized from NNMi to NA is always added or updated to an NA partition of the same name as the NNMi security group that contains the node. If an NNMi administrator later moves this node to a different security group, synchronization moves the NA device to the corresponding NA partition. If the partition does not exist, NNMi creates one with the same name as the NNMi security group and associates it with the NA `Site` view with an *NNMi Security Group* description. If the device exists in a different NA partition, synchronization moves the device to the NA partition that matches the NNMi security group. The NNMi `Default Security Group` maps to the NA `Default Site` partition. Changing either name does not change this mapping.

  > **TIP:** If multiple NNMi regional managers manage the same node, ensure that the node is in the same NNMi security group on all NNMi regional managers.

- If the **Map NNMi Security Groups to NA Partitions** check box is cleared, the NA partition for a device depends on whether the device already exists in the NA inventory.

- If the device does not already exist in the NA inventory, synchronization creates the device in the NA `Default Site` partition. If an NA administrator later moves this device to a different partition, the integration leaves the device in that different partition.
- If the device already exists in the NA inventory, that device remains in the assigned partition.

> **NOTE:** Prior to NA 10.00, each synchronization cycle moved all synchronized devices to the NA `Default Site` partition.

Nodes added to NNMi

When a node is added to the NNMi inventory in the node group specified by the **Topology Filter Node Group** parameter, the integration synchronizes that node to the NA inventory as described here.

Nodes deleted from NNMi

When a synchronized node is deleted from NNMi, the integration removes the association with that NNMi management server from the NA device. When the device no longer has any associated NNMi node UUIDs, the integration unmanages the corresponding device in NA. The device history is still available for unmanaged devices in NA.

When is the NA inventory synchronized?

When only one NNMi management server integrates with NA, the *NA/NNMi Topology Synchronization for Device Addition* event rule determines whether the integration synchronizes the NA inventory into the NNMi inventory.

- If the *NA/NNMi Topology Synchronization for Device Addition* event rule is active, synchronization occurs for the entire NA inventory as described here.
- If the *NA/NNMi Topology Synchronization for Device Addition* event rule is inactive, integration synchronization is one way from NNMi to NA.

> **NOTE:** When multiple NNMi management servers integrate with one NA deployment, the integration ignores the *NA/NNMi Topology Synchronization for Device Addition* event rule and does not synchronize the NA inventory into the NNMi inventory. One NA deployment is any of the following:

- A standalone NA core
- NA in a horizontal scalability environment

> **TIP:** In an NNMi multi-tenancy environment, note the following: Because NNMi auto-discovery always assigns new nodes to the Default Tenant, the NNMi administrator should directly control the addition of new nodes to the NNMi inventory. For this reason, the *NA/NNMi Topology Synchronization for Device Addition* event rule should always be disabled in an NNMi multi-tenancy environment.

Synchronization of the NA inventory into the NNMi inventory occurs each time the integration is enabled.

Which NA devices?

Synchronization occurs for the entire NA inventory.

NOTE: For Cisco devices that support virtual device contexts (VDC), NA discovers all VDCs during context discovery of those devices. During integration synchronization, NA sends only the resolvable management context IP addresses to NNMi. To include the remaining VDCs in the synchronized inventory, seed those VDC nodes in NNMi separately.

Where do NA devices go in the NNMi inventory?

For devices in the NA inventory that are not in the NNMi inventory, the integration sends discovery hints to NNMi.

- If an NNMi auto-discovery rule includes the hinted device, NNMi discovers the node. The NNMi node group configuration determines which node groups include the devices hinted by NA. In NNMi, the new node is added to the Default Security Group and the Default Tenant.
- If no NNMi auto-discovery rule includes the hinted device, NNMi does not discover the node.

  TIP: The integration sends discovery hints only during initial synchronization. To trigger the integration to resend discovery hints, disable and then enable the integration.

Devices added to NA

When a new device is added to the NA inventory, the integration sends a discovery hint to NNMi.

TIP: If the new device was previously in the NA inventory and was deleted after synchronization, NNMi does not respond to the discovery hint. In this case, crease a discovery seed for the device in NNMi.

Devices deleted from NA

When a synchronized device is deleted from NA, the integration deletes the corresponding node from the NNMi inventory of all NNMi management servers that manage the node.

Nodes moved after synchronization

When a synchronized node is moved out of the node group specified by the **Topology Filter Node Group** parameter to a different node group, the NA inventory is not immediately affected. However, if this node is later deleted from NNMi, the integration unmanages the corresponding device in NA. Likewise, if this node is later deleted from NA, the integration deletes the corresponding node from the NNMi inventory.

Periodic Synchronization Considerations

Periodically, the HPE NNMi–HPE NA integration performs a complete inventory synchronization from NNMi to NA. The HPE NNMi–HPE NA integration does not perform a complete inventory synchronization from NA to NNMi. If the HPE NNMi–HPE 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 **HPE NNMi–HPE NA Integration Configuration** form specifies the frequency of periodic inventory synchronization.

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

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

Support for HPE Blade System Virtual Connect Devices

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

   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 **HPE NNMi–HPE NA Integration Configuration** form with the name of the parent node group. For more information, see "Integration Behavior" on page 71.

NNMi Functionality Provided by the Integration

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

- "Launching NA Console Pages from the NNMi Console" below
- "Triggering NA Diagnostics from NNMi" on the next page
- "Identifying Layer 2 Connections with Mismatched States" on page 33
- "NA Information Displayed in the NNMi Analysis Pane" on page 34

Launching NA Console Pages from the NNMi Console

The HPE NNMi–HPE NA integration provides links to open NA console pages from the NNMi console in the context of the NNMi view.

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

- **Show HPE 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 33.

- **Rerun HPE 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 the next page.
- **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 the next page.
- **View HPE NA Device Information**—Opens the current NA **Device Details** page for the device selected in NNMi.
- **View HPE NA Device Configuration**—Opens the NA **Current Configuration** page for the device selected in NNMi.

  > **NOTE:** If real-time change detection is disabled for a device, the information shown is the configuration 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 HPE NA Device Configuration Diffs**—Opens the NA **Compare Device Configuration** page for the device selected in NNMi.
- **View HPE NA Device Configuration History**—Opens the NA **Device Configurations History** page for the device selected in NNMi.
- **View HPE NA Policy Compliance Report**—Opens the NA **Policy, Rule and Compliance Search Results** page for the device selected in NNMi.

  > **NOTE:** Compliance information requires the NA Ultimate license.

- **Telnet to HPE NA Device**—Opens a **Telnet** window for connecting to the device selected in NNMi.
- **SSH to HPE NA Device**—Opens an **SSH** window for connecting to the device selected in NNMi.
- **Launch HPE NA**—Opens the NA console.
- **Launch HPE NA Command Scripts**—Opens the **New Task—Run Command Script** page in NA. The page is pre-filled for the node or incident selected in the NNMi console.
- **Launch HPE NA Diagnostics**—Opens the **New Task—Run Diagnostics** page in 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 *HPE Network Automation User Guide*.

Triggering NA Diagnostics from NNMi

Enabling the HPE NNMi–HPE 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 2 NNMi Incidents Configured with NA Diagnostics" below lists the modified incidents.

Table 2 NNMi Incidents Configured with NA Diagnostics

NNMi Incident	NA Diagnostic
OSPFNbrStateChange	Show Neighbor

Table 2 NNMi Incidents Configured with NA Diagnostics, continued

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

Configuring NA Diagnostics and Command Scripts as Incident Actions

You can add an action that accesses 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 2 NNMi Incidents Configured with NA Diagnostics" on the previous page.

Viewing the Results of Incident Actions that Access NA

When an incident of a type that has been configured with an NA action arrives, 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 HPE NA Diagnostic Results** and **Rerun HPE 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 HPE NA Diagnostic Results**.

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

If you run the task multiple times, NNMi lists the most recent task ID on the **Custom Attributes** tab of the **Incident** form. The **Show NA 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 HPE NNMi–HPE NA integration is enabled, NNMi periodically queries NA for the speed and duplex settings of the two interfaces on either end of each layer 2 connection in the NNMi topology. Additionally, NNMi queries 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. NNMi uses a mismatch detection algorithm to determine whether the values might result in a mismatched connection.

NOTE: 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 devices that use the same MAC address for multiple ports, enable storing duplicate MAC addresses in NA. For more information, see “Configuring NA to Store Duplicate MAC Addresses” in the *NA Administration Guide*.

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

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:

- `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 **NA Connection Check Interval** parameter on the **HPE NNMi–HPE NA Integration Configuration** form specifies the frequency of the connection queries.

NA Information Displayed in the NNMi Analysis Pane

The NNMi analysis pane contains NA information for nodes and for interfaces on nodes synchronized through the HPE NNMi–HPE NA integration. "Table 3 NA Information in the NNMi Analysis Pane" below lists the NNMi views that can include the integration-provided analysis pane tabs.

Table 3 NA Information in the NNMi Analysis Pane

NNMi View	Available NA Analysis Pane Tabs
• Node inventory view • Node details form	• Node Configuration • History of Node Configuration • Node Policy Compliance
• Incident browsing view • Incident form For specific incident types. See "Node Incident Types for NA Analysis Pane Tabs" on page 36.	• Node Configuration • History of Node Configuration
• Interface inventory view • Interface details form	• Interface Configuration
• Incident browsing view • Incident form For specific incident types. See "Interface Incident Types for NA Analysis Pane Tabs" on page 37.	• Interface Configuration

NOTE: The NNMi administrator can restrict access to these analysis pane tabs to certain NNMi user roles and object access levels. For more information, see "Configuring NNMi User Access to NA Information in the NNMi Analysis Pane" on page 73.

Node Configuration Tab

The **Node Configuration** tab displays the current running configuration of the node.

The **Node Configuration** tab is available for the following NNMi views:

- Node inventory view
- Node details form for a synchronized node
- Incident browsing view
- Incident form for an incident related to a synchronized node

For the applicable incident types, see "Node Incident Types for NA Analysis Pane Tabs" on the next page.

To access this information in the NA console, in the NNMi console select **Actions** > **HPE Network Automation** > **View HPE NA Device Configuration**.

History of Node Configuration Tab

The **History of Node Configuration** tab displays a table of times that the node configuration changed.

To view additional node configuration information in the NA console, click **Compare to Previous** or **View Config**.

The **History of Node Configuration** tab is available for the following NNMi views:

- Node inventory view
- Node details form for a synchronized node
- Incident browsing view
- Incident form for an incident related to a synchronized node

For the applicable incident types, see "Node Incident Types for NA Analysis Pane Tabs" on the next page.

To access this information in the NA console, in the NNMi console select **Actions** > **HPE Network Automation** > **View HPE NA Device Configuration History**.

Node Policy Compliance Tab

The **Node Policy Compliance** tab displays a table of the active configuration policies that apply to the node with an indication of whether the node is in compliance with each policy.

NOTE: Compliance information requires the NA Ultimate license.

Possible values for the **In Compliance** column are as follows:

- Yes—The device's configuration is in compliance with all applicable policies.
- No—The device's configuration is not in compliance with one or more applicable policies.
- Unknown—No policies have been run against the device or an applicable policy contains an error. This value corresponds to the `Not checked yet` value in the output of the `show policy compliance` command in the NA API.

To view the policies for this node in the NA console, click **View Policy Compliance in NA**.

The **Node Policy Compliance** tab is available for the following NNMi views:

- Node inventory view
- Node details form for a synchronized node

The following message indicates that NA has not run policy compliance checks against this node:

```
There is no active device policy compliance information to report.
```

This message can occur in any of the following cases:

- NA has not yet run any configuration policies against this device.
- The NA configuration policies for this device are not active. The Policies page (**Policies > Policy List**) in the NA console shows the status (Active or Inactive) of the available configuration policies.
- NA is not using the NA Ultimate license.

Interface Configuration Tab

The **Interface Configuration** tab displays the current running configuration of the interface as determined from the device configuration.

The **Interface Configuration** tab is available for the following NNMi views:

- Interface inventory view
- Interface details form for an interface on a synchronized node
- Incident browsing view
- Incident form for an incident related to an interface on a synchronized node

For the applicable incident types, see "Interface Incident Types for NA Analysis Pane Tabs" on the next page.

For information about how the integration matches NNMi interfaces to NA ports, see "Interface Matching Between NNMi and NA" on the next page.

Node Incident Types for NA Analysis Pane Tabs

The Node Configuration and History of Node Configuration analysis pane tabs are available for the following incident types:

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

- RoundTripTimeHigh
- TestFailed

Interface Incident Types for NA Analysis Pane Tabs

The Interface Configuration analysis pane tab is available for the following incident types:

- InterfaceDown
- InterfaceFCSLANErrorRateHigh
- InterfaceFCSWLANErrorRateHigh
- InterfaceInputDiscardRateHigh
- InterfaceInputErrorRateHigh
- InterfaceInputUtilizationHigh
- InterfaceOutputDiscardRateHigh
- InterfaceOutputErrorRateHigh
- InterfaceOutputUtilizationHigh
- InterfaceTraffic

Interface Matching Between NNMi and NA

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

1. NNMi matches an interface IP address from NNMi to a port IP address from NA.
2. NNMi matches a port name from NA to any of the following interface attributes from NNMi: `ifName`, `ifAlias`, `ifDescr`, or `sourceObjectName`.
3. NNMi matches a MAC layer address from NA to a physical address from NNMi.

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

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

NA Functionality Provided by the Integration

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

- "Launching NA Console Pages from the NNMi Console" on page 31
- "Sending SNMP Traps to NNMi" on the next page
- "Triggering NNMi Node Config Polls from NA" on page 39
- "Disabling Network Management During Device Configuration" on page 40
- "Propagating Device Community String Changes to NA" on page 41
- "NA Event Rules for the HPE NNMi–HPE NA Integration" on page 42

NOTE: Integration behavior configured in NA applies to all integrated NNMi management servers.

Launching NNMi Console Pages from the NA Console

The HPE NNMi–HPE NA integration provides links to open NNMi console pages from the NA console.

- On the **Device Details** page, the NNMi Associations table includes the following links for each NNMi management server that manages the device:
  - NNMi server—Opens the NNMi console to the initial view for this NNMi management server.
  - NNMi node UUID—Opens the NNMi console to the **Node** form for this device.
- On the **Administrative Settings - NA/NNMi Integration** page, each value in the NNMi Server column of the Integration Server List is a link to the initial NNMi console view for this NNMi management server.

For information about using the NNMi functionality, see the NNMi help.

Sending SNMP Traps to NNMi

Enabling the HPE NNMi–HPE NA integration configures NA to send SNMP traps to NNMi when specified NA events occur for synchronized NA devices. The NNMi operator can see these traps in the incident views and investigate the changes if necessary.

In NNMi, the NASnmpTrapv1 and NASnmpTrapv2 incident types control the format of the NA trap messages in the NNMi incident views. Enabling the integration adds these incident types to the SNMP trap configurations available in NNMi.

In NA, the *NA/NNMi Integration using SNMP Traps (NNMi Server)* event rule determines the NA events that cause NA to send SNMP traps to NNMi. Additionally, this event rule determines the community string in the traps, SNMP version of the traps, and to which NNMi port NA sends the traps.

Enabling the integration adds one of these event rules for each NNMi management server. The default configuration of the *NA/NNMi Integration using SNMP Traps (NNMi Server)* event rule is as follows:

- NA sends SNMP traps for device configuration changes only.
- The traps contain the community string that NA uses to access the device.
- The traps use SNMPv1 format.
- The traps are sent to port 162 on the NNMi management server.

You can customize the event rule to be different for each NNMi management server.

Customize Sending SNMP Traps

To change the configuration of the *NA/NNMi Integration using SNMP Traps* event rule for the integration with one NNMi management server, follow these steps:

1. In the NA console, open the Event Notification & Response Rule page (**Admin > Event Notification & Response Rule**).
2. In the row for the *NA/NNMi Integration using SNMP Traps* event rule for the NNMi management server, select **Edit**.
3. On the Edit Event Notification & Response Rule page, make any of the following changes:

- In the **when the following events occur** field, select the NA events that should cause NA to send SNMP traps to NNMi.

  > **TIP:** NA sends SNMP traps only for NA events that are associated with a device. This field includes events that are not specific to a device, for example: User Added. NA ignores these non-device events.

- Set the **SNMP Trap Receiver Port** field to the value for the NNMi management server.
- Set the **SNMP Community String** field to the value to include in traps to this NNMi management server.
- Set the **SNMP Version** field to either `SNMPv1` or `SNMPv2`.

> **NOTE:** Do not change any other settings in the event rule configuration.

4. Click **Save**.

Disable Sending SNMP Traps

To prevent NA from sending SNMP traps to an NNMi management server, set the rule status to inactive for the *NA/NNMi Integration using SNMP Traps* event rule for that NNMi management server. For more information, see "Disable an NA Event Rule" on page 44.

Triggering NNMi Node Config Polls from NA

For certain device configuration tasks, after the task completes, NA triggers node rediscovery on the NNMi management servers that manage the device. This node rediscovery ensures that NNMi maintains accurate information about the device.

Customize Triggering NNMi Node Config Polls

In the NA console, the **Tasks that Request NNMi Config Poll** field on the **Administrative Settings - NA/NNMi Integration** page specifies the device configuration tasks that trigger 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

Disable Triggering NNMi Node Config Polls

To prevent NA from triggering node config polls in NNMi, set the rule status to inactive for the *NA/NNMi Integration Rediscover Host* event rule. For more information, see "Disable an NA Event Rule" on page 44.

Disabling Network Management During Device Configuration

NNMi routinely checks the status of nodes with the MANAGED management mode and generates incidents for any nodes that do not respond. During device maintenance procedures initiated by NA, the HPE NNMi–HPE NA integration can change the management mode in NNMi to OUT OF SERVICE. In this way, NNMi does not generate unnecessary incidents about nodes with a known reason for being unresponsive.

For certain device configuration tasks, NA sends an out-of-service event to the NNMi management servers that manage the device. After device configuration succeeds, NA sends an in-service event to the same NNMi management servers. NNMi responds to the in-service event by removing the OUT OF SERVICE management mode from the device and resuming regular state polling.

Customize Out-of-Service Behavior

In the NA console, the **Tasks that Place Device Out-of-Service** field on the **Administrative Settings - NA/NNMi Integration** page specifies the device configuration tasks that trigger NNMi to set a device to the OUT OF SERVICE management mode 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

In the NA console, the value of the **Out Of Service Completion Delay** field on the **Administrative Settings - NA/NNMi Integration** page specifies the time that NA should wait between completing one of the tasks selected in the **Tasks that Place Device Out-of-Service** field and triggering NNMi to reset the management mode of the device. This time prevents NNMi from creating down incidents while the device is recovering from the configuration task. For example, device startup can take several minutes.

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

- The **If the device task fails** setting specifies what the integration should do with the NNMi management mode if device configuration is not successful. Choices are:
  - Restore the management mode to its value prior to the NA out-of-service event. (This is the default setting.)
  - Retain the OUT OF SERVICE management mode.
- The **If device compliance check fails** setting specifies what the integration should do with the NNMi management mode if the device configuration is not compliant upon completion of the NA task. Choices are:
  - Restore the management mode to its value prior to the NA out-of-service event. (This is the default setting.)
  - Retain the OUT OF SERVICE management mode.

  NOTE: The device compliance check is only available for the NA Ultimate license.

These settings apply to all device tasks selected in the **Tasks that Place Device Out-of-Service** field. You cannot set the recovery behavior per task.

Disable Out-of-Service Behavior

To prevent NA from triggering node config polls in NNMi, set the rule status to inactive for the *NA/NNMi Integration Out Of Service* event rule. For more information, see "Disable an NA Event Rule" on page 44.

Propagating Device Community String Changes to NA

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

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

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

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

  NOTE: NA sends updates to NNMi for all nodes that have ever been included in the node group specified by the **Topology Filter Node Group** parameter.
- If a new device is added to the NA inventory, NA informs NNMi of the SNMPv1 and SNMP v2c community strings that NA uses for managing the device.

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

SNMP community string propagation is disabled by default. To enable SNMP community string propagation, set the rule status to active for the *NA/NNMi Integration SNMP Community String Propagate* event rule. For more information, see "Enable an NA Event Rule" on the next page.

NA Event Rules for the HPE NNMi-HPE NA Integration

NA event rules define how NA communicates with the NNMi management servers. Access these event rules on the **Event Notification & Response Rules** page (**Admin > Event Notification & Response Rules**) in the NA console.

> **CAUTION:** Do not delete these event rules from NA. Modify these event rules only as instructed elsewhere in this document.

The integration defines the following event rules in NA:

- *NA/NNMi Integration Out Of Service*

  When certain NA tasks start, the integration sets the synchronized device to the OUT OF SERVICE management mode in NNMi. After the NA task completes, the integration sets the device back to the prior management mode in NNMi.

  For this event rule, NA communicates with only those NNMi management servers that manage the device.

  Configure this event rule with the **Tasks that Place Device Out-of-Service** field on the NA **Administrative Settings - NA/NNMi Integration** page. Enable or disable this functionality by enabling or disabling this event rule.

  The default and required configuration for this event rule selects the following events in the **when the following events occur** field:

  - Task Completed
  - Task Started

  For more information, see "Disabling Network Management During Device Configuration" on page 40.

- *NA/NNMi Integration Rediscover Host*

  When the configuration of a synchronized NA device changes, NA requests that NNMi rediscover the device.

  For this event rule, NA communicates with only those NNMi management servers that manage the device.

  Configure this event rule with the **Tasks that Request NNMi Config Poll** field on the NA **Administrative Settings - NA/NNMi Integration** page. Enable or disable this functionality by enabling or disabling this event rule.

  The default and required configuration for this event rule selects the following event in the **when the following events occur** field:

  - Device Configuration Change

  For more information, see "Triggering NNMi Node Config Polls from NA" on page 39.

- *NA/NNMi Integration SNMP Community String Propagate*

  When NA changes the community string for accessing a device, NA sends that community string to NNMi.

  For this event rule, NA communicates with only those NNMi management servers that manage the device.

Configure this functionality by enabling or disabling this event rule.

The default and required configuration for this event rule selects the following events in the **when the following events occur** field:

- Device Password Change
- Last Used Device Password Changed

For more information, see "Propagating Device Community String Changes to NA" on page 41.

- *NA/NNMi Integration using SNMP Traps (NNMi Server)*

  When certain NA events occur for synchronized NA devices, NA sends an SNMP trap to NNMi. The HPE NNMi–HPE NA integration creates one copy of this event rule for each NNMi management server involved in the integration.

  If multiple NNMi management servers manage the device, NA forms the SNMP trap separately for each of those NNMi management servers according to the configuration of the event rule for that NNMi management server.

  Configure this functionality by modifying this event rule for each NNMi management server. Enable or disable this functionality by enabling or disabling this event rule for each NNMi management server.

  By default, the following events are selected in the **when the following events occur** field:

  - Device Added
  - Device Configuration Change

  For more information, see "Sending SNMP Traps to NNMi" on page 38.

- *NA/NNMi Topology Synchronization for Device Addition*

  When a new device is added to the NA inventory, NA sends a device discovery hint to NNMi.

  This event rule only applies when only one NNMi management server integrates with NA.

  This event rule is disabled by default. Configure this functionality by enabling or disabling this event rule.

  The default and required configuration for this event rule selects the following event in the **when the following events occur** field:

  - Device Added

  In an NNMi multi-tenancy environment, never enable this event rule. For more information, see "When is the NA inventory synchronized?" on page 29.

- *NA/NNMi Topology Synchronization for Device Deletion*

  When a synchronized device is deleted from the NA inventory, NA sends a request to delete the device from the NNMi inventory.

  For this event rule, NA communicates with only those NNMi management servers that manage the device.

  Configure this functionality by enabling or disabling this event rule.

  The default and required configuration for this event rule selects the following event in the **when the following events occur** field:

  - Device Deleted

Enable an NA Event Rule

To enable an NA event rule, follow these steps:

1. In the NA console, open the Event Notification & Response Rule page (**Admin > Event Notification & Response Rule**).
2. In the row for the NA event rule, select **Edit**.
3. On the Edit Event Notification & Response Rule page, set the **Rule Status** to `Active`.

   > **NOTE:** Do not change any other settings in the event rule configuration.

4. Click **Save**.

Disable an NA Event Rule

To disable an NA event rule, follow these steps:

1. In the NA console, open the Event Notification & Response Rule page (**Admin > Event Notification & Response Rule**).
2. In the row for the NA event rule, select **Edit**.
3. On the Edit Event Notification & Response Rule page, set the **Rule Status** to `Inactive`.

   > **NOTE:** Do not change any other settings in the event rule configuration.

4. Click **Save**.

Example Scenarios for Getting the Most out of the HPE NNMi-HPE NA Integration

Many network management scenarios benefit from the use of the HPE NNMi–HPE NA integration for end-to-end network management. This chapter describes several scenarios that show the power of the integration. Some of these scenarios require one or more NNM iSPIs. "Table 4 Example Scenarios" below lists the example scenarios and the minimum license type for NNMi and NA to enable each scenario.

Table 4 Example Scenarios

Scenario	NNMi License Required	NA License Required
"Scenario 1: Identify and correct an out-of-compliance device change" on the next page	Premium	Ultimate
"Scenario 2: Troubleshoot network fault issues" on page 52	Premium	Premium
"Scenario 3: Verify traffic flow through the network after a device configuration change" on page 54	Ultimate	Premium
"Scenario 4: Re-address IPv4 addresses to the appropriate IPv6 addresses" on page 56	Premium	Premium
"Scenario 5: Troubleshoot application performance problems from a network context" on page 58	Ultimate	Premium
"Scenario 6: Use baseline data to identify abnormal system utilization" on page 61	Ultimate	Premium
"Scenario 7: Identify and correct error rate and utilization problems" on page 63	Premium	Premium

Scenario 1: Identify and correct an out-of-compliance device change

Incorrect device configuration is a common cause of network problems. The HPE NNMi–HPE NA integration can monitor the network for devices with non-compliant configurations and can generate notifications when a device configuration is outside of this expected configuration. The HPE NNMi–HPE NA integration provides tools for comparing the current device configuration to the previous device configuration and for resetting the device to use a previous configuration.

Process Without the HPE NNMi-HPE NA Integration

In this scenario, an unauthorized configuration change is made to a device. With no automated notification of the device configuration change, the network operator must determine that the device is misconfigured. This awareness usually happens only when a problem is encountered or when a manual configuration audit is performed. At this point, the network operator performs the following steps:

1. Locate the device and examine the change in the configuration management system.
2. Inspect the device configuration, comparing it against documented expectations, and determine that the configuration change is out of compliance.
3. Recreate or restore the good configuration to the device.
4. Verify that device is correctly configured.

Process with the HPE NNMi-HPE NA Integration

This scenario uses functionality from the following products:

- NNMi
- NA

Integration Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- "Configure the Device to Send syslog Messages to NA" on the next page.
- An NA device configuration policy must be applied to the device. The policy rule includes an auto-remediation script.
- Workflow approval is enabled in NA.
- The NNMi operator must have permission in NA to view and modify the device configuration.
- "Customize the NA SNMP Trap Incidents" on page 48.
- "Set NA to Run the Check Policy Compliance Task When a Device Configuration Changes" on page 49.
- "Configure NA to Send SNMP Traps to NNMi When a Policy Compliance Check Fails" on page 50.

Configure the Device to Send syslog Messages to NA

1. In the NA console, click **Tasks > New Task > Configure Syslog**.
2. On the New Task/Template – Configure Syslog page, do the following:
   a. Set *Applies to* to the device.
   b. Under Scheduling Options, set Recurring Options to Periodically, and then specify an appropriate interval.
   c. Click **Save**.

Customize the NA SNMP Trap Incidents

In the NNMi console, the NASnmpTrapv1 and NASnmpTrapv2 incident configurations convert the SNMP traps sent by NA into incidents that NNMi can display and process.

If you want all traps sent by NA to NNMi to appear in the key incident views in the NNMi console, set the NASnmpTrapv1 and NASnmpTrapv2 incident configurations to be root cause.

NOTE: This action sets all NA traps to be root cause regardless of content.

In the NNMi console, edit the NASnmpTrapv1 and NASnmpTrapv2 incident configurations to be root cause. This change sets all traps sent by the NA to NNMi to appear in the key incident views in the NNMi console.

Follow these steps:

1. In the NNMi console, in the Configuration workspace, click **Incidents > SNMP Trap Configurations**.
2. Edit each of the NASnmpTrapv1 and NASnmpTrapv2 incident configurations to select the **Root Cause** check box.

Set NA to Run the Check Policy Compliance Task When a Device Configuration Changes

In the NA console, on the Event Notification & Response Rules page, create a new rule that checks for policy compliance whenever a device's configuration changes.

1. In the NA console, click **Admin > Event Notification & Response Rules**.
2. On the Event Notification & Response Rules page, click the **New Event Notification & Response Rules** link at the top of the page.
3. On the New Event Notification & Response Rule page, do the following:
   a. Enter a rule name.
   b. Set *To take this action* to **Run Task**.
   c. Set *When the following events occur* to **Device Configuration Change**.
   d. Set *And then run this task* to **Check Policy Compliance**.
4. On the New Task/Template – Check Policy Compliance page, click **Done**.
5. On the Edit Event Notification & Response Rule page, click **Save**.

Configure NA to Send SNMP Traps to NNMi When a Policy Compliance Check Fails

In the NA console, on the Event Notification & Response Rules page, update the NA/NNMi Integration via SNMP Traps rule to send SNMP traps when policy non-compliance events occur.

1. In the NA console, click **Admin > Event Notification & Response Rules**.
2. On the Event Notification & Response Rules page, locate the NA/NNMi Integration via SNMP Traps rule, and then click the **Edit** link in this row.
3. On the Edit Event Notification & Response Rule page, do the following:
   a. In the *When the following events occur* list, verify that **Policy Non-Compliance** is selected.
   b. If necessary, **Ctrl-click** this row to add it to the selection list.
   c. Note the value set for SNMP Version, and change this value if appropriate.
   d. Click **Save**.

Integration Scenario Overview

After the scenario prerequisites are in place, the HPE NNMi–HPE NA integration can be used as follows:

1. NA receives a syslog event (or another change trigger), captures the new configuration, and automatically runs a compliance check on the new configuration.
2. NA sends an SNMP trap that describes the non-compliance to NNMi. NNMi displays this trap in the Open Key Incidents view.
3. From the NNMi incident, in the analysis pane, open the **Node Policy Compliance** tab to identify the policy for which the device configuration is out of compliance.
4. From the NNMi incident, in the analysis pane, open the **History of Node Configuration** tab, and then click **Compare to previous** for the most recent row to see a comparison of the current device configuration with the previous device configuration.
5. In the NA console, approve the auto-remediation task for the device.

   Alternatively, connect to the device and edit the device configuration.
6. NA runs the auto-remediation task and captures the new configuration. Then, NA automatically checks for compliance against the new configuration.

Benefits

In this scenario, the HPE NNMi–HPE NA integration provides the following benefits:

- More efficient operations.
- Automatic change detection.
- Automatic compliance checking.

- Configuration and compliance awareness in single incident view, which reduces MTTR.
- Increased security and service availability, which increases ROI.

Scenario 2: Troubleshoot network fault issues

When a device fault occurs, it is helpful to gather information about the device at the time of the fault. The HPE NNMi–HPE NA integration can query a device automatically and provides tools for responding to device fault incidents.

Process Without the HPE NNMi-HPE NA Integration

In this scenario, the ACL configuration on a router blocks traffic with a destination address of 224.0.0.5. Because OSPF depends on this address to broadcast hello packets, the router cannot establish adjacency with the neighboring router. With no automation, the network operator responds to a network fault incident with a thorough diagnostic procedure that includes connecting directly to the router to investigate and update the configuration. The process is similar to the following steps:

1. Categorize the network fault incident.
2. Log on to the router to run a diagnostic that identifies the cause of the incident.
3. On the router, update the configuration.
4. On the router, visually inspect the configuration to verify that it is correct.

Process with the HPE NNMi-HPE NA Integration

This scenario uses functionality from the following products:

- NNMi
- NA

Integration Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- The device must be configured to send traps to the NNMi management server.
- OSPF traps must be enabled on the device.
- The NNMi operator must have permission in NA to view and modify the device configuration.

Enable the OSPFNbrStateChange Incident

In the NNMi console, enable the OSPFNbrStateChange incident configuration and set this incident type to trigger an NA diagnostic.

1. In the NNMi console, in the Configuration workspace, click **Incidents > SNMP Trap Configurations**.
2. Open the OSPFNbrStateChange incident configuration.
3. Select the **Enabled** check box.
4. Save the configuration.

Integration Scenario Overview

After the scenario prerequisites are in place, the HPE NNMi–HPE NA integration can be used as follows:

1. NNMi determines that an OSPF neighbor state has changed and generates an OSPFNbrStateChange incident for that router. This incident triggers NA to gather information about the router.
2. NA runs a show neighbor device diagnostic to determine the OSPF neighbors of the router and then stores the task ID of the diagnostic as an attribute of the NNMi OSPFNbrStateChange incident.
3. From the NNMi incident, launch the NA console to view the diagnostic report of the OSPF neighbor router and observe the ACL configuration error.
4. In the NA console, modify the ACL of the OSPF neighbor router to permit hello packets.
5. *(NA Ultimate only)* To prevent this problem from recurring, create an NA device configuration policy that the problem ACL is not permitted on this device or any other relevant device. Violations of this policy are handled by "Scenario 1: Identify and correct an out-of-compliance device change" on page 46.

Benefits

In this scenario, the HPE NNMi–HPE NA integration provides the following benefits:

- Configuration data available at the point of need.
- More efficient operations.
- Reduced network downtime.
- Fewer network performance issues.
- Increased security and service availability, which increases ROI.

Scenario 3: Verify traffic flow through the network after a device configuration change

As part of completing an approved device configuration change, a network engineer wants proof that the change has the correct impact on application traffic. The HPE NNMi–HPE NA integration can display graphs of the traffic between two network devices. A network engineer can view these graphs before and after a device configuration change to validate the effectiveness of that change.

Process Without the HPE NNMi-HPE NA Integration

In this scenario, a network engineer plans to update a device's configuration with a change, such as which routing protocols the device can use, that is expected to improve the efficiency of the network in that area. With no network automation, the network engineer builds a statistical picture of network traffic flow over time. After changing the network in a way that impacts traffic flow, the network engineer again collects traffic flow information to verify that the change has not adversely affected network traffic. The process is similar to the following steps:

1. Over time, preferably at regular intervals, collect traffic flow data:
   a. Log on to a NetFlow exporter.
   b. On the NetFlow exporter, run commands (for example, `show`) to observe NetFlow statistics for the device to be changed.
   c. Record traffic statistics
   d. Repeat this step over time.
2. Change the network configuration in a way that impacts traffic routing.
3. Repeat the data gathering process.
4. To verify that traffic has reconverged after the network change, compare the traffic flow data from before and after the network change.

Process with the HPE NNMi-HPE NA Integration

This scenario uses functionality from the following products:

- NNMi
- NA
- NNM iSPI Performance for Traffic

Integration Scenario Prerequisites

- The devices must be in the NNMi topology.
- A flow protocol (for example, NetFlow, sFlow, ipfix, or jflow,) must be enabled on at least one device in the area of the network.

No additional configuration is needed to enable this scenario.

Integration Scenario Overview

After the scenario prerequisites are in place, the HPE NNMi–HPE NA integration can be used as follows:

1. In the NNMi console, open the traffic path view (**Actions > Traffic Maps > Traffic Path View**) representing the source and destination nodes for the traffic flow in the area of the network to be re-engineered.
2. Select the flow-enabled interface, and then, in the analysis pane, open the **Performance** tab.

   TIP: For comparison purposes, take a screen capture of the traffic graphs.

3. Change the network configuration in a way that impacts traffic routing.
4. To verify that traffic has reconverged after the network change, refresh the **Performance** tab to see the updated traffic graphs.

Benefits

In this scenario, the HPE NNMi–HPE NA integration provides the following benefits:

- Simplified process for collecting traffic flow data.
- No risk of transcription errors.
- Traffic flow visualization.

Scenario 4: Re-address IPv4 addresses to the appropriate IPv6 addresses

When completed manually, the process of re-addressing an IPv4 network to use IPv6 addresses is time-consuming and error prone. The HPE NNMi–HPE NA integration can automate both the collection of current IPv4 addresses in use and the setting of IPv6 addresses on managed devices.

Process Without the HPE NNMi-HPE NA Integration

In this scenario, a network engineer manually collects IPv4 information from each device and then manually configures each interface with an IPv6 address. The process is similar to the following steps:

1. Determine the current IPv4 addresses of each device:
   a. Log on to the device.
   b. Determine and record the IP address of each interface in a spreadsheet file.
2. In the spreadsheet file, map each IPv4 address to an IPv6 address.
3. Configure each device with IPv6 addresses:
   a. Log on to the device.
   b. Referring to the spreadsheet file, configure the correct IPv6 address on each interface.
   c. Visually inspect the configuration to verify that it is correct.

Process with the HPE NNMi-HPE NA Integration

This scenario uses functionality from the following products:

- NNMi
- NA

Integration Scenario Prerequisites

- The area of the network to be re-addressed must be in the NNMi topology and the NA inventory.
- Prepare a list of available IPv6 addresses.

Integration Scenario Overview

After the scenario prerequisites are in place, the HPE NNMi–HPE NA integration can be used as follows:

1. In the NNMi console, filter the IP Addresses inventory view to show only the area of the network to be re-addressed, and then export that list to comma-separated values (CSV) format.
2. With the CSV file open in a spreadsheet application, map each IPv4 address to an IPv6 address, and then save the spreadsheet file in CSV format.
3. Create a script that configures the new IPv6 addresses on the devices.
4. In the NA console, assign a scheduled task to run the script against the appropriate devices at the appropriate time.
5. In the NNMi console, export the IP Addresses inventory view to CSV format.
6. Compare the configured IPv6 addresses to the planned IPv6 addresses.

Benefits

In this scenario, the HPE NNMi–HPE NA integration provides the following benefits:

- Automation of the data collection and configuration processes.
- Reduced risk of re-addressing errors.

Scenario 5: Troubleshoot application performance problems from a network context

Unexpected network traffic across important network interfaces is a common cause of application performance problems. The HPE NNMi–HPE NA integration can monitor the utilization of important interfaces and can generate notifications when that utilization is beyond the acceptable level. The HPE NNMi–HPE NA integration provides tools for updating the device configuration to block unauthorized traffic on important interfaces.

Process Without the HPE NNMi-HPE NA Integration

In this scenario, unauthorized traffic consumes so much bandwidth across a network interface that the application using that interface experiences delayed response times. With no automated notification of the increased traffic, the network operator is usually unaware of the increased traffic until an application user submits a complaint against the application. At this point, the network operator performs the following steps:

1. Determine which communication paths and servers the application uses.
2. Run traceroute to determine the routed infrastructure for the application traffic.
3. Study each router in the routed infrastructure:
   a. Log on to the router.
   b. Examine the routing table to identify the interfaces associated with the application path.
   c. Gather performance metrics for the router as a whole and for the individual interfaces involved in the application path.
4. Gather traffic metrics from sniffer or probe tools deployed on the application path. Examine this data to determine which abnormal or unauthorized traffic is interfering with target application traffic across over-utilized routers.
5. Log on to the appropriate network devices to block unauthorized traffic or to reroute the application traffic through alternate, less utilized routes.

Process with the HPE NNMi-HPE NA Integration

This scenario uses functionality from the following products:

- NNMi
- NA
- NNM iSPI Performance for Metrics
- NNM iSPI Performance for Traffic

Integration Scenario Prerequisites

- The devices must be in the NNMi topology and the NA inventory.
- Performance monitoring and interface utilization thresholds must be enabled and configured in NNMi for the interfaces.
- A flow protocol (for example, NetFlow, sFlow, ipfix, or jflow,) must be enabled on at least one device in the area of the network.
- "Enable the InterfaceInputUtilizationHigh and InterfaceInputUtilizationLow Incidents" on the next page.

Enable the InterfaceInputUtilizationHigh and InterfaceInputUtilizationLow Incidents

In the NNMi console, enable the InterfaceInputUtilizationHigh and InterfaceInputUtilizationLow incident configurations.

1. In the NNMi console, in the Configuration workspace, click **Incidents > Management Event Configurations**.
2. Open the InterfaceInputUtilizationHigh incident configuration.
3. Select the **Enabled** check box.
4. Save the configuration.
5. Repeat "Open the InterfaceInputUtilizationHigh incident configuration." above through "Save the configuration." above for the InterfaceInputUtilizationLow incident configuration.

Integration Scenario Overview

After the scenario prerequisites are in place, the HPE NNMi–HPE NA integration can be used as follows:

1. NNMi generates a management event incident to indicate that interface utilization is beyond acceptable boundaries for an important network interface.
2. In the traffic inventory, locate the source interface of the NNMi incident and, in the analysis pane, view the **Top Apps-In** tab.

   This tab displays a pie chart of the applications generating the most traffic. The chart reveals competing traffic from an unauthorized application.
3. From the NNMi incident, launch the NA console to the device details page. (Use **View HPE NA Device Information**.)
4. From the device details page in the NA console, run a Batch Insert ACL Line task to modify multiple ACLs to multiple devices to block unauthorized traffic.
5. Network traffic across the interface returns to acceptable levels, and the interface utilization incident automatically closes in the NNMi console.

Benefits

In this scenario, the HPE NNMi–HPE NA integration provides the following benefits:

- Proactive management of network utilization issues for increased service levels on mission critical applications.
- One set of tools for detecting, troubleshooting, and fixing the cause of network utilization issues, which reduces MTTR.
- Proactive remediation of network configuration issues that affect critical services across the entire network.

- Automated collection of performance and traffic data.
- Detection and blocking of unauthorized traffic.

Scenario 6: Use baseline data to identify abnormal system utilization

Irregular traffic patterns can signal inappropriate use of the network. The HPE NNMi–HPE NA integration can determine normal traffic patterns and can generate notifications when traffic patterns are outside the normal range.

Process Without the HPE NNMi-HPE NA Integration

In this scenario, company customers complain about the slowness in accessing the company's main web site across the Internet. At this point, the network operator performs the following steps:

1. Examine the network utilization of the web servers and the outside router to observe high utilization.
2. Use sniffers, run performance tools, and examine firewall logs to determine the source of the slowness.
3. Determine that the web site URL is being loaded with many HTTP requests. The requests seem to be an attack on the web site.
4. Close all connections to the web site, which brings the web site completely down.
5. Contact security specialists for assistance with the situation.

Process with the HPE NNMi-HPE NA Integration

This scenario uses functionality from the following products:

- NNMi
- NA
- NNM iSPI Performance for Metrics
- NNM iSPI Performance for Traffic

Integration Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- An NNM iSPI Performance for Traffic site must be defined for the IP addresses of the web site locations.

Integration Scenario Overview

After the scenario prerequisites are in place, the HPE NNMi–HPE NA integration can be used as follows:

1. NNMi generates a management event incident to indicate a deviation from normal behavior with regards to utilization on the interfaces involved in the path to the web site.
2. NNM iSPI Performance for Traffic generates a management incident to indicate a high volume of HTTP traffic toward an NNM iSPI Performance for Traffic site that represents the web site locations.
3. From the NNM iSPI Performance for Traffic incident, in the analysis pane, open the **Top Apps - In** tab for the interface identified in the incident.

   This tab displays a pie chart of the applications generating the most traffic.
4. From the Traffic Reporting Interfaces table in the Traffic Analysis workspace, double-click the interface mentioned in the NNM iSPI Performance for Traffic incident.

The **Top 5 Sources** and **Top 5 Destinations** tabs show that the high interface utilization comes from a few hosts.

5. Determine that the web site URL is being loaded with many HTTP requests. The requests seem to be an attack on the web site.
6. From the NNMi incident, launch the NA console to the device details page. (Use **View HPE NA Device Information**.)
7. From the device details page in the NA console, run a Batch Insert ACL Line task to modify the ACLs on the device hosting the web server to deny traffic from the sources of the attack.
8. Network traffic across the interface returns to acceptable levels, and the interface utilization incident automatically closes in the NNMi console.

Benefits

In this scenario, the HPE NNMi–HPE NA integration provides the following benefits:

- Proactive management of network utilization issues for increased customer satisfaction.
- One set of tools for detecting, troubleshooting, and fixing the cause of network utilization issues, which reduces MTTR.
- Detection and blocking of unauthorized traffic.
- High quality service delivery.

Scenario 7: Identify and correct error rate and utilization problems

A high error rate on an interface usually causes the workstation, server, or any other device connected to that interface to work significantly slower. The HPE NNMi–HPE NA integration can monitor interfaces and generate notifications when the error rate, or utilization, or both crosses pre-defined thresholds.

Process Without the HPE NNMi-HPE NA Integration

In this scenario, a critical application responds slowly and eventually times out, but the problem clears on its own. Because this failure happens intermittently during peak usage periods, the application is moved to a more powerful server. This change does not prevent the application from timing out. Eventually a duplex mismatch is discovered. Correcting the duplex configuration resolves the timeout issue.

Process with the HPE NNMi-HPE NA Integration

This scenario uses functionality from the following products:

- NNMi
- NA
- NNM iSPI Performance for Metrics

Integration Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- Performance monitoring and thresholds must be enabled and configured in NNMi for the interface.
- "Enable the InterfaceInputErrorRateHigh and InterfaceInputUtilizationHigh Incidents" on the next page.

Enable the InterfaceInputErrorRateHigh and InterfaceInputUtilizationHigh Incidents

In the NNMi console, enable the InterfaceInputErrorRateHigh and InterfaceInputUtilizationHigh incident configurations.

1. In the NNMi console, in the Configuration workspace, click **Incidents > Management Event Configurations**.
2. Open the InterfaceInputErrorRateHigh incident configuration.
3. Select the **Enabled** check box.
4. Save the configuration.
5. Repeat "Open the InterfaceInputErrorRateHigh incident configuration." above through "Save the configuration." above for the InterfaceInputUtilizationHigh incident configuration.

Integration Scenario Overview

After the scenario prerequisites are in place, the HPE NNMi–HPE NA integration can be used as follows:

1. NNMi generates a management event incident to indicate a high error rate on an interface. The connection table on the incident details tab indicates a duplex mismatch.
2. In the NNMi console, open the node details page for the router on each end of the connection. In each analysis pane, open the **History of Node Configuration** tab, and then click **Compare to previous** for the most recent row to see a comparison of the current device configuration with the previous device configuration. Observe which duplex is configured on this interface and whether that configuration has been changed recently.
3. Open an NNM iSPI Performance for Metrics interface health report for the LAN collision rate and LAN collision count metrics grouped by qualified interface name. Also open an NNM iSPI Performance for Metrics interface health report for the LAN FCS error rate and LAN FCS error count metrics grouped by qualified interface name.

   This combination of reports shows one side of the connection with high errors while the other side has high collisions. This information is indicative of duplex mismatch.
4. From the NNMi incident, launch the NA console and update the switch configuration.
5. Check the interface performance history in the NNM iSPI Performance for Metrics reports to verify that the error problem no longer occurs.

Benefits

In this scenario, the HPE NNMi–HPE NA integration provides the following benefits:

- Proactive detection of network configuration errors before they impact application performance.
- One set of tools for detecting, troubleshooting, and fixing the cause of network utilization issues, which reduces MTTR.

Administering the HPE NNMi-HPE NA Integration

This chapter contains information about administering the HPE NNMi–HPE NA integration. It includes the following topics:

- "Changing the HPE NNMi–HPE NA Integration" below
- "Disabling the HPE NNMi–HPE NA Integration" below
- "Troubleshooting the HPE NNMi–HPE NA Integration" on the next page
- "Application Failover and the HPE NNMi–HPE NA Integration" on page 68

Changing the HPE NNMi-HPE NA Integration

1. In the NA console, open the **Administrative Settings - NA/NNMi Integration** page (**Admin > Administrative Settings > NA/NNMi Integration**).
   a. Modify the values as appropriate. For information about the fields on this form, see the following references:
      - "Triggering NNMi Node Config Polls from NA" on page 39
      - "Disabling Network Management During Device Configuration" on page 40

   b. Click **Save** at the bottom of the page.
2. *Optional*. In the NA console, modify the *NA/NNMi Integration using SNMP Traps (NNMi Server)* and *NA/NNMi Integration SNMP Community String Propagate* event rules as described in the following references:
   - "Sending SNMP Traps to NNMi" on page 38
   - "Propagating Device Community String Changes to NA" on page 41
3. In the NNMi console, open the **HPE NNMi–HPE NA Integration Configuration** form (**Integration Module Configuration > HPE NA**).
   a. Modify the values as appropriate. For information about the fields on this form, see "HPE NNMi–HPE NA Integration Configuration Form Reference" on page 69.

   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.

Disabling the HPE NNMi-HPE NA Integration

1. In the NNMi console, open the **HPE NNMi–HPE NA Integration Configuration** form (**Integration Module Configuration > HPE 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.
3. Optional. If you do not plan to re-enable the integration in the future, in the NA console, delete the NA/NNMi event rules from the **Event Notification & Response Rules** page (**Admin > Event Notification & Response Rules**).

Troubleshooting the HPE NNMi-HPE NA Integration

This section contains the following topics:

- "Test the Integration" below
- "NA Devices are Missing from the NNMi Inventory" on page 68

Test the Integration

> **NOTE:** 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 "HPE NNMi–HPE NA Integration Configuration Form Reference" on page 69, before walking through this entire procedure.

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

   For information about the fields on this form, see "HPE NNMi–HPE NA Integration Configuration Form Reference" on page 69.

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

   > **TIP:** When successful, this step initiates a complete inventory synchronization between NNMi and NA.

   A new window displays a status message.

   If the message indicates a problem with connecting to the NA core server, NNMi and NA are not able to communicate. Continue with the next step.

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

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

4. To verify that the connection to the NA core 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 **HPE NNMi–HPE 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 core server responds with a message similar to:

   ```
   NAS SOAP API: Only handles HTTP POST requests
   ```

   - If the expected message appears, continue with "Verify that the connection to NNMi is configured correctly:" on the next page.

- If you see an error message, the connection to the NA core 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 NA until you see the expected message.

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

   > **NOTE:** If you used the information described in this step to connect to the NNMi console in the 1st step of this procedure, you do not need to reconnect to the NNMi console. Continue with the next step.

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

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

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

      - If the **NNMi SSL Enabled** check box is selected, `<protocol>` is `https`.
      - If the **NNMi SSL Enabled** check box is cleared, `<protocol>` is `http`.
      - `<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 NNMi. Continue to troubleshoot the connection to NNMi until the NNMi console appears.

      > **NOTE:** 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 **HPE NNMi–HPE 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 "Contact the NNMi administrator to verify the values of the NNMi User with the Web Service Client role and the corresponding NNMi Password." above on this form.

   For more information, see "HPE NNMi–HPE NA Integration Configuration Form Reference" on page 69.
8. Click **Submit** at the bottom of the form.
9. If the status message still indicates a problem with connecting to the NA core 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 HPE NNMi–HPE NA Integration" on page 28.

NA Devices are Missing from the NNMi Inventory

NOTE: The information in this section applies only when both of the following conditions are met:

- Only one NNMi management server integrates with NA.
- The *NA/NNMi Topology Synchronization for Device Addition* event rule is enabled.

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

1. Examine the NNMi node inventory to determine whether the device is in the inventory 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 NNMi.

   If the IP address is included in NNMi, determine which node hosts the IP address. This node should be synchronized with the NA device. NNMi might be using a different management address for this node than the IP address that NA sent as a discovery hint.
3. Modify the NNMi auto-discovery rules to include those devices that are in the NA inventory, but not in the NNMi inventory. Then re-enable the integration.

   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 NA during a network outage or before the NNMi auto-discovery rules were correctly included, re-enable the integration to cause NA to re-send the discovery hint.

Application Failover and the HPE NNMi-HPE NA Integration

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

The integration does not support failover of the NA core. If the integrated NA core fails over to a different NA core, update the **HPE NNMi–HPE NA Integration Configuration** form on each NNMi management server with the information for connecting to the new NA core.

HPE NNMi-HPE NA Integration Reference

This chapter contains reference information for the HPE NNMi–HPE NA integration. It includes the following topics:

- "Ports Used By the HPE NNMi–HPE NA Integration" below
- "HPE NNMi–HPE NA Integration Configuration Form Reference" below
- "Configuration Parameters in the NA Console" on page 74

Ports Used By the HPE NNMi-HPE NA Integration

On the NNMi management server, the HPE NNMi–HPE NA integration uses the following ports:

- Port for receiving calls to the NNMi web services, which is 80 (non-SSL) or 443 (SSL) by default
- Port 162 for receiving SNMP traps from NA

On the NA core server, the HPE NNMi–HPE NA integration uses the following port for receiving calls to the NA web services:

- If NA is on a separate computer from NNMi, this port is 80 (non-SSL) or 443 (SSL).
- If NA is on the same computer as NNMi, this port is 8080 (non-SSL) or 8443 (SSL).

HPE NNMi-HPE NA Integration Configuration Form Reference

In the NNMi console, the **HPE NNMi–HPE NA Integration Configuration** form contains the parameters for configuring communications from NNMi to NA. The form is available from the **Integration Module Configuration** workspace. The communication parameters on this form populate a row of the Integration Server List on the NA/NNMi Integration page in the NA console.

NOTE: Only NNMi users with the Administrator role can access the **HPE NNMi–HPE NA Integration Configuration** form.

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

- "NNMi Management Server Connection" below
- "NA Core Server Connection" on the next page
- "Integration Behavior" on page 71
- "Configuring NNMi User Access to NA Information in the NNMi Analysis Pane" on page 73

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

NNMi Management Server Connection

"Table 5 NNMi Management Server Information in the NNMi Console" on the next page lists the parameters for connecting to the NNMi management server from 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 5 NNMi Management Server Information in the NNMi Console

Field	Description
NNMi SSL NA SSL	For SSL communication, verify that you exchanged certificates in step 2 before selecting either of these check boxes.
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` • *Linux*: `$NnmDataDir/conf/nnm/props/nms-local.properties`
NNMi User	The user name for connecting to the NNMi web services. 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 Core Server Connection

"Table 6 NA Core Server Information in the NNMi Console" below lists the parameters for connecting to the web services on the NA core server. Coordinate with the NA administrator to determine the appropriate values for this section of the configuration form.

Table 6 NA Core Server Information in the NNMi Console

NA Core Server Parameter	Description
NNMi SSL NA SSL	For SSL communication, verify that you exchanged certificates in step 2 before selecting either of these check boxes.
NA Host	The fully-qualified domain name or the IP address of the NA core server.
NA Port	The port for connecting to the NA web services. The default NA ports are as follows: • 443—for SSL connections to NA on a separate computer from NNMi • 8443—for SSL connections to NA on the same computer as NNMi • 80—for non-SSL connections to NA on a separate computer from NNMi • 8080—for non-SSL connections to NA on the same computer as NNMi
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 7 Integration Behavior Information in the NNMi Console" below lists the NNMi console parameters for configuring the behavior of the HPE NNMi–HPE NA integration.

Table 7 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 inventory. 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. The default selection is the Networking Infrastructure Devices node group. If no node group is specified, the integration synchronizes the entire NNMi inventory into the NA inventory.
Topology Synchronization Interval (hrs)	The frequency with which NNMi performs a complete inventory synchronization with NA as described in "Inventory Synchronization Between NNMi and NA" on page 28. The default interval for the connection check is 24 hours. To disable periodic inventory synchronization, set this value to `0`.
Discover Device Drivers in NA	The NA configuration specification. If the **Discover Device Drivers in NA** check box is selected, NA automatically discovers the device drivers for the devices added to NA as a result of inventory synchronization with NNMi. The default setting is selected. When the **Discover Device Drivers in NA** check box is cleared, you can initiate device driver discovery manually. If the NA inventory already contains the NNMi inventory, the integration does not need to discover device drivers again.
Map NNMi Security Groups to NA Partitions	If the **Map NNMi Security Groups to NA Partitions** check box is selected, a device synchronized from NNMi to NA is always added or updated to an NA partition of the same name as the NNMi security group that contains the node. If the **Map NNMi Security Groups to NA Partitions** check box is not selected (the default), the NNMi nodes not currently in the NA inventory are added the NA Default Site partition and NNMi nodes currently in the NA inventory remain in the partition assigned in NA. If the **Topology Filter Node Group** field specifies a node group, it is possible that only some nodes in each NNMi security group are synchronized to the corresponding NA partition. To synchronize the entire NNMi inventory to the NA inventory, clear the **Topology Filter Node Group** field.
NA Connection Check Interval (hrs)	The frequency with which NNMi verifies with 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 33. The default interval for the connection check is 24 hours. To disable the periodic connection check, set this value to `0`.

Table 7 Integration Behavior Information in the NNMi Console, continued

Parameter	Description
Minimum NNMi Role for Analysis Pane Data	The NNMi access level for viewing NA information in the NNMi analysis pane. The available options for the **Minimum NNMi Role for Analysis Pane Data** field are as follows: • Disable Feature: Disables 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, or Administrator role. • NNMi Guest Users: Shows NA data in the NNMi analysis pane to all NNMi users. For more information, see "Configuring NNMi User Access to NA Information in the NNMi Analysis Pane" on the next page.
Minimum Object Access Privilege for Analysis Pane Data	The NNMi object access level for viewing NA information in the NNMi analysis pane. The available options for the **Minimum Object Access Privilege for Analysis Pane Data** field are as follows: • Object Administrator: Shows NA data in the NNMi analysis pane to NNMi users having the Object Administrator privilege for the NNMi node. • Object Operator Level 2: Shows NA data in the NNMi analysis pane to NNMi users having the Object Operator Level 2 or Object Administrator privilege for the NNMi node. • Object Operator Level 1: Shows NA data in the NNMi analysis pane to NNMi users having the Object Operator Level 1, Object Operator Level 2, or Object Administrator privilege for the NNMi node. • Object Guest: For all NNMi nodes, shows NA data in the NNMi analysis pane to all NNMi users who pass the minimum role filter. If security groups are not configured in NNMi, select this option. For more information, see "Configuring NNMi User Access to NA Information in the NNMi Analysis Pane" on the next page.
Activate/Deactivate Device in NA	If you select this option, the integration controls the management status of the devices in NA. That is: • When a node is re-seeded in NNMi, the integration manages the corresponding device in NA. • When a synchronized node is deleted from NNMi , the integration stops managing the corresponding device in NA. If you clear this option, , the integration does not control the management status of the devices in NA. That is: • When a synchronized node is deleted from NNMi, the integration does not unmanage the corresponding device in NA.

Table 7 Integration Behavior Information in the NNMi Console, continued

Parameter	Description
	• When a synchronized node is re-seeded in NNMi, the integration does not activate the corresponding device in NA. This option is selected by default.

Configuring NNMi User Access to NA Information in the NNMi Analysis Pane

For NNMi nodes that are synchronized with the NA inventory, the NNMi administrator can restrict NNMi user access to NA information about these nodes in the NNMi analysis pane. This restriction is accomplished using both of the following fields on the **HPE NNMi–HPE NA Integration Configuration** form:

- **Minimum NNMi Role for Analysis Pane Data**
- **Minimum Object Access Privilege for Analysis Pane Data**

An NNMi user must meet both the minimum role and the minimum object access privilege for an NNMi node to view NA information in the NNMi analysis pane.

- To permit all NNMi users to see all NA information in the analysis pane for all NNMi nodes, set the **Minimum NNMi Role for Analysis Pane Data** field to `Disable Feature`. This setting makes the **Minimum Object Access Privilege for Analysis Pane Data** field unavailable.
- To control access only by NNMi role, do the following:
  - Set the **Minimum NNMi Role for Analysis Pane Data** field to one of the limiting options (`NNMi Administrators`, `NNMi Level 2 Operators`, or `NNMi Level 1 Operators`).
  - Set the **Minimum Object Access Privilege for Analysis Pane Data** field to `Object Guest`.
- To control access by object access privilege only, do the following:
  - Set the **Minimum NNMi Role for Analysis Pane Data** field to `NNMi Guest Users`.
  - Set the **Minimum Object Access Privilege for Analysis Pane Data** field to one of the limiting options (`Object Administrator`, `Object Operator Level 2`, or `Object Operator Level 1`).
- To control access by both NNMi role and object access privilege, do the following:
  - Set the **Minimum NNMi Role for Analysis Pane Data** field to one of the limiting options (`NNMi Administrators`, `NNMi Level 2 Operators`, or `NNMi Level 1 Operators`).
  - Set the **Minimum Object Access Privilege for Analysis Pane Data** field to one of the limiting options (`Object Administrator`, `Object Operator Level 2`, or `Object Operator Level 1`).

    For example, consider the following integration configuration:

    - The **Minimum NNMi Role for Analysis Pane Data** is `NNMi Level 2 Operators`.
    - The **Minimum Object Access Privilege for Analysis Pane Data** is `Object Operator Level 1`.

    For a given node, Node1, that is synchronized through the HPE NNMi–HPE NA integration, the following NNMi users can view NA information in the analysis pane for Node1 and for the interfaces of Node1:

- All NNMi users having the Administrator role. The integration ignores the object access privilege for these users.
- For NNMi users having the Operator Level 2 role, only those users who have the Object Administrator, Object Operator Level 2, or Object Operator Level 1 privilege on Node1.

The following NNMi users do *not* see NA information in the analysis page for Node1 or for the interfaces of Node1:

- For NNMi users having the Operator Level 2 role, those users who have the Object Guest privilege on Node1.
- All NNMi users having the Operator Level 1 role or the Guest role.

"Table 8 Example: Ability to View NA Information in the Analysis Pane for Node1" below presents this information visually.

Table 8 Example: Ability to View NA Information in the Analysis Pane for Node1

NNMi Object Access Privilege	**NNMi Role**			
	Administrator	**Operator Level 2**	**Operator Level 1**	**Guest**
Object Administrator	✓	✓		
Object Operator Level 2	✓	✓		
Object Operator Level 1	✓	✓		
Object Guest	✓			

For information about assigning NNMi roles and node object access levels to NNMi users, see the following information:

- “Configuring Security” in the NNMi help
- “NNMi Security and Multi-Tenancy” in the NNMi Deployment Reference

Configuration Parameters in the NA Console

In the NA console, the **Administrative Settings - NA/NNMi Integration** page contains the parameters for configuring communications from NA to NNMi. Access this page to change the integration behavior for NNMi out-of-service triggers and device rediscovery (configuration poll) triggers.

The **Administrative Settings - NA/NNMi Integration** page is available from **Admin > Administrative Settings > NA/NNMi Integration**. To apply changes to the integration configuration, update the values on this page, and then click **Save**.

NOTE: Only NA users with the Administrator role can access the **Administrative Settings - NA/NNMi Integration** page.

Integration Communication

"Table 9 Integration Server List Columns in the NA Console" on the next page lists the columns in the Integration Server List on the **Administrative Settings - NA/NNMi Integration** page. Each row in the table describes the connection between NA and one NNMi management server. The integration populates a row with the information from the **HPE NNMi–HPE NA Integration Configuration** form in the NNMi console.

Table 9 Integration Server List Columns in the NA Console

Field	Description
Integration Enabled	The status of the integration with the NNMi management server identified in the NNMi Server column.
NNMi Server	The official fully-qualified domain name of the NNMi management server.
NNMi System ID	The unique identifier of the NNMi management server.
NNMi Protocol	The protocol for connecting to the NNMi web services.
NNMi Port	The port for connecting to the NNMi web services.
NNMi User	The user name for connecting to the NNMi web services.
NA User	A valid NA user account name with the NA Administrator role.

Additional Integration Behavior

"Table 10 Integration Behavior Information in the NA Console" below lists the NA console parameters for configuring the behavior of the HPE NNMi–HPE NA integration.

Table 10 Integration Behavior Information in the NA Console

Field	Description
Tasks That Place Device Out-of-Service	The NA tasks that request NNMi to place the device out-of-service. NNMi does not generate incidents for out-of-service devices. After the task completes, the integration waits for the time shown in the Out-of-Service Completion Delay field and then requests NNMi to resume managing the device. 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 To disable this feature, clear all selections from the task list. For more information, see "Disabling Network Management During Device Configuration" on page 40.
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 NNMi.
If device compliance check fails	The device compliance check failure recovery specification for out-of-service events. The default setting is to return the device to service in NNMi. **NOTE:** The device compliance check is only available for the NA Ultimate license.

Table 10 Integration Behavior Information in the NA Console, continued

Field	Description
Out-of-Service Completion Delay	The time (in minutes) that the integration waits between completion of a task that placed a device out-of-service and restoring the NNMi device management mode. This delay provides time for devices to recover after NA completes the task. The default value is 10 minutes. The maximum value is 1440 minutes (24 hours). To change the maximum value, add the `nnm/integration/max_out_of_service_delay` option to the NA `adjustable_options.rcx` file.
Tasks That Request NNMi Config Poll	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 "Triggering NNMi Node Config Polls from NA" on page 39.

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 HPE Network Node Manager i Software—HPE Network Automation Integration Guide (Network Node Manager i Software 10.21)

Just add your feedback to the email and click send.

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

We appreciate your feedback!

Glossary

A

AES

Advanced Encryption Standard

Anycast Rendezvous Point IP Address

Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

Autonomous System

An Autonomous System (AS) is a collection of connected Internet Protocol (IP) routing prefixes that present a common, clearly defined Border Gateway Protocol (BPG) routing policy to the Internet by having an officially registered Autonomous System Number (ASN).

B

BGP

Border Gateway Protocol

C

Causal Engine

The NNMi Causal Engine analyzes the health of your network and provides the ongoing health status reading for each device. The Causal Engine also extensively evaluates problems and determines the root cause for you, whenever possible, sending incidents to notify you of problems. Any incident generated from a Causal Engine management event has an Origin of NNMi in your incident views.

CBC

Cipher Block Chaining

CE

Customer Edge router. The router in your network that sends data to an Internet Service Provider's router (the Provider Edge) on the path to the data's final desination.

CRC

Cyclic Redundancy Check

Custom Node Collection

A Custom Node Collection identifies a topology node that has at least one associated Custom Poller Policy. Because a topology node can be associated with more than one Policy, the same topology node might appear in multiple Custom Node Collections.

Custom Polled Instance

A Custom Polled Instance represents the results of a MIB variable when it is evaluated against a node. The first time a MIB variable is validated with discovery information, the results appear in the Monitoring workspace's Custom Polled Instances view. The Custom Polled Instance is updated whenever a change in State occurs and includes the most recent polled value that caused the State to change. These results are then used to determine the Status of the associated Custom Node Collection.

Custom User Groups

Custom User Groups are the User Groups that you create. These User Groups are additional to the NNMi User Groups, which are those User Groups that NNMi provides.

D

DES

Data Encryption Standard

E

EIGRP

Enhanced Interior Gateway Routing Protocol

EVPN

Ethernet Virtual Private Network.

G

global unicast address

(2000:: to 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff) A publically routable IPv6 unicast address, used for communication between nodes anywhere on the internet. The first part of the address is a global routing prefix in the 2000::/3 address space for your organization (assigned by the Internet Service Providers). The complete host address can either be manually configured or automatically assigned using IPv6 auto-configuration and neighbor discovery.

H

HMAC

Hash-based Message Authentication Code

hops

A hop is a node representing any network device, such as a workstation, gateway, or switch, which is connected by a link with no intermediate nodes.

HSRP
Hot Standby Router Protocol

hypervisor
The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.

I

IPv6 link-local address
A non-routable IPv6 unicast address only used for communication with other nodes on the same link (LAN or VLAN). Link local addresses cannot be used for communication that must be forwarded through a router. IPv6 auto-configuration automatically assigns a unique link local address in the fe80::/10 address space to each IPv6-enabled interface on a system.

ISIS
Intermediate System to Intermediate System Protocol

J

Jython
Jython is a programming language (successor of JPython) uses Java class, instead of Python modules.

K

Key Incident
Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

L

Layer 2
Refers to the Data Link layer of the multilayered communication model, Open Systems Interconnection (OSI). The Data Link layer moves data across the physical links in the network. The switches and switch-routers are devices that redirect data messages at the layer 2 level, using the destination Media Access Control (MAC) address to determine where to direct the message.

Layer 3
Refers to the Network layer of the multilayered communication model, Open Systems Interconnection (OSI). The Network layer is concerned with knowing the address of the neighboring nodes in the network, selecting routes and quality of service, and recognizing and forwarding incoming messages to

local host domains. The router and switch-router are the devices that redirect data messages at the Layer 3 level. Everything in a subnet is connected at the Layer 3 (IP) level.

Link Aggregation

Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface).

loopback address

The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using ifType Number 24, softwareloopback from the IANA ifType-MIB.

M

MAC address

The Media Access Control address (hardware address or physical address) that the factory burns into a network adapter or device with built-in networking capability. A MAC address has six pairs of hexadecimal digits, separated by colons or dashes. For example 02:1F:33:16:BC:55

MAC addresses

The Media Access Control address (hardware address or physical address) that the factory burns into a network adapter or device with built-in networking capability. A MAC address has six pairs of hexadecimal digits, separated by colons or dashes. For example 02:1F:33:16:BC:55

MD5

Message-Digest algorithm 5

MIB file

Management Information Base files are the basic building block of SNMP communication protocol. SNMP Agents are configured to respond to requests defined by a group of supported MIB files.

MPLS

Multiprotocol Label Switching

multicast address

Used to identify a group of hosts joined into a group. IPv4 multicast addresses are in the range 224.0.0.0 to 239.255.255.255 and IPv6 multicast addresses have the prefix ff00::/8.

multiconnection

A multiconnection is a thick line on a map view between two Node icons, two Node Group icons, or between a Node icon and a Node Group icon (with no Interface icon or IP Address icon at either end of the line). This thick line represents a set of multiple connections that have been combined to preserve space and simplify the map. Your NNMi administrator specifies the number of connections that must exist before NNMi condenses them into a multiconnection line (User Interface Configuration's Multiconnection Threshold attribute). Double-click the thick line to convert it into the original set of connections with Interface icons or IP Address icons at either end of the lines.

N

NAT

Network Address Translation. NNMi supports the following protocols: Static Network Address Translation, Dynamic Network Address Translation, Dynamic Port Address Translation.

NIC

Network Interface Controller

NNMi Role

Determined by your membership in one of four special NNMi User Groups (NNMi Administrators, NNMi Level 2 Operators, NNMi Level 1 Operators, or NNMi Guest Users). This membership determines what you can see and do within the NNMi console.

NNMi User Group

NNMi User Groups are those User Groups provided by NNMi. Users cannot access the NNMi console until their User Account is mapped to at least one of the following NNMi User Groups: NNMi Administrators, NNMi Level 2 Operators, NNMi Level 1 Operators (with more limited access privileges than Level 2 Operators), and NNMi Guest Users

Node

A physical or virtual collection of network interfaces that NNMi can pragmatically associate together.

O

OSPF

Open Shortest Path First Protocol

P

PE

Provider Edge router. The Internet Service Provider's router that receives your data on the path to your data's final desination. The Customer Edge (CE) router in your network connects to this PE.

private IP addresses

These are IPv4 addresses that can be reused in home and office local area networks (LANs). Following the standards set by RFC 1918 and RFC 4193 (10.*.*.*, 169.254.*.*, 172.16-31.*.*, and 192.168.*.*)

R

RAMS

HP Router Analytics Management System

routing prefixes

A network protocol technique used to shorten or filter the amount of required routing information in each packet by declaring a prefix for an entire group of packets. This prefix also indicated the number of bits in the address.

S

SHA

Secure Hash Algorithm

SNMP

Simple Network Management Protocol

SNMP Agent

Simple Network Management Protocol (SNMP) is an Internet-standard protocol used to manage devices on IP networks. The SNMP Agent uses this protocol to report information to authorized management programs.

SOAP

Simple Object Access Protocol

Split Link Aggregation

Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

U

unique local address

(fd00:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff) A privately routable IPv6 unicast address used only for communication between nodes within your organization. The unique local addresses cannot be routed to the public internet. The address consists of a routing prefix in the fd00:/8 address spaces, assigned locally by your organization. And the full host address might be manually configured or automatically assigned using IPv6 auto-configuration and neighbor discovery.

Unmanaged

Indicates the Management Mode is "Not Managed" or "Out of Service".

USM

User-based Security Model

UUID

Universally Unique Object Identifier, which is unique across all databases.

V

virtual machine

A device that utilizes components from multiple physical devices. Depending on the manufacture's implementation, the virtual machine may be static or dynamic.

VMware

VMware ESX and VMware ESXi software uses SOAP protocol to implement bare-metal hypervisors.

VRRP

Virtual Router Redundancy Protocol

W

WAN Cloud

Layer 3 connectivity between your network and any MPLS networks.

Web Agent

The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.