Hewlett Packard
Enterprise

HPE Network Node Manager i Software

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

HPE Network Node Manager i Software–HPE Business Service Management/Universal CMDB Topology 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**

HPE Software Integrations, Solutions and Best Practices

Visit the Integrations and Solutions Catalog at https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710 to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

Visit the Cross Portfolio Best Practices Library at **https://hpln.hpe.com/group/best-practices-hpsw** to access a wide variety of best practice documents and materials.

Contents

Integrate NNMi with BSM/OMi

The HPE Business Service Management (BSM) platform provides tools for managing the availability of applications in production, monitoring system performance, monitoring infrastructure performance, and proactively resolving problems when they arise.

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

You can also use the instructions provided in this guide to integrate NNMi with HPE Operations Manager i (OMi).

This chapter introduces the available integrations between NNMi and BSM/OMi. It contains the following topics:

- "Comparison of Approaches to Integrating NNMi with HPE BSM Operations Management or OMi" below
- "HPE NNMi–HPE BSM Operations Management Integration" on page 10
- "NNMi Integrated with HPOM Integrated with HPE BSM Operations Management" on page 11
- "NNMiVisualizations in BSM" on page 12

Comparison of Approaches to Integrating NNMi with HPE BSM Operations Management or OMi

"Table 1 Comparison of NNMi Integrations with BSM Operations Management/OMi and HPOM" below compares the HPE NNMi—HPE BSM Operations Management with the HPE NNMi—HPOM integration.

See "HPE NNMi–HPE BSM Operations Management Integration" on page 10 for information about integrating NNMi with BSM Operations Management.

See the *HP Network Node Manager i Software—HP Operations Manager Integration Guide* for information about integrating NNMi with HPOM.

Table 1 Comparison of NNMi Integrations with BSM Operations Management/OMi and HPOM

Comparison Item	Direct Integration with the BSM Connector	Indirect Integration Through HPOM
Instruction text	Events cannot contain instructional text. To make instructional text available, create a	Events can contain instruction text.

Table 1 Comparison of NNMi Integrations with BSM Operations Management/OMi and HPOM, continued

Comparison Item	Direct Integration with the BSM Connector	Indirect Integration Through HPOM
	tool to launch user-defined instructions as a URL. (You would need to create external documentation for this tool.) If BSM is installed with the Monitoring Automation component, you can do the following: 1. Make sure the SNMP trap policy for which you want to view trap conditions contains help text. 2. Import the SNMP trap policy using either of the following commands: Windows: • <*BSM_Root_Directory*>\opr\bin\ConfigExchange.bat -username <username> -password <password> uploadOM -input <policy header file> OR • <*BSM_Root_Directory*>\opr\bin\ConfigExchange.bat -username <username> -password <password> -uploadOM -input <dir in which the policy header file is located> • where: • <username> is the BSM user name • <password> is the BSM user password Linux:	

Table 1 Comparison of NNMi Integrations with BSM Operations Management/OMi and HPOM, continued

Comparison Item	Direct Integration with the BSM Connector	Indirect Integration Through HPOM
	• <*BSM_Root_ Directory*>\opr\bin\ConfigExchange -username <username> -password <password> uploadOM -input <policy header file> OR • <*BSM_Root_ Directory*>\opr\bin\ConfigExchange -username <username> -password <password> -uploadOM -input <dir in which the policy header file is located> • where: • <username> is the BSM user name • <password> is the BSM user password The SNMP trap policy on the BSM Connector OM Agent is imported to the BSM server. Also see "Using the HPE NNMi—HPE BSM Operations Management or OMi Integration" on page 48	
Actions	Events cannot contain operator-initiated actions or automatic actions. You could create tools for these purposes.	Events can contain operator-initiated, automatic actions, or both.
NNMi management server monitoring	The BSM Connector serves as an event forwarder only. It does not monitor the NNMi management server.	The NNMi management server can be fully monitored by an HP Operations agent and policies.

Table 1 Comparison of NNMi Integrations with BSM Operations Management/OMi and HPOM, continued

Comparison Item	Direct Integration with the BSM Connector	Indirect Integration Through HPOM
Policy management	If your environment contains multiple NNMi management servers, you must manually exchange policies among the BSM Connectors associated with the NNMi management servers.	For the agent implementation of the HPE NNMi—HPOM integration: If your environment contains multiple NNMi management servers, HPOM can centrally manage the policies for the events forwarded from NNMi.
Licensing costs	The BSM Connector is not licensed, so there is no licensing cost.	The HP Operations Agent license adds customer cost per NNMi management server.
Communication	If an event's lifecycle state changes to the `closed` state in BSM, it can be synchronized back to the event source through the BSM Connector.	• The agent implementation of the HPE NNMi—HPOM integration is unidirectional. • The web services implementations of the HPE NNMi—HPOM integration provides bidirectional event handling.

HPE NNMi-HPE BSM Operations Management Integration

The HPE NNMi—HPE BSM Operations Management integration forwards NNMi management event incidents as SNMPv2c traps to the BSM Connector. The BSM

Connector filters the NNMi traps and forwards them to the HPE BSM Operations Management event browser. The adapter configuration determines which BSM Operations Management event browser receives the forwarded incident. If you have an Event Management Foundation license, NNMi events are displayed in the Event Browser in Operations Management. You can also access the NNMi console from the Operations Management Event Browser.

The HPE NNMi—HPE BSM Operations Management integration can also forward the SNMP traps that NNMi receives to the BSM Connector.

The BSM Connector must be installed on the NNMi management server.

After installing the BSM Connector on the NNMi management server, you must run the following command:

On Windows: **%nnminstalldir%\lbin\changeUser.ovpl**

On Linux: **/opt/OV/lbin/changeUser.ovpl**

If the NNMi events have corresponding health indicators defined, these health indicators affect the status of the relevant CIs in BSM applications, such as Service Health and Service Level Management.

If you enable northbound forwarding as recommended (using the `-omi_hi` option to `nnmopcexport.ovpl`), the events visible in the HPE BSM Operations Management event browser can include health indicators. If you enable the NNMi- BSM topology synchronization, the events are matched to CIs in the BSM RTSM inventory. For more information, see "Health Indicators" on page 49.

For more information, see "HPE NNMi—HPE BSM Operations Management/OMi Integration" on page 40.

HPE NNMi-OMi Integration

NNMi and OMi can be integrated in the same way you can integrate NNMi with HPE BSM Operations Management.

NNMi Integrated with HPOM Integrated with HPE BSM Operations Management

If you want NNMi incidents to appear in the HPOM active messages browser as well as the BSM Operations Management event browser, do *both* of the following in any order:

- Configure the agent implementation of the HPE NNMi—HPOM integration, as described in the *HP NNMi—HPOM Integration (Agent Implementation)* section of the *HP Network Node Manager i Software - HP Operations Manager Integration Guide*

- Configure the HPOM integration with the BSM Operations Management event browser as described in the *BSM - Operations Manager Integration Guide*.

NNMiVisualizations in BSM

When both NNMi and BSM are running in your environment, proper integration between the two products provides access to the following visualizations of NNMi data within BSM:

- NNMi components in the MyBSM portal of BSM. For more information, see "MyBSM Portal" on page 62.
- NNMi components in the My Workspace portal of OMi.
- NNMi console views launched from events in the BSM Operations Management and OMi event browsers. For more information, see "Using the HPE NNMi—HPE BSM Operations Management or OMi Integration" on page 48.

Topology Integration with HP Universal CMDB

For NNMi 10.00 or later, it is recommended to use the HPE NNMi–HPE BSM/OMi/UCMDB Topology integration method (explained in this chapter).

HP Universal Configuration Management Database (UCMDB) software provides the following benefits:

- Configuration and asset management
- Tracking relationships between applications and supporting hardware, servers, and network infrastructure
- Using impact modeling to show the rippling effect of infrastructure and application changes before they occur
- Tracking actual planned and unplanned changes through discovered change history
- Gaining a shared, authoritative view of the environment through awareness of existing repositories

HP Business Service Management (BSM) and OMi provide some of the same benefits as UCMDB as well as tools for managing the availability of applications in production, monitoring system performance, monitoring infrastructure performance, and proactively resolving problems when they arise.

For information about the advantages and disadvantages of the two methods for integrating NNMi topology into BSM and UCMDB, see *"Comparing Methods of Integrating NNMi with BSM/UMCDB" on page 80*.

For information about purchasing BSM, OMi, or HP UCMDB, contact your HP sales representative.

This chapter contains the following topics:

- "Disabling the HPE NNMi–HPE BSM/OMi/UCMDB Topology Integration" on page 32
- "Troubleshooting the HPE NNMi–HPE BSM/OMi/UCMDB Topology Integration" on page 32
- "Application Failover and the HPE NNMi–HPE BSM/OMi/UCMDB Topology Integration" on page 32
- "HPE NNMi–HPE BSM/OMi/UCMDB Topology Integration Configuration Form Reference" on page 33

HPE NNMi-HPE BSM/OMi/UCMDB Topology Integration

The HPE NNMi–HPE BSM/OMi/UCMDB Topology integration populates NNMi topology into either the BSM/OMi Run-time Service Model (RTSM) or the UCMDB database. Each device and device component in the NNMi topology is stored as a configuration item (CI) in RTSM or UCMDB. BSM or UCMDB users and integrated applications can also see the relationships between NNMi managed layer 2 network devices and BSM-discovered or UCMDB-discovered servers, hosted applications, and more.

Additionally, the integration stores the identifier of populated CIs in the NNMi database. Uses for the CIs of the NNMi-managed devices include the following:

- NNMi components in the MyBSM portal. For more information, see "MyBSM Portal" on page 62.
- Path health views available from the BSM Real User Monitor (RUM). For more information, see "Configuring an HTTPS Connection" on page 64.
- Using the agent implementation of the HPE NNMi—HPOM integration, and pointing to a BSM Connector, results in an HP NNMi–HP BSM Operations Management integration that associates incidents regarding NNMi-managed devices with BSM CIs. For more information, see "Configuration Item Identifiers" on page 49.
- Using the agent implementation of the HPE NNMi—HPOM integration, and pointing to an HPOM agent on the NNMi management server, can associate incidents regarding NNMi-managed devices with BSM CIs. For more information, see the *Configuration Item Identifiers* section of the *HP Network Node Manager i Software - HP Operations Manager Integration Guide*.
- The comprehensive relationships maintained by RTSM or UCMDB enable an NNMi operator to view the impact of a network access switch infrastructure failure on other supported devices and applications. The NNMi operator selects an incident or a node in NNMi and then enters a request for impacted CIs.

Value

The HPE NNMi–HPE BSM/OMi/UCMDB Topology integration sets up NNMi as the authoritative source for network infrastructure device status and relationship information. By supplying this topology information to RTSM or the UCMDB database, the integration enables performing change management activities, impact analysis, and event reporting as an enabler for other integrations with BSM or UCMDB.

Integrated Products

The information in this chapter applies to the following products:

- BSM or OMi
- UCMDB

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

- NNMi 10.20

NNMi and BSM/OMi or UCMDB must be installed on separate computers. The NNMi management server and the BSM/OMi gateway server or UCMDB server can be of the same or different operating systems.

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

Documentation

This chapter describes how to configure NNMi to communicate with BSM or UCMDB.

The BSM documentation suite describes the BSM features and capabilities in detail. The UCMDB documentation suite describes the UCMDB features and capabilities in detail. The documentation suites are included on the associated product media.

Enabling the HPE NNMi-HPE BSM/OMi/UCMDB Topology Integration

CAUTION: UCMDB provides a legacy integration method for pulling topology data from NNMi. NNMi cannot simultaneously integrate with UCMDB using this legacy method and the method described in this chapter. If the legacy UCMDB integration is configured to pull data from this NNMi management server, disable that configuration before enabling the HPE NNMi–HPE BSM/OMi/UCMDB Topology integration. If you want NNMi information in both databases, do *both* of the following in any order:

- Configure the HPE NNMi–HPE BSM/OMi/UCMDB Topology integration, as described in this chapter.
- Configure the BSM integration with UCMDB, as described in the *UCMDB Data Flow Management Guide*, which is included on the UCMDB product media. This manual is also available for the UCMDB product at:
  https://softwaresupport.hp.com

> **TIP:** For better accountability and auditing, create and use a new RTSM user. The CIs that are created or updated by this integration set the attributes `Created By` and `Updated By`. By using a different user for the integration, these attributes are set to `UCMDB:User:<integration_user>` instead of the more generic `UCMDB:User:admin.` A new RTSM user name makes it easier to discern the source responsible for the CI. For details, see "Creating a New RTSM User" on page 82.

On the NNMi management server, configure the connection between NNMi and BSM/OMi or UCMDB by following these steps:

1. *Prerequisite*: Verify that the BSM/OMi or UCMDB license and the NNMi license are installed. For details, see “License Management Overview”in the *BSM Platform Administration Guide* or “Licensing” in the *UCMDB Installation and Configuration Guide*.
2. *Optional*. Update the RTSM or UCMDB model for interfaces to set the interface display label to prefer interface name over MAC address:
   a. If you use BSM, in the BSM or UCMDB user interface, open the **CI Type Manager** page (**Admin > RTSM Administration > Modeling > CI Type Manager**).

      If you use OMi, in the OMi user interface, open the **CI Type Manager** page (**Administration > RTSM Administration > Modeling > CI Type Manager**).
   b. In the **CI Types** pane, select Interface (**Configuration Item > Infrastructure Element > Node Element > Interface**).
   c. On the **Default Label** tab in the editing pane, under **CI Type Attributes**, select **InterfaceName**.
   d. Under **CI Type Label Definition Format**, set the format to:

      ```
      interface_name | mac_address
      ```
3. In the NNMi console, open the **HPE NNMi–HPE BSM/OMi/UCMDB Topology Integration Configuration** form (**Integration Module Configuration > HP BSM/UCMDB Topology**).
4. Select the **Enable Integration** check box to make the remaining fields on the form available.

5. Enter the information for connecting to the NNMi management server. For information about these fields, see "NNMi Management Server Connection" on page 33.
6. Enter the information for connecting to the BSM gateway server or the UCMDB server. For information about these fields, see "BSM/OMi Gateway Server or UCMDB Server Connection" on page 34.
7. *Optional:* Select **Only synchronize managed objects** if you want to exclude unmanaged CIs and unconnected interfaces from the integration.
8. *Optional*: Select the **More Options** button for finer grain control over the types of CIs to be included in the topology synchronization. For information about these fields, see "Configuration Item Topology Filter" on page 35.
9. *Optional*: Enter the information that describes which NNMi nodes should be maintained in BSM. For information about these fields, see "Node Topology Filter" on page 35.
10. *Optional*: Adjust the **Topology Synchronization Interval** hours to increase the period between full topology synchronizations.

    The HPE NNMi–HPE BSM/OMi/UCMDB Topology integration continually updates the RTSM or the UCMDB database as CIs or CI relationships change. However, it is possible that some dynamic updates are missed due to network communication issues or the temporary unavailability of BSM/OMi or UCMDB. For this reason, the integration performs a full topology synchronization every 24 hours by default. For large scale installations involving more than 5000 node CIs, it might be preferable to increase the synchronization interval to 48, 72 or more hours.
11. Enter a **Rule bundle name** that defines the set of rules used to identify impacted CIs during the **Find BSM/UCMDB impacted CIs** integration action from an NNMi node. BSM, OMi, and UCMDB maintain a set of rule groups in their Impact Analysis Manager.

    These rules determine which CIs can be impacted by a network event, for example, the selected node goes down. The default rule group used by the integration is `NNMi`.

    You can also enter a **Rule severity level**, which determines the impact analysis trigger severity when applying the rules.
12. 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 NNMi management server, click **Return**, and then adjust the values as suggested by the text of the error message.

    > **NOTE:** If you cannot connect to the NNMi management server, and suspect a problem with certificates, see *Working with Certificates for NNMi* in the *NNMi 10.20 Deployment Reference*.

13. Make sure that single sign-is configured in both BSM, OMi, or UCMDB and NNMi with the same initialization string values.

    For information about configuring the initialization string values in UCMDB, see the section about enabling LW-SSO between Configuration Manager and UCMDB in the *HP Universal CMDB Deployment Guide*.

    For information about configuring the initialization string values in NNMi, see "Configuring an HTTPS Connection" on page 64.

14. To display NNMi data in BSM or OMi, complete the steps shown in "Enabling NNMi Visualizations from BSM or OMi" on page 79.

15. If you use BSM, you can view NNMi data in MyBSM and EUM, as described in "NNMi Components Available in MyBSM" on page 62 and "End User Management Reports with Drilldown to NNMi" on page 77.

    If you use OMi, you can view NNMi data in My Workspace.

    For more information about Impact Analysis rules for BSM or OMi, see **RTSM Guides > Modeling > Modeling > Impact Analysis Manager** in the BSM Console help or OMi online help or **Modeling > Modeling > Impact Analysis Manager** in the UCMDB console help.

Configuring Single Sign-On Between NNMi and BSM, OMi, or UCMDB

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

If the HP NNMi and HP Business Service Management (HP BSM) user names are exactly the same for a particular individual, that person can log on to the MyBSM portal and view NNMi portlets without also logging on to HP NNMi. This single sign-on feature maps user names, but not passwords, between the two products. The passwords for logging on to MyBSM and HP NNMi 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 normal privileges in HP BSM and administrator privileges in HP NNMi.

For more information about single sign-on, see “Using Single Sign-On (SSO) with NNMi” in the NNMi Deployment Reference.

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

NNMi initialization string

Locate the NNMi initialization string as follows:

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 =
   ```
3. Make sure the `com.hp.nms.ui.sso.isEnabled` property is set to `true`.
4. 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
   ```

   Copy this string.
5. If you change the value of the `initString` parameter shown in "Look for a section in the file that resembles the following:" above, run the following command to commit the changes:

   ```
   nnmsso.ovpl -reload
   ```

BSM initialization string

Locate the BSM initialization string as follows:

1. In the BSM console, go to **Admin > Platform > Users and Permissions > Authentication Management**.
2. Under the Single Sign-On Configuration section, click **Configure**. The Single Sign-On Configuration wizard opens.
3. In the Single Sign-On Configuration wizard:
   - Select **Lightweight**.
   - In the Token Creation Key box, type the value of the `initString` parameter that was copied in "Look for a section in the file that resembles the following:" above.
   - Follow the instructions in BSM Online Help for configuring other settings in the Single Sign-On Configuration wizard.

OMi initialization string

Locate the OMi initialization string as follows:

1. In the OMi console, go to **Administration > Users > Authentication Management**.
2. Under the Single Sign-On Configuration section, click **Configure**. The Single Sign-On Configuration wizard opens.
3. In the Single Sign-On Configuration wizard:
   - Select **Lightweight**.
   - In the Token Creation Key box, type the value of the `initString` parameter that was copied in "Look for a section in the file that resembles the following:" on the previous page.
   - Follow the instructions in OMi Online Help for configuring other settings in the Single Sign-On Configuration wizard.

Configure NNMi for the Proper Source Character Encoding for SNMP Agents

Node reconciliation in UCMDB and BSM/OMi Topology often depends on string matching of values provided by different data providers. In some cases, the values NNMi sends to BSM/OMi/UCMDB contain null bytes at the end. Interface Description values are one example.

This can prevent an exact match with data provided by other data providers and causes problems for object reconciliation. The Interface Description value contains these characters because NNMi by default interprets OCTET STRING values from SNMP Agents with the UTF-8 character encoding, but the SNMP Agent returns the data in some other character encoding, such as the ISO-8859-1 character encoding.

The SNMP OCTET STRING data is interpreted based on any character encodings defined by the `com.hp.nnm.sourceEncoding` property in the `nms-jboss.properties` file.

To configure NNMi for the proper source character encoding to expect for SNMP Agents, you must configure the character set encoding settings in the `nms-jboss.properties` file.

For example, set the property value of `com.hp.nnm.sourceEncoding` to `ISO-8859-1, UTF-8` to properly interpret the SNMP OCTET STRING data as follows:

1. Open the `nms-jboss.properties` file:

   Windows: `%NNM_PROPS%\nms-jboss.properties`

   Linux: `$NNM_PROPS/nms-jboss.properties`

2. Search for the text block containing the following line:

   ```
   #!com.hp.nnm.sourceEncoding=UTF-8
   ```

3. Edit the line as follows:

   ```
   com.hp.nnm.sourceEncoding=ISO-8859-1, UTF-8
   ```

NOTE: The ISO 8859-1 is only one example of possible conflicting source character encoding. A different environment may require different values for the source encoding.

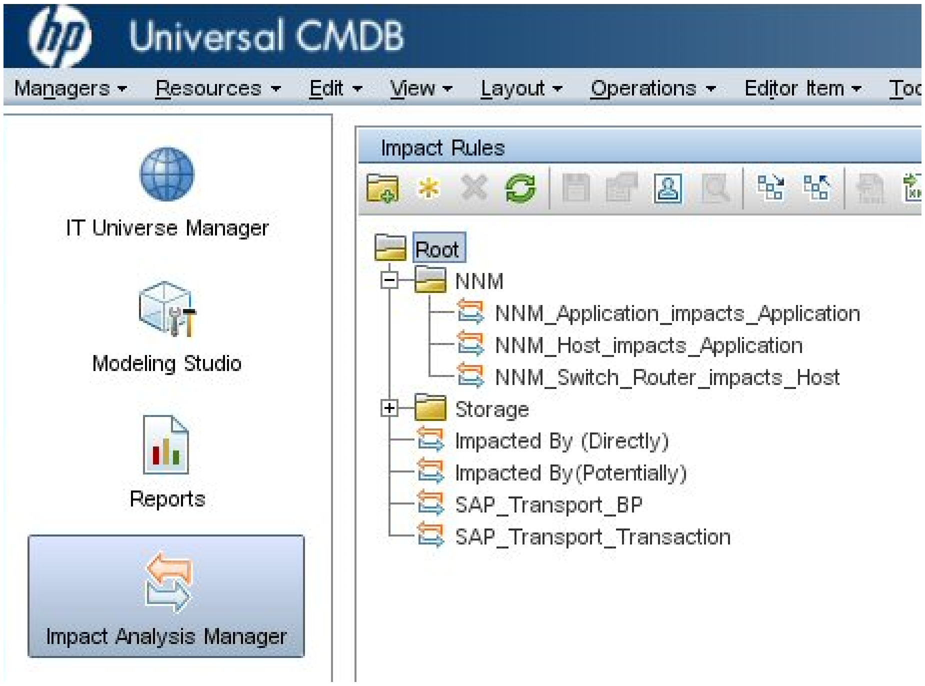
For more information, see "Configuring Character Set Encoding Settings for NNMi" in the NNMi Deployment Reference.

Enabling the Find BSM/OMi/UCMDB Impacted CIs Feature

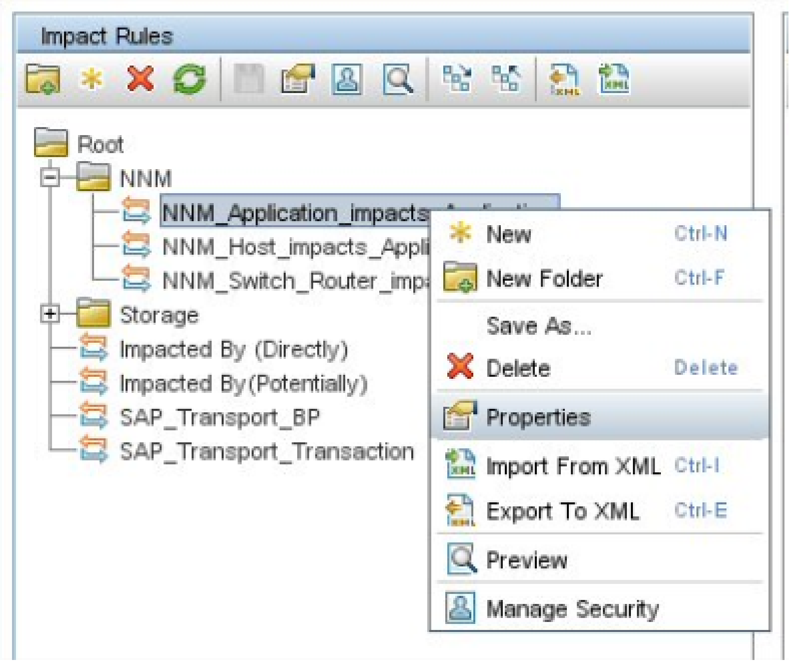
To enable the **Find BSM/UCMD impacted CIs** feature in the NNMi-BSM integration, you must add the rules provided by NNMi to the NNMi Rule bundle using the **Impact Analysis Manager** as follows:

Caution: If the default **NNMi** rule bundle is selected when the NNMi-BSM integration is enabled and you do not add the rules provided to the NNMi Rule bundle using the **Impact Analysis Manager** as described in the following steps, the set of CIs will be empty.

1. Click **Impact Analysis Manager**.
2. From the **Impact Rules** pane, navigate to the **Root/NNM** folder:



3. For each rule listed:
   a. Right-click the rule and select **Properties**:

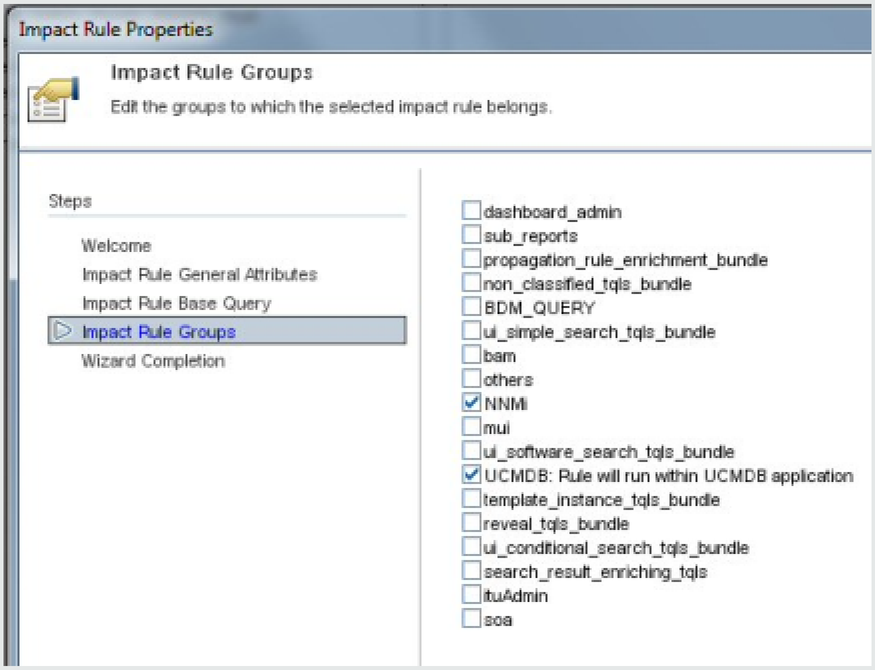


   b. In the **Properties** wizard, click **Next**.

c. Navigate to the **Impact Rules Group**.

d. Click to select **NNMi.**

> **Tip:** If the **NNMi** Rule Bundle is not visible, first enable the NNMi-BSM integration as described in "Enabling the HPE NNMi–HPE BSM/OMi/UCMDB Topology Integration" on page 15:



Impact Rule Properties

Impact Rule Groups

Edit the groups to which the selected impact rule belongs.

Steps

- Welcome
- Impact Rule General Attributes
- Impact Rule Base Query
- ▷ Impact Rule Groups
- Wizard Completion

□ dashboard_admin
□ sub_reports
□ propagation_rule_enrichment_bundle
□ non_classified_tqls_bundle
□ BDM_QUERY
□ ui_simple_search_tqls_bundle
□ bam
□ others
☑ NNMi
□ mui
□ ui_software_search_tqls_bundle
☑ UCMDB: Rule will run within UCMDB application
□ template_instance_tqls_bundle
□ reveal_tqls_bundle
□ ui_conditional_search_tqls_bundle
□ search_result_enriching_tqls
□ ituAdmin
□ soa

Using the HPE NNMi-HPE BSM/OMi/UCMDB Topology Integration

The HPE NNMi–HPE BSM/OMi/UCMDB Topology integration populates the following CI types in the BSM RTSM or the UCMDB database:

- InfrastructureElement > Node

  The nodes in the NNMi topology. You can limit the set of nodes as described in "Node Topology Filter" on page 35.

- InfrastructureElement > NodeElement> Interface

  The interfaces associated with the Node CIs that the integration populates.

- InfrastructureElement > NetworkEntity > IpAddress

  The IP addresses of the interfaces associated with the Node CIs that the integration populates in BSM, OMi, or UCMDB.

- InfrastructureElement > NodeElement> HardwareBoard

The cards associated with the Node CIs that the integration populates in BSM or UCMDB.

> **NOTE:** The HP NNMi–HP UCMDB integration reports chassis elements to UCMDB/RTSM, as those chassis elements host ports. RTSM/UCMDB displays these chassis elements as hardware boards. This is done to differentiate NNMi chassis elements from the CI called Chassis in UCMDB/RTSM.

- InfrastructureElement > NodeElement> PhysicalPort

  The ports associated with the Node CIs that the integration populates in BSM or UCMDB.
- InfrastructureElement > NetworkEntity > IpSubnet

  All subnets in the NNMi topology. Unless explicitly excluded, all subnets are provided to the RTSM or UCMDB database so that they are available for IP address relationships when node IP address CIs are created from the NNMi topology. For information about excluding CI types from the integration, see "Configuration Item Topology Filter" on page 35.
- InfrastructureElement > NetworkEntity > Layer2Connection

  The NNMi Layer 2 connections with at least two connection ends that the integration populates as Node CIs in BSM.
- InfrastructureElement > NetworkEntity > Vlan

  The NNMi VLANs with at one port that the integration populates as a Port CI in BSM, OMi, or UCMDB.

For each CI created in the BSM/OMi RTSM, the integration stores the RTSM identifier or the UCMDB Global Id in the NNMi database.

> **TIP:** By default, NNMi does not discover end nodes. Update the NNMi discovery and monitoring configuration to include the end nodes that you want to see in BSM, OMi, or UCMDB.

Best practice: Use the **NodeRole** attribute to track any role changes for network devices. For example, a device role might change from switch to a switch-router. Devices such as switches, routers, and servers are all defined as Node CI Types. The device type is identified by the Node CI’s **NodeRole** attribute. The **NodeRole** attribute is set to one or more of the following values:

- `hub`
- `load_balancer`
- `printer`
- `router`

- `server`
- `lan_switch`
- `voice_gateway`
- `desktop`

TIP: A single node can have multiple node roles. NNMi uses the node's **Device Category** and the node's capabilities to determine which **NodeRoles** to set.

If a node has an IP forwarding capability (com.hp.nnm.capability, node.ipforwarding), NNMi sets the **NodeRole** to `router`. If a node has switching capability (com.hp.nnm.capbility.node, node.lan_switching), NNMi sets the **NodeRole** to `lan_switch`.

The following table shows the mapping of NNMi **Device Category** to **NodeRole** attribute.

NNMi Device Category	NodeRole Attribute
Hub	hub
LoadBalancer	load_balancer
Printer	printer
Router	router
Server	server
Switch	lan_switch
Switch_Router	router, lan_switch
Voice Gateway	voice_gateway
Workstation	desktop

The NNMi-BSM/OMi topology integration creates the following relationships:

- Membership: **IpSubnet > IpAddress**
- Membership:**Layer2Connection > Interface**
- Composition: **Node > Interface**
- Containment: **Node > IpAddress**
- Composition: **Node > HardwareBoard**
- Composition: **HardwareBoard > HardwareBoard**

- Composition: **HardwareBoard > PhysicalPort**
- Realization: **PhysicalPort > Interface**

See "NNMi - CI Attribute Mapping" on page 83 for the mapping of NNMi attributes to the equivalent CI attributes for each CI type.

The HPE NNMi–HPE BSM/OMi/UCMDB Topology integration forwards NNMi information and updates to the BSM/OMi RTSM or the UCMDB database as a one-way communication. Because NNMi does not know or control how the BSM CI information is used, the integration relies on the BSM/OMi CI aging settings to delete CIs that have not been updated for a set period of time.

TIP: For information about the CI lifecycle, including instructions about enabling and running the aging mechanism, see “CI Lifecycle and the Aging Mechanism” and the related links in the *BSM help* or the *UCMDB help*. In the BSM console, this information is available from: **RTSM Guides > RTSM Administration > Administration > CI Lifecycle and the Aging Mechanism**. In the UCMDB console, this information is available from: **Administration > Administration > CI Lifecycle and the Aging Mechanism**.

The HPE NNMi–HPE BSM/OMi/UCMDB Topology integration enables other products to use the NNMi topology information when they integrate with BSM or UCMDB.

Network Topology Views

The network topology views in BSM are designed to work with the historical NNMi – UCMDB integration method. This is because the TQLs includes a **Net Device CI** type or a **Computer** CI type, whereas the NNMi - BSM topology integration creates nodes as **Node** CIs only, setting the **NodeRole** attribute to identify the device types as servers, switches, and so forth.

Until the views are updated in the product, you can easily modify them to work with the NNMi populated network topology. The following sections describe how to modify views to suit modeling with RTSM, Service Health and Operations Management.

Layer 2 Topology View

The following two figures show the results, comparing an NNMi Layer 2 Neighbor View with the equivalent Layer 2 by NNMi view in BSM. The third figure shows the Layer 2 by NNMi view in UCMDB using the historical NNMi – UCMDB integration method, to show that the results are equivalent.

Figure 1 NNMi Layer 2 neighbor view

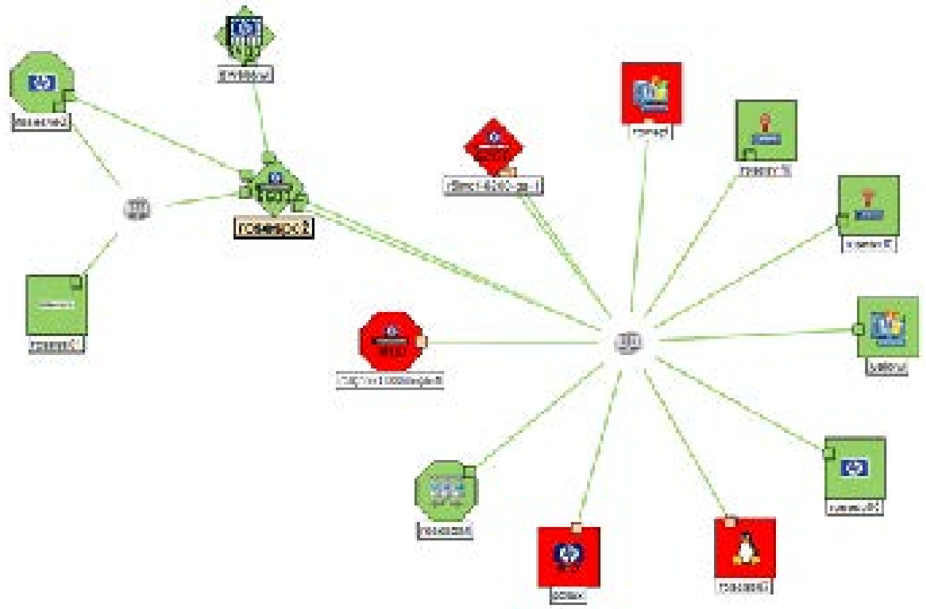


Figure 2 BSM Layer 2 by NNMi view

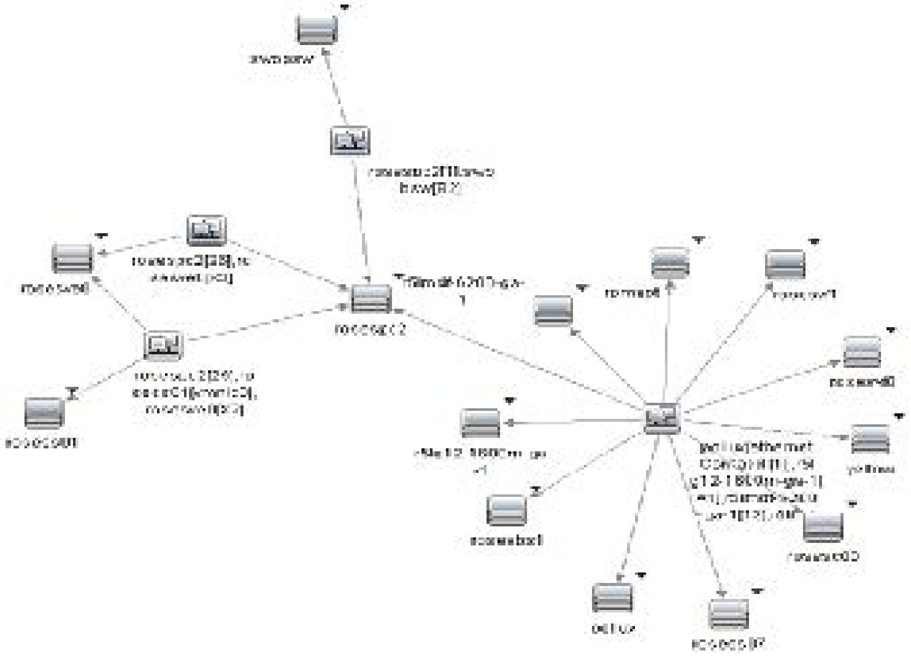
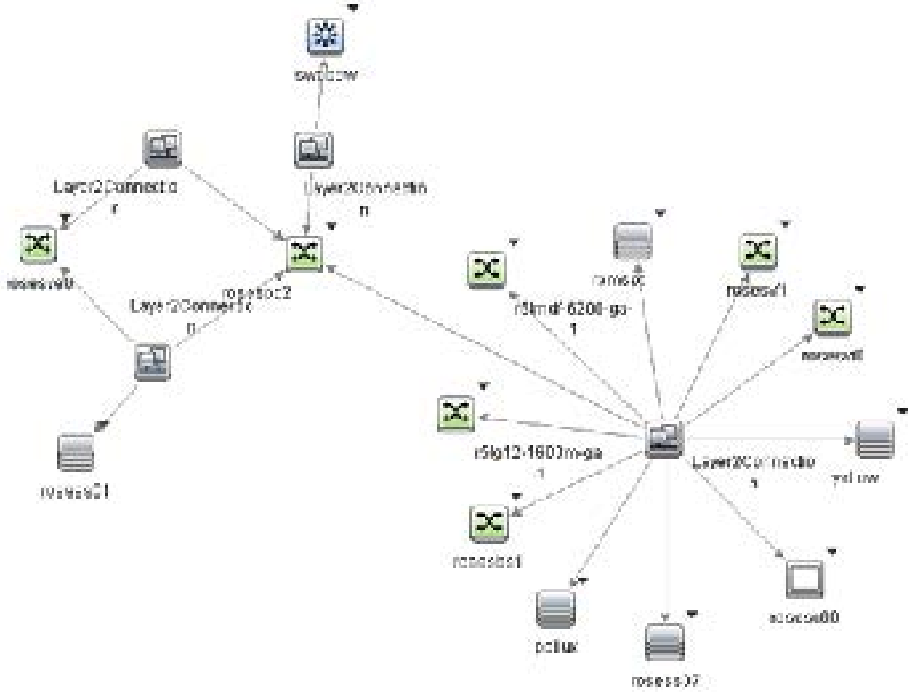


Figure 3 UCMDB Layer 2 by NNMi view



This type of view (Layer 2 by NNMi) is primarily useful as a basis for a TBEC rule, or to filter OMi events in View Selector. It is not optimal for use in Service Health. Refer to the "Service Health Views" on page 30 section for recommendations on creating views that include network devices. However, if you do want to display this view in Service Health, you need to modify the View Definition Properties and set the Bundles to **Service_ Health**.

For a view that is used in the View Selector to filter OMi events, you might want to include all CIs that may have network events associated with them. NNMi events resolve to **Node**, **Interface**, **Layer 2 Connection** or **IP Address** CI Types; you therefore might add **IP Address** to the view. The following two figures show an example view containing the network elements associated with the **OBA1** business application.

Figure 4 Example of Layer 2 topology applied to a business application

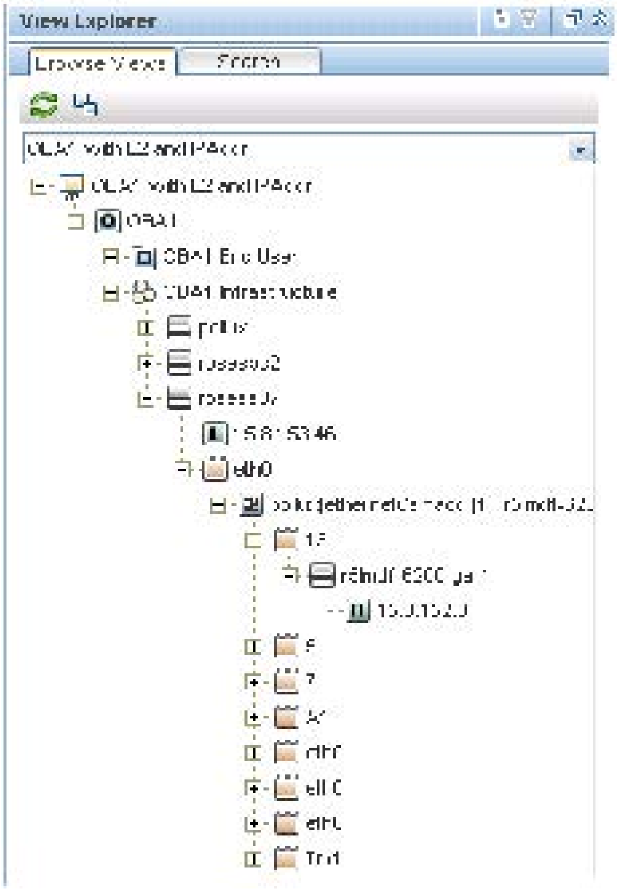
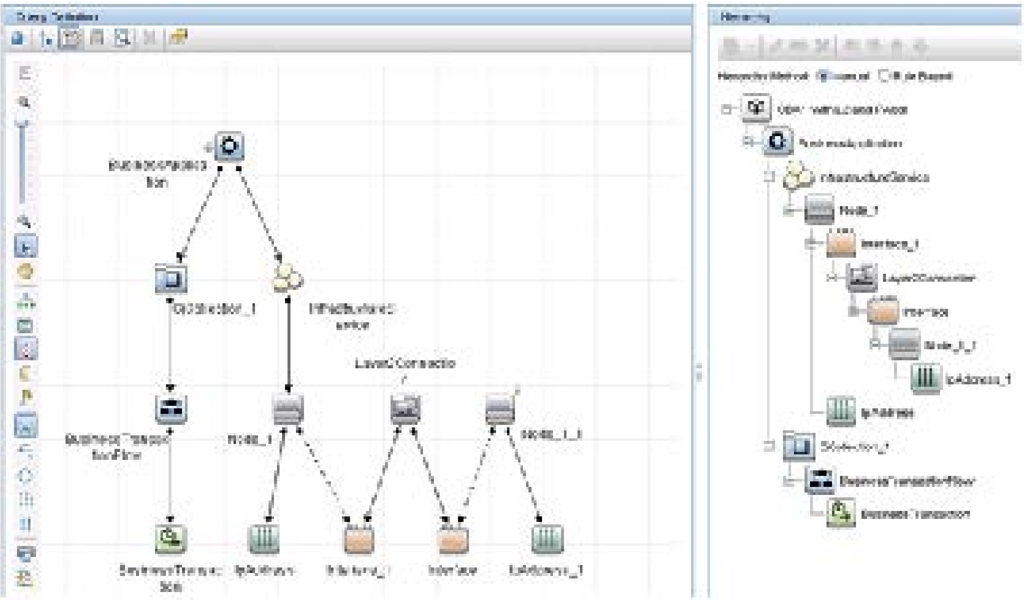


Figure 5 View Definition:

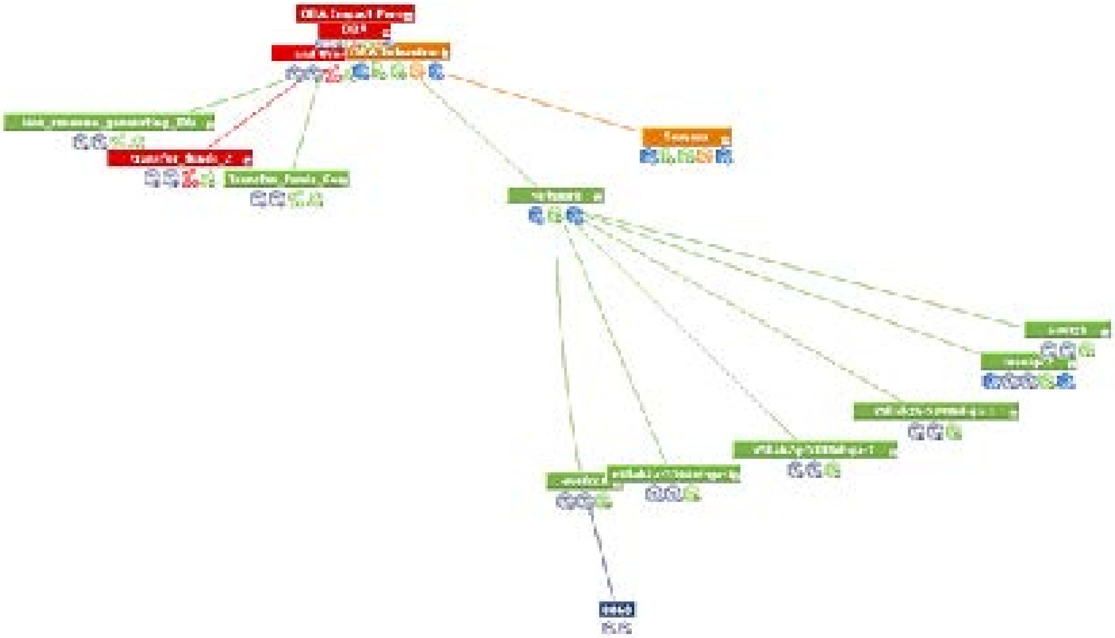


Service Health Views

It is difficult to display traditional network topology within Service Health. A relationship of **Node -> Interface -> Layer2Connection -> Interface -> Node** is meaningless, since (for example) there is no impact relationship (that is, KPI status propagation) between Layer2Connection and Interface.

If you need to include network devices in a Service Health view, it is best to show them in a flat structure rather than to attempt to reproduce a traditional network topology. Since there is an impact relationship between Interface and Node, one approach is to create a view that contains **Node -> Interface**, possibly grouped together as **Network** as shown in the following example:

Figure 6 Top view:



OMi Health Perspectives

In OMi Health Perspectives, the **Health Top View** displays a view based on the Related CI of the selected event. The default view is determined by **View Mappings** for the CI.

The default View Mappings used in Health Perspectives do not work for the Node CI and Interface CI.

For the Node CI, there is no default **View Mapping**. If you use OMi Health Perspectives, you may want to define such a view.

For the Interface CIT, the default View Mappings of *NetworkInterface_Infrastructure* and *Systems_Infrastructure* depend on a Computer CI. Thus, for nodes that are populated from NNMi, these views will fail. You might want to modify the **NetworkInterface_Infrastructure** view to use Node CI instead of Computer CI.

Additional NNMi Functionality Provided by the Integration

The HPE NNMi–HPE BSM/OMi/UCMDB Topology integration provides access to the RTSM or UCMDB Impact Analysis Manager to determine what CIs may be affected by a network outage.

Running the BSM, OMi, or UCMDB Impact Analysis from the NNMi Console

The HPE NNMi–HPE BSM/OMi/UCMDB Topology integration provides links to BSM or UCMDB from the NNMi console.

Enabling the HPE NNMi–HPE BSM/OMi/UCMDB Topology integration adds the following item to the **Actions** menu for nodes in the NNMi console:

Find BSM Impacted CIs—Displays a list of the CIs returned from the BSM or UCMDB Impact Analysis Manager after applying the group of rules with the severity trigger value as configured on the **HP NNMi-HP BSM/UCMDB Topology Integration Configuration** form. For additional CI details, you can select **Open CI in BSM** from any of the listed impacted CIs to launch CI details in the BSM console or the UCMDB console.

Changing the HPE NNMi-HPE BSM/OMi/UCMDB Topology Integration Configuration

1. In the NNMi console, open the **HP NNMi-HP BSM/UCMDB Topology Integration Configuration** form (**Integration Module Configuration > HP BSM Topology**).
2. Modify the values as appropriate. For information about the fields on this form, see "HPE NNMi–HPE BSM/OMi/UCMDB Topology Integration Configuration Form Reference" on page 33.
3. 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.

NOTE: The changes take effect immediately.

Disabling the HPE NNMi-HPE BSM/OMi/UCMDB Topology Integration

1. In the NNMi console, open the **HP NNMi-HP BSM/UCMDB Topology Integration Configuration** form (**Integration Module Configuration > HP BSM Topology**).
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 URL actions are no longer available.

NOTE: The changes take effect immediately.

Troubleshooting the HPE NNMi-HPE BSM/OMi/UCMDB Topology Integration

This section contains the following topics:

- "Interface Labels Appear as MAC Addresses in the BSM User Interface" below
- "Duplicate CIs for Managed Nodes in the RTSM" below

For information about troubleshooting the connection to the RTSM, see the BSM documentation suite.

Interface Labels Appear as MAC Addresses in the BSM User Interface

By default, the RTSM or UCMDB model prefers MAC addresses over interface names for an interface label. To display interface names in the BSM console or the UCMDB console, edit the interface model in the BSM or OMi console or the UCMDB console.

Duplicate CIs for Managed Nodes in the RTSM

If HP Operations Manager also synchronizes with the RTSM, you might see duplicate CIs for managed nodes in the RTSM. Nodes discovered by HPOM are of CI type Computer, while nodes discovered by NNM iSPI NET are of CI type Node. This duplication does not affect product performance.

Application Failover and the HPE NNMi-HPE BSM/OMi/UCMDB Topology Integration

If the NNMi management server participates in NNMi application failover, the HPE NNMi–HPE BSM/OMi/UCMDB Topology continues with the new NNMi management server hostname after failover occurs. Failover should be transparent to users of the integration.

The integration does not support automatic failover of the BSM/OMi server.

HPE NNMi-HPE BSM/OMi/UCMDB Topology Integration Configuration Form Reference

The **HP NNMi-HP BSM/UCMDB Topology Integration Configuration** form contains the parameters for configuring communications between NNMi and BSM, OMi, or UCMDB. This form is available from the **Integration Module Configuration** workspace.

NOTE: Only NNMi users with the Administrator role can access the **HP NNMi-HP BSM/UCMDB Topology Integration Configuration** form.

The **HP NNMi-HP BSM/UCMDB Topology Integration Configuration** form collects information for the following areas:

- "NNMi Management Server Connection" below
- "BSM/OMi Gateway Server or UCMDB Server Connection" on the next page
- "Node Topology Filter" on page 35

To apply changes to the integration configuration, update the values on the **HP NNMi-HP BSM/UCMDB Topology Integration Configuration** form, and then click **Submit**.

NNMi Management Server Connection

"Table 2 NNMi Management Server Information" below lists the parameters for connecting to the NNMi management server. This is the same information that you use to open the NNMi console. You can determine many of these values by examining the URL that invokes an NNMi console session. Coordinate with the NNMi administrator to determine the appropriate values for this section of the configuration form.

Table 2 NNMi Management Server Information

Field	Description
NNMi SSL Enabled	The connection protocol specification. • If the NNMi console is configured to use HTTPS, select the **NNMi SSL Enabled** check box. • If the NNMi console is configured to use HTTP, clear the **NNMi SSL Enabled** check box. The integration selects the port for connecting to the NNMi console based on this specification.
NNMi Host	The official fully-qualified domain name of the NNMi management server. This field is read-only.
NNMi User	The user name for connecting to the NNMi web services. This

Table 2 NNMi Management Server Information, continued

Field	Description
	user must have the NNMi Administrator or Web Service Client role.
NNMi Password	The password for the specified NNMi user.

BSM/OMi Gateway Server or UCMDB Server Connection

"Table 3 BSM Gateway Server Information" below lists the parameters for connecting to the BSM/OMi gateway server or the UCMDB server to communicate with the BSM RTSM or the UCMDB database. Coordinate with the BSM, OMi, or UCMDB administrator to determine the appropriate values for this section of the configuration.

> **NOTE:** References to BSM in the configuration form apply to either the BSM gateway server, OMi gateway server, or the UCMDB server.

Table 3 BSM Gateway Server Information

BSM/OMi Gateway Server or UCMDB Server Parameter	Description
BSM SSL Enabled	The connection protocol specification for connecting to BSM, OMi, or UCMDB. • If BSM, OMi, or UCMDB is configured to use HTTPS, select the **BSM SSL Enabled** check box. • If BSM, OMi, or UCMDB is configured to use HTTP, clear the **BSM SSL Enabled** check box. • If you cannot connect to the NNMi management server, and suspect a problem with certificates, see *Working with Certificates for NNMi* in the *NNMi 10.20 Deployment Reference*.
BSM Host	The fully-qualified domain name of the BSM gateway server, OMi gateway server, or the UCMDB server.
BSM Port	The port for connecting to BSM or UCMDB. If you are using the default BSM configuration, use the default http port `80` for BSM or the default http port 8080 for UCMDB.

Table 3 BSM Gateway Server Information, continued

BSM/OMi Gateway Server or UCMDB Server Parameter	Description
	The default https port is 443 for BSM and UCMDB.
BSM RTSM User	The user name for the BSM RTSM or UCMDB administrator.
BSM RTSM Password	The password for the BSM RTSM or UCMDB administrator. The BSM RTSM administrator is not a BSM administrator, but is an RTSM administrator for the internal RTSM. A BSM Administrator must configure the RTSM user with the administrator role. For more information, see "Creating a New RTSM User" on page 82.

Configuration Item Topology Filter

By default, the HPE NNMi–HPE BSM/OMi/UCMDB Topology integration populates information about nodes and also about several other NNMi topology items including IP subnets, interfaces, IP addresses, cards, ports, layer 2 connections, and VLANs. Use the Node Topology Filter field described in the next section to configured the set of nodes to be populated. For the other CI types, select the **More Options** button on the **HP NNMi-HP BSM/UCMDB Topology Integration Configuration** form and deselect any CI types that should not be populated into the RTSM or the UCMDB database. For example, NNMi might monitor many thousands of interfaces that are unconnected in the topology. Populating this information into the RTSM or the UCMDB database could result in longer synchronization times and more complex maps. If this information is not needed in the RTSM or the UCMDB database, you can safely exclude it from the integration.

Remember that some CI types depend on the presence of others. For example, VLANs require knowledge of the associated ports. For this reason, some CI types are not selectable if a required dependent CI type is not selected.

Node Topology Filter

By default, the HPE NNMi–HPE BSM/OMi/UCMDB Topology integration conveys information about all nodes and, optionally, node sub-components, in the NNMi topology to BSM or UCMDB. If you want the integration to maintain only a subset of the NNMi node topology information in BSM, specify one or both of the optional node groups as described in this section.

The scenarios for the filtering NNMi topology information are as follows:

- Definitive—In NNMi, create one node group that explicitly defines every NNMi node to be included in the BSM RTSM or the UCMDB database. This approach requires an intimate knowledge of your network topology.

  For example, you might create a node group called BSM_Topology containing the following types of devices:

  - The application servers in the managed environment
  - The routers and switches that connect the application servers

  In this case, specify the node group (for example, BSM_Topology) as the topology filter node group. Do not specify an additional connections node group.

  The integration forwards information about every node in the specified topology filter node group (for example, BSM_Topology) and ignores all other nodes in the NNMi topology.

- Additive—In NNMi, identify (or create) a node group that defines the core infrastructure of the monitored network, and then create another node group that defines the end nodes of interest.

  For example, you might create the following NNMi node groups:

  - The BSM_Core group that contains the Networking Infrastructure Devices node group and other key connective devices
  - The BSM_End_Nodes group that contains the application servers in the managed network

  In this case, specify the first node group (for example, BSM_Core) as the topology filter node group. Also, specify the second node group (for example, BSM_End_Nodes) as the additional connections node group.

  The integration forwards information about every node in the topology filter node group (for example, BSM_Core). The integration then examines each node in the additional connections node group (for example, BSM_End_Nodes) as follows:

  - If the node is connected to one or more nodes in the topology filter node group, the integration forwards the information about that node to BSM, OMi, or UCMDB.
  - If the node is not connected to any of the nodes in the topology filter node group, the integration ignores that node.

"Table 4   Node Topology Filter Information" on the next page lists the optional parameters for specifying a node topology filter and provides information about entering values for these parameters.

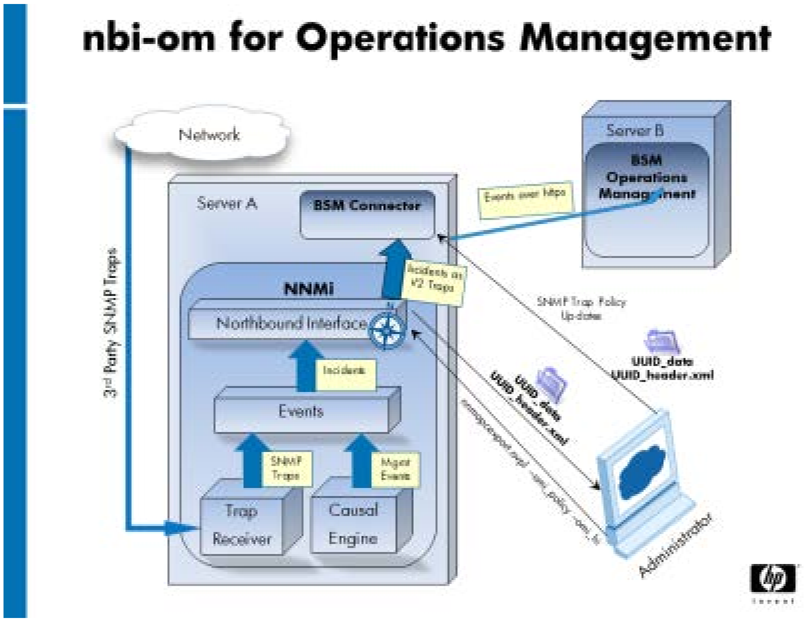
Table 4 Node Topology Filter Information

Node Topology Filter Parameter	Description
Topology Filter Node Group	The NNMi node group containing the primary set of nodes to populate in BSM. The integration populates the RTSM or the UCMDB database with information about every node in this node group. Enter the name of the node group exactly as it is written (with no quotation marks or extra characters) in the **Name** field of the **Node Group** form in NNMi. If you do not specify a topology filter node group, the HPE NNMi–HPE BSM/OMi/UCMDB Topology integration populates the RTSM or the UCMDB database with all nodes and interfaces in the NNMi topology. In this case, the integration ignores the value of the **Connections Node Group** field.
Additional Connections Node Group	The NNMi node group containing hints of additional nodes to populate in BSM or UCMDB. The integration populates the RTSM or the UCMDB database with information about only those nodes in this node group that are connected (in the NNMi topology) to one or more nodes in the topology filter node group. Enter the name of the node group exactly as it is written (with no quotation marks or extra characters) in the **Name** field of the **Node Group** form in NNMi. If you specify a topology filter node group and specify an additional connections node group, the HPE NNMi–HPE BSM/OMi/UCMDB Topology integration forwards information about the nodes and interfaces in the topology filter node group and the connected nodes in the additional connections node group. If you specify a topology filter node group but do not specify an additional connections node group, the HPE NNMi–HPE BSM/OMi/UCMDB Topology integration forwards information about the nodes and interfaces in the topology filter node group only. If you do not specify a topology filter node group, the HPE NNMi–HPE BSM/OMi/UCMDB Topology integration populates the RTSM with all nodes and interfaces in the NNMi topology. In this case, the integration ignores the value of the **Additional**

Table 4 Node Topology Filter Information, continued

Node Topology Filter Parameter	Description
	Connections Node Group field.

HPE BSM Operations Management and OMi



nbi-om for Operations Management

The Operations Management functionality of the HPE Business Service Management (BSM) platform and OMi provide comprehensive event management, proactive performance monitoring; and automated alerting, reporting, and graphing for management operating systems, middleware, and application infrastructure. HPE NNMi—HPE BSM Operations Management/OMi consolidates events from a wide range of sources into a single view.

For information about purchasing BSM or OMi, contact your HP sales representative.

This chapter contains the following topics:

- "HPE NNMi—HPE BSM Operations Management/OMi Integration" on the next page
- "Enabling the HPE NNMi—HPE BSM Operations Management/OMi Integration" on page 42
- "Configuring NNMi to Close Incidents After the Corresponding BSM Events are Closed" on page 47
- "Using the HPE NNMi—HPE BSM Operations Management or OMi Integration" on page 48
- "Changing the HPE NNMi—HPE BSM Operations Management or OMi Integration" on page 51

- "Disabling the HPE NNMi—HPE BSM Operations Management or OMi Integration" on page 52
- "Troubleshooting the HPE NNMi—HPE BSM Operations Management Integration" on page 53
- "NNMi–HPOM Agent Destination Form Reference (BSM Operations Management Integration)" on page 57

HPE NNMi–HPE BSM Operations Management/OMi Integration

The HPE NNMi—HPE BSM Operations Management/OMi integration forwards NNMi management event incidents as SNMPv2c traps to the BSM Connector. The BSM Connector filters the NNMi traps and forwards them to the HPE BSM Operations Management event browser. The adapter configuration determines which BSM Operations Management event browser receives the forwarded incident.

The HPE NNMi—HPE BSM Operations Management/OMi integration can also forward the SNMP traps that NNMi receives to the BSM Connector.

The BSM Connector must be on the NNMi management server.

The HPE NNMi—HPE BSM Operations Management/OMi integration also provides for accessing the NNMi console from within the BSM Operations Management or OMi event browser.

TIP: This chapter describes the direct integration between NNMi and the BSM Operations Management or OMi event browser. For a comparison of these approaches to integrating NNMi with BSM Operations Management, see "Comparison of Approaches to Integrating NNMi with HPE BSM Operations Management or OMi" on page 7.

The HPE NNMi—HPE BSM Operations Management integration is a specific implementation of the NNMi northbound interface, which is described in the *NNMi Northbound Interface* chapter of the NNMi Deployment Reference.

The HPE NNMi—HPE BSM Operations Management/OMi integration consists of the following components:

- nnmi-hpom agent integration module
- nnmopcexport.ovpl tool

Value

The HPE NNMi—HPE BSM Operations Management/OMi integration provides event consolidation in the BSM Operations Management or OMi event browser for the network management, system management, and application management domains, so that users of the BSM Operations Management or OMi event browser can detect and investigate potential network problems.

The primary features of the integration are as follows:

- Automatic incident forwarding from NNMi to the BSM Connector. Forwarded incidents appear in the BSM Operations Management or OMi event browser.
- Access to the NNMi console from the BSM Operations Management or OMi event browser.
  - Open the NNMi **Incident** form in the context of a selected event.
  - Open an NNMi view (for example, the Layer 2 Neighbor view) in the context of a selected event and node.
  - Launch an NNMi tool (for example, status poll) in the context of a selected event and node.

Integrated Products

The information in this chapter applies to the following products:

- BSM with the HP Operations Management license

  or

  HP Operations Manager i (OMi)

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

- NNMi 10.20 on the Windows or Linux operating system only

NNMi and BSM/OMi must be installed on separate computers. The NNMi management server and the BSM/OMi server computer can be of the same or different operating systems.

The BSM Connector must be installed *after* NNMi installation. The BSM Connector must be on the NNMi management server. It is recommended to install the BSM Connector on the NNMi management server computer to avoid network problems such as high latency between NNMi and the BSM Connector.

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

Documentation

This chapter describes how to configure NNMi to communicate with the BSM Operations Management or OMi event browser.

The BSM documentation describes how to install and use the BSM Connector and the applications that access the NNMi console from the BSM Operations Management event browser.

- *BSM Application Administration Guide*
- *BSM Connector Installation and Upgrade Guide*
- *BSM Connector User Guide*
- *BSM Connector Help*
- BSM Operations Management Extensibility Guide

The OMi documentation describes how to install and use the BSM Connector and the applications that access the NNMi console from the OMi event browser.

- *OMi User Guide*
- *OMi Administration Guide*
- *OMi Extensibility Guide*

After installing the BSM Connector on the NNMi management server, you must run the following command:

On Windows: **%nnminstalldir%\lbin\changeUser.ovpl**

On Linux: **/opt/OV/lbin/changeUser.ovpl**

Enabling the HPE NNMi–HPE BSM Operations Management/OMi Integration

It is recommended that an experienced BSM Connector user complete the procedure for enabling the HPE NNMi—HPE BSM Operations Management/OMi integration.

NOTE: When NNMi integrates with the HPE Business Service Management (BSM) topology database, the HPE NNMi—HPE BSM Operations Management/OMi integration can associate incidents regarding NNMi-managed devices with BSM configuration items (CIs). This information is not available with the standard NNMi northbound interface. For more information, see "Configuration Item Identifiers" on page 49.

To enable the HPE NNMi—HPE BSM Operations Management/OMi integration, follow these steps:

1. On the NNMi management server, generate an SNMP trap policy file for the traps that NNMi forwards:
   a. Verify that the NNMi services are running:
      ```
      ovstatus -c
      ```
      All NNMi services should show the state RUNNING.

b. Generate the SNMP trap policy file by entering the following command:

```
nnmopcexport.ovpl -u <username> -p <password> \
-template "NNMi Management Events" -application "NNMi" \
-omi_policy -omi_hi
```

The values for ***<username>*** and ***<password>*** correspond to an NNMi console user with the Administrator role.

This command creates two files in the current directory:

- The `<UUID>_data` file is the SNMP trap policy file, where `<UUID>` is a universally unique identifier.
- The `<UUID>_header.xml` file identifies the `<UUID>_data` file to the BSM Connector.

CAUTION: Do not rename these output files, as doing so renders them unusable by the BSM Connector.

The SNMP trap policy file includes a policy condition for each management event and SNMP trap configuration in the current NNMi incident configuration. For information about customizing the output of this command, see the *nnmopcexport.ovpl* reference page, or the Linux manpage.

For information about the default policy conditions and customizing conditions, see "Using the HPE NNMi—HPE BSM Operations Management or OMi Integration" on page 48.

c. If you want to forward the NNMi severity information (that is, if you performed "Optional. (Only with the HP Operations agent 11.12 or higher) Additionally, configure the agent to forward NNMi severity to BSM:" on page 45), run the following commands:

On Windows:

a. `findstr /V SEVERITY <UUID>_data > <UUID>_data_new`

b. `robocopy /mov <UUID>_data_new <UUID>_data`

On Linux:

a. `grep -v SEVERITY <UUID>_data > <UUID>_data_new`

b. `mv <UUID>_data_new <UUID>_data`

2. Install and configure the BSM Connector:

Note: After installing the BSM Connector on the NNMi management server, you must run the following command:

On Windows: **%nnminstalldir%\lbin\changeUser.ovpl**

On Linux: **/opt/OV/lbin/changeUser.ovpl**

a. On the NNMi management server or a separate server, install the BSM Connector as described in the *BSM Connector Installation and Upgrade Guide*.

b. In BSM/OMi, configure the BSM Connector integration with BSM/OMi as described in the *BSM Application Administration Guide* or *OMi Administration Guide.*

> **TIP:** The HP Operations agent from HPOM and the BSM Connector can run simultaneously on one system. See the *BSM Connector User Guide* for more information.

c. Use the BSM Connector user interface to import the header and policy files created in "On the NNMi management server, generate an SNMP trap policy file for the traps that NNMi forwards:" on page 42 of this procedure.

   For more information, see *Working with BSM Connector> Policy Management> How to Import Policies* in the *BSM Connector Help*.

d. Use the BSM Connector user interface to activate the new policies.

   For more information, see *Working with BSM Connector > Policy Management > How to Activate and Deactivate Policies* in the *BSM Connector Help*.

3. Identify an available port for SNMP communications between NNMi and the BSM Connector.

   The BSM Connector will listen on this port for the SNMP traps that NNMi forwards to this port. While enabling the integration, this port number is used in both "On the server where the BSM Connector is installed, configure the agent inside the BSM Connector with a custom port for receiving SNMP traps from NNMi by entering the following commands:" on the next page (for the BSM Connector) and "On the NNMi management server, configure NNMi incident forwarding to the BSM Connector:" on the next page (for NNMi) of this procedure.

   > **TIP:** The SNMP communications port is different from the HTTP and HTTPS ports for the Apache Tomcat server you specified when using the BSM Connector Configuration Wizard during the post-installation phase.

   If the BSM Connector is installed on the NNMi management server, this port number must be different from the port on which NNMi receives SNMP traps. Identify an available port as follows:

   a. From the NNMi management server, run the **`nnmtrapconfig.ovpl -showProp`** command. Look for the current `trapPort` value in the command output. This value is typically 162, which is the standard UDP port for receiving SNMP traps. Do not use this `trapPort` value when configuring SNMP communications between NNMi and the BSM Connector.

b. Select a port for configuring SNMP communications between NNMi and the BSM Connector. A good practice is to use a port number similar to the value of `trapPort`. For example, if port 162 is not available, try port 5162.

c. From the NNMi management server, run the **`netstat -a`** command and search the output for the port you selected in "Select a port for configuring SNMP communications between NNMi and the BSM Connector. A good practice is to use a port number similar to the value of trapPort. For example, if port 162 is not available, try port 5162." above. If that port number does not appear in the output, it is probably available for the BSM Connector to use.

4. On the server where the BSM Connector is installed, configure the agent inside the BSM Connector with a custom port for receiving SNMP traps from NNMi by entering the following commands:

   a. Configure the agent:

      If using the HP Operations agent 11.00 or higher:

      ```
      ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> \
      -set SNMP_SESSION_MODE NETSNMP
      ```

      If using a version of the HP Operations agent older than 11.00:

      ```
      ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> \
      -set SNMP_SESSION_MODE NNM_LIBS
      ```

   b. *Optional.* (*Only with the HP Operations agent 11.12 or higher*) Additionally, configure the agent to forward NNMi severity to BSM:

      ```
      ovconfchg -ns eaagt.integration.nnm -set OPC_SNMP_SET_SEVERITY
      TRUE
      ```

      NOTE: You can forward the severity of the NNMi incidents to BSM Operations Management only if you use the HP Operations agent 11.12 or higher. Skip this step if you use a lower version of the HP Operations agent.

   c. Restart the agent:

      ```
      ovc -restart opctrapi
      ```

   For *`<custom_port>`*, use the port that you identified in "Identify an available port for SNMP communications between NNMi and the BSM Connector." on the previous page of this procedure.

5. On the NNMi management server, configure NNMi incident forwarding to the BSM Connector:

   a. In the NNMi console, open the **NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).

   b. Click **HPOM agent implementation**, and then click **New**.

      (If you have selected an available destination, click **Reset** to make the **New** button available.)

c. On the **NNMi–HPOM Agent Destination** form, select the **Enabled** check box to make the remaining fields on the form available.

d. Enter the information for connecting to the BSM Connector. The trap destination port is the port that you identified in "Identify an available port for SNMP communications between NNMi and the BSM Connector." on page 44 of this procedure.

   For information about these fields, see "BSM Connector Connection" on page 57.

e. Specify the sending options. Select the **HTTP** option for the **NNMi Console Access** field.

   For information about these fields, see "BSM Operations Management or OMi Integration Content" on page 58.

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

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

6. *Optional*. To make instructional text available on the BSM gateway server, complete the following steps:

   BSM/OMi must be installed with the Monitoring Automation component.

   a. Make sure the SNMP trap policy for which you want to view trap conditions contains help text.

   b. Import the SNMP trap policy using either of the following commands:

      - Windows:

        ```
        <BSM_Root_Directory>\opr\bin\ConfigExchange.bat -username
        <BSM_username> -password <password> -uploadOM -input <policy_
        header_file>
        ```

        OR

        ```
        <BSM_Root_Directory>\opr\bin\ConfigExchange.bat -username
        <BSM_username> -password <password> -uploadOM -input
        <directory_containing_policy_header_file>
        ```

      - Linux:

        ```
        <BSM_Root_Directory>/opr/bin/ConfigExchange -username <BSM_
        username> -password <password> -uploadOM -input <policy_
        header_file>
        ```

        OR

        ```
        <BSM_Root_Directory>/opr/bin/ConfigExchange -username <BSM_
        username> -password <password> -uploadOM -input <directory_
        ```

```
containing_policy_header_file>
```

The BSM/OMi user must have BSM RTSM or UCMDB administrative privileges.

The SNMP trap policy on the BSM Connector’s agent is imported to the BSM/OMi server.

Configuring NNMi to Close Incidents After the Corresponding BSM Events are Closed

You can configure NNMi to permit NNMi incidents to close automatically after the corresponding event is closed in HPE BSM Operations Management/OMi.

1. On the NNMi management server, run the following command:

   Windows: `%nnminstalldir%\bin\nmsconfigurebacksync.ovpl`

   Linux: `/opt/OV/bin/nmsconfigurebacksync.ovpl`

   When prompted to provide the user name and password, specify the credentials of an NNMi user with administrative privileges.

2. *Windows Only*: Run the following command from the `%ovinstalldir%` directory:

   ```
   newconfig\HPNmsCommon\scripts\nnm-configure-perl.ovpl -source
   newconfig\HPNmsCommon\perl\a -target nonOV\perl\a
   ```

3. Run the following command to restart the ombacksync process:

   `ovc -restart ombacksync`.

4. On the NNMi management server, use the `nnmopcexport.ovpl` script to regenerate each policy file for the new traps.

   After modifying these existing policies, the BSM Connector finds and runs new scripts that initiates automatic incident synchronization with HPE BSM Operations Management/OMi as it detects alerts being acknowledged.

CAUTION: If you reinstall NNMi, you must reinstall the BSM Connector and repeat "On the NNMi management server, run the following command:" above through "On the NNMi management server, use the nnmopcexport.ovpl script to regenerate each policy file for the new traps." above.

CAUTION: If you reinstall the BSM Connector, you must repeat "On the NNMi management server, run the following command:" above and "Run the following command to restart the ombacksync process:" above.

5. Import the policy files (*_header.xml and *_data) to the BSM Connector as described in the following steps:

   a. In the BSM Connector user interface, click in the tool bar.

      A file selection dialog box opens.

b. Navigate to the policy files and, for each policy, select both the header (*_header.xml) and the data (*_data) files.

c. Click **Open** to start the import process.

If the same policies already exist in BSM Connector, you are asked whether you would like to replace them with the newly imported policies.

The imported policies appear in the list of policies in the BSM Connector user interface. They are by default deactivated.

For more information, see the *BSM Connector User Guide*.

6. Activate the policy files as described in the following steps:

a. In the list of policies in the BSM Connector user interface, select the policies that you want to activate.

The activation state of at least one of the selected policies must be deactivated or activated (reactivate for new version). (If you include an already activated policy in your selection, the policy is ignored and not activated again.)

b. Click ◌ in the tool bar. The activation state changes to activated.

For more information, see the *BSM Connector User Guide*.

Using the HPE NNMi–HPE BSM Operations Management or OMi Integration

As discussed in the previous section, you can configure NNMi to permit NNMi incidents to close automatically after the corresponding event is closed in HPE BSM Operations Management or OMi. The HPE NNMi—HPE BSM Operations Management or OMi integration provides a two-way flow of NNMi management events and SNMP traps to and from BSM/OMi and the BSM Operations Management or OMi event browser. The NNMi SNMP trap policy determines how the BSM Operations Management or OMi event browser treats and displays the incoming traps. For example, you can change a policy condition to include the value of a trap custom attribute in the event title.

NOTE: NNMi sends only one copy of each management event or SNMP trap to the BSM Connector.

View the forwarded NNMi incidents in the BSM Operations Management or OMi event browser. Menu commands in the BSM Operations Management or OMi event browser provide access to NNMi views in the context of the selected event. Information embedded in each event supports this cross-navigation:

- The `nnmi.server.name` and `nnmi.server.port` custom attributes in the event identify the NNMi management server.

- The `nnmi.incident.uuid` custom attribute identifies the incident in the NNMi database.

In the BSM Operations Management or OMi event browser, the original source object appears in the **Object** field on the **Additional Info** tab and in the `nnm.source.name` custom attribute.

Configuration Item Identifiers

In HPE Business Service Management (BSM)/OMi and HPE Universal CMDB Software (HPE UCMDB), a configuration item (CI) is a database representation of a component in the IT environment. A CI can be a line of business, business process, application, server hardware, or a service.

When NNMi integrates with the BSM topology database or HPE UCMDB, NNMi shares CI information with BSM or HPE UCMDB for the devices that NNMi manages. In this case, the HPE NNMi—HPE BSM Operations Management integration can associate incidents regarding NNMi-managed devices with BSM or HPE UCMDB CIs. The SNMP trap policy conditions enable this association.

For information about the integrations with BSM and HPE UCMDB, see "Topology Integration with HP Universal CMDB" on page 13.

Health Indicators

Because the NNMi SNMP trap policy file was created with the `-omi_hi` option to `nnmopcexport.ovpl`, the policy file associates a health indicator with each standard NNMi management event in the SNMP trap policy file, as appropriate. (Not all management event types have health indicators.) The health indicator is available in the `EtiHint` custom attribute.

For the specific health indicators, see the SNMP trap policy file.

Default Policy Conditions

The default integration behavior varies with the integration content, as described here:

- NNMi management event incidents
  - The NNMi SNMP trap policy file includes conditions for all NNMi management event configurations defined in the NNMi incident configuration when the file was generated.
  - The events created from NNMi management events appear in the BSM Operations Management event browser.

  - These traps include the CI information described in "Configuration Item Identifiers" on the previous page.
  - The events created from these traps include health indicators described in "Health Indicators" on the previous page.
- Third-party SNMP traps
  - The NNMi SNMP trap policy file includes conditions for all SNMP trap configurations defined in the NNMi incident configuration when the file was generated.
  - The events created from third-party traps appear in the BSM Operations Management event browser.
  - These traps include the CI information described in "Configuration Item Identifiers" on the previous page.
  - The events created from these traps do not include health indicators.
  - If you configure the integration to forward all received SNMP traps and the BSM Operations Management or OMi event browser receives SNMP traps directly from devices that NNMi manages, the BSM Operations Management or OMi event browser receives device traps. You can set the policies to correlate SNMP traps from NNMi with those that the BSM Operations Management or OMi event browser receives directly from managed devices.
- Syslog
  - NNMi receives Syslogs from managed devices and forwards them to the BSM Connector.
- EventLifecycleStateClosed traps
  - The BSM Connector logs the events created from these traps. Generally, they do not appear in the BSM Operations Management or OMi event browser.
  - The NNMi SNMP trap policy file causes the BSM Connector to acknowledge the event that corresponds to the closed NNMi incident in the BSM Operations Management or OMi event browser.
- LifecycleStateChangeEvent traps
  - The NNMi SNMP trap policy file does not include conditions for processing these traps. The BSM Connector does not forward these traps to the BSM Operations Management or OMi event browser.
- EventDeleted traps

  - The NNMi SNMP trap policy file does not include conditions for processing these traps. The BSM Connector does not forward these traps to the BSM Operations Management or OMi event browser.

- Correlation notification traps
  - The BSM Connector logs the events created from these traps. They do not appear in the BSM Operations Management or OMi event browser.
  - The BSM Connector processes the NNMi correlation traps to replicate NNMi incident correlation in the BSM Operations Management or OMi event browser.

Customizing Policy Conditions

Use the BSM Connector user interface to customize the default policy conditions. For more information, see *Integrating Data With BSM Connector > SNMP Trap Policies > SNMP Policy User Interface > Configuring Rules in SNMP Policies* in the *BSM Connector help*.

More Information

For more information about the HPE NNMi—HPE BSM Operations Management or OMi integration, see the following references:

- For descriptions of the trap types that the integration sends to the BSM Connector, see the *Using the NNMi Northbound Interface* section contained in the *NNMi Northbound Interface* chapter of the NNMi Deployment Reference.
- For information about the format of the traps that NNMi sends to the BSM Connector, see the `hp-nnmi-nbi.mib` file.
- For detailed information about using the HPE NNMi—HPE BSM Operations Management integration, see the BSM Operations Management Extensibility Guide.

Changing the HPE NNMi–HPE BSM Operations Management or OMi Integration

This section contains the following topics:

- "Update the SNMP Trap Policy Conditions for New NNMi Traps" below
- "Change the Configuration Parameters" on the next page

Update the SNMP Trap Policy Conditions for New NNMi Traps

If new SNMP trap incident configurations have been added to NNMi since the integration was configured, follow these steps:

1. On the NNMi management server, use the `nnmopcexport.ovpl` command to create an SNMP trap policy file for the new traps.

   For the `-template` option, specify a name that is different from the names of the existing SNMP trap policy files.

   Use the `-omi_policy` and `-omi_hi` options.

   You can limit the file contents to a specific author or OID prefix value. For more information, see the *nnmopcexport.ovpl* reference page, or the Linux manpage.
2. Use the BSM Connector user interface to import and activate the new header and policy files.

Alternatively, you can re-create the SNMP trap policy file for all NNMi management events and SNMP traps. If you take this approach, delete the old policies from the BSM Connector user interface.

> **NOTE:** If the BSM Connector configuration includes multiple policy conditions for one NNMi incident, messages appear in the BSM Operations Management or OMi event browser.

Change the Configuration Parameters

To change the integration configuration parameters, follow these steps:

1. In the NNMi console, open the **NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **HPOM agent implementation**.
3. Select a destination, and then click **Edit**.
4. Modify the values as appropriate.

   For information about the fields on this form, see "NNMi–HPOM Agent Destination Form Reference (BSM Operations Management Integration)" on page 57.
5. Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Disabling the HPE NNMi–HPE BSM Operations Management or OMi Integration

No SNMP trap queuing occurs while a destination is disabled.

To discontinue the forwarding of NNMi incidents to the BSM Connector, follow these steps:

1. In the NNMi console, open the **NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **HPOM agent implementation**.
3. Select a destination, and then click **Edit**.

   Alternatively, click **Delete** to entirely remove the configuration for the selected destination.
4. Clear the **Enable Integration** check box at the top of the form, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Optionally deactivate or delete the SNMP trap policy as described in the *BSM Connector help*.

Troubleshooting the HPE NNMi–HPE BSM Operations Management Integration

This section contains the following topics:

- "BSM Operations Management Event Browser Contains No Forwarded Incidents" below
- "BSM Operations Management Event Browser Contains Only Some Forwarded Incidents" on page 56

BSM Operations Management Event Browser Contains No Forwarded Incidents

TIP: In the following procedure, the `OVBIN` environment variable refers to the `bin` directory containing the commands for configuring the agent inside the BSM Connector. The `OVBIN` environment variable defaults to the following value:

- *Windows*: `<drive>\Program Files (x86)\HP\HP BTO Software\bin`
- *Linux*: `/opt/OV/bin`

If the BSM Operations Management event browser does not contain any incidents from NNMi, follow these steps:

1. On the server where the BSM Connector is installed, verify the agent configuration:
   - *Windows*:

     ```
     %OVBIN%\ovconfget eaagt
     ```
   - *Linux*:

     ```
     $OVBIN/ovconfget eaagt
     ```

The command output should include the following information:

- *Windows*:

  ```
  SNMP_SESSION_MODE=NNM_LIBS
  SNMP_TRAP_PORT=<custom_port>
  ```

- *Linux*:

  ```
  SNMP_SESSION_MODE=NO_TRAPD
  SNMP_TRAP_PORT=<custom_port>
  ```

The value of `<custom_port>` should *not* be 162 and should match the value of the **Port** field on the **NNMi–HPOM Agent Destination** form.

2. Evaluate the agent configuration by considering the results from "On the server where the BSM Connector is installed, verify the agent configuration:" on the previous page:

   - If the agent configuration is as expected, continue with "On the server where the BSM Connector is installed, verify that the agent is running:" below of this procedure.

   - If the `SNMP_SESSION_MODE` parameter is not set correctly, repeat "On the server where the BSM Connector is installed, configure the agent inside the BSM Connector with a custom port for receiving SNMP traps from NNMi by entering the following commands:" on page 45 until the `ovconfget` command returns the expected results.

   - If the value of `<custom_port>` is 162 or does not match the value of the **Port** field on the **NNMi–HPOM Agent Destination** form, repeat "Identify an available port for SNMP communications between NNMi and the BSM Connector." on page 44 through "On the NNMi management server, configure NNMi incident forwarding to the BSM Connector:" on page 45, as appropriate, until the `ovconfget` command returns the expected results.

3. On the server where the BSM Connector is installed, verify that the agent is running:

   - *Windows*:

     `%OVBIN%\opcagt -status`

   - *Linux*:

     `$OVBIN/opcagt -status`

   The command output should include an opctrapi entry similar to the following example:

   ```
   opctrapi  OVO SNMP Trap Interceptor  AGENT,EA  (4971)  Running
   ```

   If the output is not as expected, restart the agent:

```
ovc -restart opctrapi
```

4. On the server where the BSM Connector is installed, verify that the agent is listening on the expected SNMP trap port:

   a. Run the following command:

      - *Windows*: **`netstat -an | findstr`** *<custom_port>*
      - *Linux*: **`netstat -an | grep`** *<custom_port>*

      Where *`<custom_port>`* is the value of `SNMP_TRAP_PORT` from "On the server where the BSM Connector is installed, verify the agent configuration:" on page 53 of this procedure.

   b. Verify that the output includes the state LISTENING or LISTEN.

      If the output is not as expected, restart the agent:

      ```
      ovc -restart opctrapi
      ```

5. On the server where the BSM Connector is installed, verify that the SNMP trap policy file for NNMi has been deployed to the BSM Connector on the NNMi management server:

   - *Windows*:

     ```
     %OVBIN%\ovpolicy -list
     ```

   - *Linux*:

     ```
     $OVBIN/ovpolicy -list
     ```

   The command output should include an entry similar to the following example:

   ```
   Type     Name                           Status     Version
   ------------------------------------------------------------------
   trapi    "NNMi Management Events"    enabled    0001.0000
   ```

   The value of the `Name` field is the name of the SNMP trap policy file from the `-template` option to `nnmopcexport.ovpl` in "On the NNMi management server, generate an SNMP trap policy file for the traps that NNMi forwards:" on page 42.

6. On the server where the BSM Connector is installed, check the agent log file for any errors. The log file can be found in the following location:

   - *Windows*:`%ovdatadir%\log\System.txt`
   - *Linux*: `/var/opt/OV/log/System.txt`

7. Verify that the BSM Connector is receiving traps:

   a. Verify that the BSM Connector can send events to the BSM Operations Management event browser. To do this, create a simple `open message interface` policy using the BSMC policy management UI. You must have **forward unmatched events to active browser** enabled on the **options** tab of the policy. **Save and activate** this new `open message interface` policy. After activating this `open message interface` policy, you can send events to the BSM Operations Management event browser using the `opcmsg` command.

b. Enable tracing of the BSM Connector to determine whether the traps arrive at the BSM Connector. To do this, in the `options` tab of the appropriate SNMP policy, there is the possibility to configure the policy to log incoming trap events. These events are logged on the local node in the following log file:

   - *Windows*: `%ovdatadir%\log\OpC\opcmsglg`
   - *Linux*: `/var/opt/OV/log/OpC/opcmsglg`

8. Verify that NNMi is forwarding management events to the BSM Connector.

   For more information, see the *Troubleshooting the NNMi Northbound Interface* section contained in the *NNMi Northbound Interface* chapter of the NNMi Deployment Reference.

BSM Operations Management Event Browser Contains Only Some Forwarded Incidents

If one or more NNMi incidents do not appear in the BSM Operations Management event browser, follow these steps:

1. On the NNMi management server, verify that the SNMP trap policy does not suppress the trap.
2. On the BSM server, verify that BSM Operations Management is running.

   NOTE: On a windows BSM server, there is a web page showing the status of the BSM server. Use the **Start** > **All Programs** > **HP Business Service Management** > **Administration** -> **HP Business Service Management Status** menu to view the status.

   If the BSM server shuts down, the BSM Connector queues received traps. The BSM Connector forwards the queued traps when the BSM Operations Management event browser becomes available.

   If the BSM Connector shuts down, the forwarded traps are lost. NNMi does not resend traps.

3. On the NNMi management server, verify that the NNMi processes are running:

   ```
   ovstatus -c
   ```

   Any traps sent to NNMi while it is shut down are lost.

NNMi-HPOM Agent Destination Form Reference (BSM Operations Management Integration)

The **NNMi–HPOM Agent Destination** form contains the parameters for configuring communications between NNMi and the BSM Connector. This form is available from the **Integration Module Configuration** workspace. (On the **NNMi–HPOM Integration Selection** form, click **HPOM agent implementation**. Click **New**, or select a destination, and then click **Edit**.)

> **NOTE:** Only NNMi users with the Administrator role can access the **NNMi–HPOM Agent Destination** form.

The **NNMi–HPOM Agent Destination** form collects information for the following areas:

- "BSM Connector Connection" below
- "BSM Operations Management or OMi Integration Content" on the next page
- "BSM Connector Destination Status Information" on page 61

To apply changes to the integration configuration, update the values on the **NNMi–HPOM Agent Destination** form, and then click **Submit**.

BSM Connector Connection

"Table 5 BSM Connector Connection Information" below lists the parameters for configuring the connection to the BSM Connector.

Table 5 BSM Connector Connection Information

Field	Description
Host	The fully-qualified domain name (preferred) or the IP address of the NNMi management server, which is the system on which the BSM Connector receives SNMP traps from NNMi. The integration supports the following methods for identifying the BSM Connector host: • **NNMi FQDN** NNMi manages the connection to the BSM Connector and the **Host** field becomes read-only. This is the default and recommended configuration. • **Use Loopback** Do not use this option.

Table 5 BSM Connector Connection Information, continued

Field	Description
	- **Other** Do not use this option. **NOTE:** If the NNMi management server participates in NNMi application failover, see *Application Failover and the NNMi Northbound Interface* in the *NNMi Northbound Interface* chapter of the NNMi Deployment Reference.
Port	The UDP port where the BSM Connector receives SNMP traps. Enter the port number specific to the BSM Connector. This value is the port that you identified in "Identify an available port for SNMP communications between NNMi and the BSM Connector." on page 44. To determine the port, run the **`ovconfget eaagt`** command on the server where the BSM Connector is installed. The trap port is the value of the `SNMP_TRAP_PORT` variable. **NOTE:** This port number must be different from the port on which NNMi receives SNMP traps, as set in the **SNMP Port** field on the **Communication Configuration** form in the NNMi console.
Community String	A read-only community string for the BSM Connector to receive traps. For the HPE NNMi—HPE BSM Operations Management integration, use the default value, which is `public`.

BSM Operations Management or OMi Integration Content

"Table 6 BSM Operations Management Integration Content Configuration Information" below lists the parameters for configuring which content NNMi sends to the BSM Connector.

Table 6 BSM Operations Management Integration Content Configuration Information

Field	Description
Incidents	The incident forwarding sending options. - **Management**

Table 6 BSM Operations Management Integration Content Configuration Information, continued

Field	Description
	NNMi forwards only NNMi-generated management events to the BSM Connector. • **SNMP 3rd Party Trap** NNMi forwards only SNMP traps that NNMi receives from managed devices to the BSM Connector. • **Syslog** NNMi forwards both NNMi-generated management events and SNMP traps that NNMi receives from managed devices to the BSM Connector. This is the default configuration. For more information, see the *NNMi Northbound Interface* chapter of the NNMi Deployment Reference.
Lifecycle State Changes	The incident change notification sending options. • **Enhanced Closed** NNMi sends an incident closed trap to the BSM Connector for each incident that changes to the CLOSED lifecycle state. This is the default configuration. • **State Changed** NNMi sends an incident lifecycle state changed trap to the BSM Connector for each incident that changes to the IN PROGRESS, COMPLETED, or CLOSED lifecycle state. • **Both** NNMi sends an incident closed trap to the BSM Connector for each incident that changes to the CLOSED lifecycle state. Additionally, the integration sends an incident lifecycle state changed trap to the BSM Connector for each incident that changes to the IN PROGESS, COMPLETED, or CLOSED lifecycle state. **NOTE:** In this case, each time an incident changes to the CLOSED lifecycle state, the integration sends two notification traps: an incident closed trap and an incident lifecycle state changed trap.
Correlations	The incident correlation sending options. • **None** NNMi does not notify the BSM Connector of incident

Table 6 BSM Operations Management Integration Content Configuration Information, continued

Field	Description
	correlations resulting from NNMi causal analysis. This is the default configuration. • **Single** NNMi sends a trap for each parent-child incident correlation relationship resulting from NNMi causal analysis. • **Group** NNMi sends one trap per correlation that lists all child incidents correlated to a parent incident. **NOTE**: HP recommends you select this value if you also want events correlated in BSM.
Deletions	The incident deletion sending options. • **Don't Send** NNMi does not notify the BSM Connector when incidents are deleted in NNMi. This is the default configuration. • **Send** NNMi sends a deletion trap to the BSM Connector for each incident that is deleted in NNMi.
NNMi Console Access	The connection protocol specification in the URL for browsing to the NNMi console from the BSM Operations Management or OMi event browser. The traps that NNMi sends to the BSM Connector include the NNMi URL in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). The integration requires an HTTPS or HTTP connection to the NNMi console. Select the **HTTPS** or **HTTP** option.
Incident Filters	A list of object identifiers (OIDs) on which the integration filters the events sent to the BSM Connector. Each filter entry can be a valid numeric OID (for example, .1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9) or OID prefix (for example, .1.3.6.1.6.3.1.1.5.*). Select one of the following options: • **None** NNMi sends all events to the BSM Connector. This is the default configuration. • **Include**

Table 6 BSM Operations Management Integration Content Configuration Information, continued

Field	Description
	NNMi sends only the specific events that match the OIDs identified in the filter. - **Exclude** NNMi sends all events except for the specific events that match the OIDs identified in the filter. Specify the incident filter: - To add a filter entry, enter the text in the lower text box, and then click **Add**. - To delete a filter entry, select that entry from the list in the upper box, and then click **Remove**.

BSM Connector Destination Status Information

"Table 7 BSM Connector Destination Status Information" below lists the read-only status information for the BSM Connector. This information is useful for verifying that the integration is working correctly.

Table 7 BSM Connector Destination Status Information

Field	Description
Trap Destination IP Address	The IP address to which the BSM Connector destination host name resolves. This value is unique to this destination.
Uptime (seconds)	The time (in seconds) since the northbound component was last started. The traps that NNMi sends to the BSM Connector include this value in the sysUptime field (1.3.6.1.2.1.1.3.0). This value is the same for all integrations that use the NNMi northbound interface. To see the latest value, either refresh or close and re-open the form.
NNMi URL	The URL for connecting to the NNMi console. The traps that NNMi sends to the BSM Connector include this value in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). This value is unique to this northbound destination.

NNMi Visualizations

The HPE Business Service Management (BSM) platform and OMi provide tools for managing the availability of applications in production, monitoring system performance, monitoring infrastructure performance, and proactively resolving problems when they arise.

For information about purchasing BSM or OMi, contact your HP sales representative.

This chapter contains the following topics:

- "MyBSM Portal" below
- "Configuring an HTTPS Connection" on page 64
- "NNMi Data Available from BSM End User Management Reports" on page 76
- "Enabling NNMi Visualizations from BSM or OMi" on page 79

For information about NNMi console views launched from events in the BSM Operations Management event browser, see "Using the HPE NNMi—HPE BSM Operations Management or OMi Integration" on page 48.

MyBSM Portal

MyBSM is a portal-based dashboard environment for viewing data across the HP Software portfolio. The MyBSM portal provides a collection of portal pages and portlets that display information relevant to a users specific business task

The MyBSM administrator sets up pages that include components that are of interest to specific users or groups of users. The MyBSM workspace provides smooth interactions between different BSM applications and reports.

> **NOTE:** There is a single limitation integrating multiple NNMi instances with one BSM: While the event and topology integrations function as expected, you should consider the functionality of other NNMi components in the MyBSM portal. These NNMi components are shown in "NNMi Components Available in MyBSM" below. For the MyBSM integration only, you are limited to communicating with a single (pre-configured in BSM) NNMi instance.

To access the NNMi components, you must have the appropriate licenses installed. NNMi components are only displayed if you have configured a connection to an NNMi management server (**Admin** >**Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations** > **Integrations with other applications** > **HP NNM**).

NNMi Components Available in MyBSM

The BSM component gallery includes the following NNMi components:

- Open Key Incidents

  Shows the incidents that are most important to network operators, and that often require more immediate action.
- Layer 2 Neighbor View

  Shows a map view of a selected device and its connector devices within a specified number of hops from the selected device. This view is useful for understanding the switch connectivity between devices.
- Layer 3 Neighbor View

  Shows a map view of a selected device and it connector devices within a specified number of hops from the selected device. This view is useful for understanding the router connectivity between devices.
- MPLS VPN Inventory

  This is an enterprise customer view of how their sites are connected using service provided MPLS networks.
- Overall Network Health (Node Group Overview)

  Shows a map containing all (top-level) node groups that do not have parent node groups.
- Overall Network Health

  Shows a node group map of the router connectivity in your network.
- Path View

  Shows the path view between two selected nodes.
- Router Redundancy Groups Inventory

  Shows the available router redundancy groups created by the NNMi administrator. Each router redundancy group is a set of two or more routers that use one or more virtual IP addresses to help ensure that information packets reach their intended destination.

Viewing the NNMi Components in MyBSM

To view the NNMi components in MyBSM, follow these steps:

1. If you have not already done so, configure a connection from BSM to NNMi as described in "Enabling NNMi Visualizations from BSM or OMi" on page 79.
2. If you have not already done so, enable single sign-on between BSM and NNMi as described in "Configuring Single Sign-On Between NNMi and BSM, OMi, or UCMDB" on page 18.
3. If you have not already done so, configure NNMi to push topology information directly to the RTSM or UCMDB as described in "Enabling the HPE NNMi–HPE BSM/OMi/UCMDB Topology Integration" on page 15.

> **NOTE:** If you are configuring NNMi to push topology information to UCMDB, ensure the required CIs and relationships are pushed from UCMDB to BSM using the *UCMDB Data Flow Management Guide* which is included on the UCMDB product media. This manual is also available for the UCMDB product at:
> http://h20230.www2.hp.com/selfsolve/manuals

4. Add the NNMi components to the MyBSM portal:
   a. Within a user-defined MyBSM page, open the **Component Gallery**.
   b. Select one of the NNMi components and add it to your page.

   For details, see *How to Create Your MyBSM Workspace* in the *HP BSM Using MyBSM Guide*.

My Workspace in OMi

In OMi 10.00 (and higher), My Workspace offers the same features as MyBSM. When integrated with NNMi, My Workspace of OMi shows the same NNMi components as MyBSM.

Configuring an HTTPS Connection

To configure an SSL connection to BSM or OMi, follow the steps documented in this topic.

NNMi 10.20 introduces a stronger, more secure certificate scheme with the help of `keystore` and `truststore` files in the PKCS #12 format. In all new installations, PKCS #12 format-based certificate scheme is enabled by default. On systems where you upgraded NNMi from an older versions, you may have the old scheme of certificate management.

To see the configuration procedure with the certificates in the PKCS #12 format, see Configure with the nnm-key.p12 File.

To see the configuration procedure with the certificates in the old format, see Configure with the nnm.keystore File.

Configure with the nnm-key.p12 File

1. On the BSM or OMi gateway server, in a command window, change to the following directory:
   - *Windows*: `<drive>:\HPBSM\JRE64\bin`
   - *Linux*: `/opt/HP/BSM/JRE64/bin`

2. If you want to use a self-signed certificate, you must generate a new 2048-bit certificate by running the following command:
   - *On Windows:*
     keytool -genkey -keyalg rsa -keysize 2048 -alias <*alias_name*> **-keystore** <*Install_Dir*>**\odb\conf\security\server.keystore -validity "7200" -dname** <*distinguished_name*>

   - *On Linux:*
     ./keytool -genkey -keyalg rsa -keysize 2048 -alias <*alias_name*> **-keystore** <*Install_Dir*>**/odb/conf/security/server.keystore -validity "7200" -dname** <*distinguished_name*>

     In this instance, <*Install_Dir*> is the directory where you installed BSM or OMi; <*distinguished_name*> is the distinguished name of the gateway server.

3. If you want to use a CA-signed certificate, follow these steps to a Certificate Signing Request (CSR) file:
   a. Run the following command:
      - *On Windows:*
        keytool -keystore <*Install_Dir*>**\odb\conf\security\server.keystore -certreq -storepass hppass -alias** <*alias_name*> **-filename** <*cert_file_name*>
      - *On Linux:*
        ./**keytool -keystore** <*Install_Dir*>**/odb/conf/security/server.keystore -certreq -storepass hppass -alias** <*alias_name*> **-filename** ***<cert_file_name>***

        In this instance, <*Install_Dir*> is the directory where you installed BSM or OMi; <*cert_file_name*> is the name of the certificate file; <*alias_name*> is the alias name of the CA-signed certificate.

   b. Send the CSR to your CA signing authority which signs and returns the certificate files.

4. Run the command shown in step 5, substituting `server.truststore` for `server.keystore`:
   - *Windows*:
     ```
     keytool.exe -import -alias <NNMi_FQDN>.selfsigned -keystore
     <drive>:\HPBSM\odb\conf\security\server.truststore -storepass
     hppass -trustcacerts -file <drive>:\bsm_temp\nnmicert
     ```

   - *Linux*:
     ```
     keytool -import -alias <NNMi_FQDN>.selfsigned -keystore
     /opt/HP/BSM/odb/conf/security/server.truststore -storepass
     hppass -trustcacerts -file /bsm_tmp/nnmicert
     ```

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=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16
11:23:26 EET 2111
Certificate fingerprints:
     MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
     SHA1:
42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
     Signature algorithm name: SHA1withRSA
     Version: 1
Trust this certificate? [no]: yes
Certificate was added to keystore
```

5. To add the NNMi certificate to JRE, run the following command:
   - *Windows*:
     keytool.exe -import -alias <*NNMi_FQDN*>.selfsigned -keystore <*drive*>:\HPBSM\JRE\lib\security\cacerts -storepass changeit -trustcacerts -file <*drive*>:\bsm_temp\nnmicert

   - *Linux*:
     keytool -import -alias <*NNMi_FQDN*>.selfsigned -keystore /opt/HP/BSM/JRE/lib/security/cacerts -storepass changeit -trustcacerts -file /bsm_tmp/nnmicert

   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=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16
11:23:26 EET 2111
Certificate fingerprints:
     MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
     SHA1:
42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
     Signature algorithm name: SHA1withRSA
     Version: 1
Trust this certificate? [no]: yes
Certificate was added to keystore
```

6. To add the NNMi certificate to JRE64, run the following command:
   - *Windows*:
     ```
     keytool.exe -import -alias <NNMi_FQDN>.selfsigned -keystore
     <drive>:\HPBSM\JRE64\lib\security\cacerts -storepass changeit
     -trustcacerts -file <drive>:\bsm_temp\nnmicert
     ```
   - *Linux*:
     ```
     keytool -import -alias <NNMi_FQDN>.selfsigned -keystore
     /opt/HP/BSM/JRE64/lib/security/cacerts -storepass changeit
     -trustcacerts -file /bsm_tmp/nnmicert
     ```

   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=hpbsm_server.example.com
   Issuer: CN=hpbsm_server.example.com
   Serial number: 4d525d0e
   Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16
   11:23:26 EET 2111
   Certificate fingerprints:
        MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
        SHA1:
   42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
        Signature algorithm name: SHA1withRSA
        Version: 1
   Trust this certificate? [no]: yes
   Certificate was added to keystore
   ```
7. To import the BSM or OMi certificates into the NNMi management server, complete the following steps:

   a. Run the following command on the BSM or OMi gateway server:
      - *Windows*:
        ```
        keytool.exe -export -alias hpcert -file <path>\keystore
        -keystore <drive>:\HPBSM\odb\conf\security\server.keystore
        -storepass hppass
        ```
      - *Linux*:
        ```
        keytool.exe -export -alias hpcert -file <path>/keystore
        -keystore /opt/HP/BSM/odb/conf/security/server.keystore
        -storepass hppass
        ```

      After the command finishes, the BSM or OMi keystore certificate is stored in the specified `keystore` file.

   b. Run the following command on the BSM or OMi gateway server:

- *Windows*:

  ```
  keytool.exe -export -alias clientcert -file <path>\truststore
  -keystore <drive>:\HPBSM\odb\conf\security\server.truststore
  -storepass hppass
  ```

- *Linux*:

  ```
  keytool -export -alias clientcert -file <path>/truststore
  -keystore /opt/HP/BSM/odb/conf/security/server.truststore
  -storepass hppass
  ```

After the command finishes, the BSM or OMi truststore certificate is stored in the specified `truststore` file.

c. Copy the `truststore` file created in step b to a temporary directory on the NNMi management server. In the remaining commands, these files are shown as residing on the NNMi management server in the following locations:

- *Windows*:

  ```
  <drive>:\nnmi_temp\keystore
  <drive>:\nnmi_temp\truststore,
  ```

- *Linux*:

  ```
  /nnmi_tmp/keystore
  /nnmi_tmp/truststore
  ```

d. To merge the truststore files, run the following command on the NNMi management server:

- *Windows*:

  ```
  %nnminstalldir%\bin\nnmkeytool.ovpl -import -alias hpcert -
  keystore %NnmDataDir%\shared\nnm\certificates\nnm-key.p12
  -storetype PKCS12 -storepass nnmkeypass -file <drive>:\nnmi_
  temp\keystore
  ```

- *Linux*:

  ```
  /opt/OV/bin/nnmkeytool.ovpl -import -alias hpcert -keystore
  $NnmDataDir/shared/nnm/certificates/nnm.keystore
  -storetype PKCS12 -storepass nnmkeypass -file /nnmi_
  tmp/keystore
  ```

e. Complete this step only if BSM or OMi uses one or more certificate authority (CA) signed certificates (not a self-signed certificate). Import the CA root certificate, as well as any CA intermediate certificates, into the NNMi trust store.

Import each CA certificate separately. For example, to import the CA root certificate and one CA intermediate certificate, run the following commands on the NNMi management server:

- *Windows*:

  ```
  %nnminstalldir%\bin\nnmkeytool.ovpl -import -alias <bsm_ca_
  root_cert> -keystore
  ```

```
    %NnmDataDir%\shared\nnm\certificates\nnm-trust.p12
    -storetype PKCS12 -storepass ovpass -file
    <drive>:\temp\keystore
    ```

    -
      ```
      /opt/OV/bin/nnmkeytool.ovpl -alias <bsm_ca_intermediate_cert>
      -keystore $NnmDataDir/shared/nnm/certificates/nnm-trust.p12
      -storetype PKCS12 -storepass ovpass -file /tmp/keystore
      ```
    - *Linux*:
      ```
      /opt/OV/bin/nnmkeytool.ovpl -import -alias <bsm_ca_
      intermediate_cert>
      -keystore %NnmDataDir%\shared\nnm\certificates\
      nnm-trust.p12 -storetype PKCS12 -storepass ovpass -file
      <drive>:\temp\keystore
      ```

    -
      ```
      /opt/OV/bin/nnmkeytool.ovpl -import -alias <bsm_ca_
      intermediate_cert> -keystore
      $NnmDataDir/shared/nnm/certificates/nnm-trust.p12
      -storetype PKCS12 -storepass ovpass -file /tmp/keystore
      ```

8. *Optional*: Run the following command sequence on the NNMi management server:

   a. `ovstop`

   b. `ovstart`

9. *Optional*: Run the following commands on both the NNMi management server and the BSM or OMi gateway server. Compare the outputs to make sure the keystore certificates reside\ on both servers:

   - *NNMi management server*:
     - *Windows*:
       ```
       %nnminstalldir%\bin\nnmkeytool.ovpl -list -keystore
       %NnmDataDir%\shared\nnm\certificates\nnm-key.p12
       -storetype PKCS12 -storepass nnmkeypass -v
       ```
     - *Linux*:
       ```
       /opt/OV/bin/nnmkeytool.ovpl -list -keystore
       /var/opt/OV/shared/nnm/certificates/nnm-key.p12 -storetype
       PKCS12 -storepass nnmkeypass -v
       ```

   - *BSM or OMi gateway server*:
     - *Windows*:
       ```
       keytool.exe -list -keystore
       <drive>:\HPBSM\odb\conf\security\server.keystore
       -storepass hppass -v
       ```
     - *Linux*:
       ```
       keytool -list -keystore
       /opt/HP/BSM/odb/conf/security/server.keystore
       -storepass hppass -v
       ```

10. Check the date range to verify the certificate is still valid.

Configure with the nnm.keystore File

1. Export the NNMi certificate from the `nnm.keystore` file using the following command:
   - *Windows*:
     `%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -export -alias <NNMi_FQDN>.selfsigned -file <drive>:\temp\nnmicert -keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore -storepass nnmkeypass`

     > **NOTE:** If you include the full path to the `keytool.exe` command when you run it, you might see command errors due to unexpected spaces residing in the command string. To remedy this, enclose the path plus the `keytool.exe` command in quotation marks. For example, use "C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\hpsw\bin\keytool.exe" to avoid command errors.

   - *Linux*:
     `$NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -export -alias <NNMi_FQDN>.selfsigned -file /tmp/nnmicert -keystore $NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass`
2. Verify that you see the `Certificate stored in file <path_and_cert_file>` message.
3. Copy the NNMi certificate file created in "Configuring an HTTPS Connection" on page 64 to a temporary directory on the BSM or OMi gateway server. In the remaining commands, this file is shown as residing on the BSM or OMi gateway server in the following location:
   - *Windows*: `<drive>:\bsm_temp\nnmicert`
   - *Linux*: `/bsm_tmp/nnmicert`
4. On the BSM or OMi gateway server, in a command window, change to the following directory:
   - *Windows*: `<drive>:\HPBSM\JRE64\bin`
   - *Linux*: `/opt/HP/BSM/JRE64/bin`
5. Run the following command:
   - *Windows*:
     `keytool.exe -import -alias <NNMi_FQDN>.selfsigned -keystore`

```
<drive>:\HPBSM\odb\conf\security\server.keystore -storepass
hppass -trustcacerts -file <drive>:\bsm_temp\nnmicert
```

- *Linux*:
  ```
  keytool -import -alias <NNMi_FQDN>.selfsigned -keystore
  /opt/HP/BSM/odb/conf/security/server.keystore -storepass hppass
  -trustcacerts -file /bsm_tmp/nnmicert
  ```

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=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
   Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16
11:23:26 EET 2111
Certificate fingerprints:
     MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
     SHA1:
42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
     Signature algorithm name: SHA1withRSA
     Version: 1
Trust this certificate? [no]: yes
Certificate was added to keystore
```

6. Run the command shown in step 5, substituting `server.truststore` for `server.keystore`:

   - *Windows*:
     ```
     keytool.exe -import -alias <NNMi_FQDN>.selfsigned -keystore
     <drive>:\HPBSM\odb\conf\security\server.truststore -storepass
     hppass -trustcacerts -file <drive>:\bsm_temp\nnmicert
     ```

   - *Linux*:
     ```
     keytool -import -alias <NNMi_FQDN>.selfsigned -keystore
     /opt/HP/BSM/odb/conf/security/server.truststore -storepass
     hppass -trustcacerts -file /bsm_tmp/nnmicert
     ```

   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=hpbsm_server.example.com
   Issuer: CN=hpbsm_server.example.com
   Serial number: 4d525d0e
   Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16
   ```

```
11:23:26 EET 2111
Certificate fingerprints:
     MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
     SHA1:
42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
     Signature algorithm name: SHA1withRSA
     Version: 1
Trust this certificate? [no]: yes
Certificate was added to keystore
```

7. To add the NNMi certificate to JRE, run the following command:
   - *Windows*:
     keytool.exe -import -alias <*NNMi_FQDN*>.selfsigned -keystore <*drive*>:\HPBSM\JRE\lib\security\cacerts -storepass changeit -trustcacerts -file <*drive*>:\bsm_temp\nnmicert
   - *Linux*:
     keytool -import -alias <*NNMi_FQDN*>.selfsigned -keystore /opt/HP/BSM/JRE/lib/security/cacerts -storepass changeit -trustcacerts -file /bsm_tmp/nnmicert

   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=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16
11:23:26 EET 2111
Certificate fingerprints:
     MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
     SHA1:
42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
     Signature algorithm name: SHA1withRSA
     Version: 1
Trust this certificate? [no]: yes
Certificate was added to keystore
```

8. To add the NNMi certificate to JRE64, run the following command:
   - *Windows*:
     keytool.exe -import -alias <*NNMi_FQDN*>.selfsigned -keystore <*drive*>:\HPBSM\JRE64\lib\security\cacerts -storepass changeit -trustcacerts -file <*drive*>:\bsm_temp\nnmicert

- *Linux*:
  keytool -import -alias <*NNMi_FQDN*>.selfsigned -keystore /opt/HP/BSM/JRE64/lib/security/cacerts -storepass changeit -trustcacerts -file /bsm_tmp/nnmicert

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=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16
11:23:26 EET 2111
Certificate fingerprints:
     MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
     SHA1:
42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
     Signature algorithm name: SHA1withRSA
     Version: 1
Trust this certificate? [no]: yes
Certificate was added to keystore
```

9. To import the BSM or OMi certificates into the NNMi management server, complete the following steps:
   a. Run the following command on the BSM or OMi gateway server:
      - *Windows*:
        keytool.exe -export -alias hpcert -file <*path*>\keystore -keystore <*drive*>**:\HPBSM\odb\conf\security\server.keystore -storepass hppass**
      - *Linux*:
        keytool.exe -export -alias hpcert -file <*path*>/keystore -keystore /opt/HP/BSM/odb/conf/security/server.keystore -storepass hppass

      After the command finishes, the BSM or OMi keystore certificate is stored in the specified `keystore` file.
   b. Run the following command on the BSM or OMi gateway server:
      - *Windows*:
        keytool.exe -export -alias clientcert -file <*path*>\truststore -keystore <*drive*>:\HPBSM\odb\conf\security\server.truststore -storepass hppass
      - *Linux*:
        keytool -export -alias clientcert -file <*path*>/truststore

```
-keystore /opt/HP/BSM/odb/conf/security/server.truststore
-storepass hppass
```

After the command finishes, the BSM or OMi truststore certificate is stored in the specified `truststore` file.

c. Copy the `keystore` file created in "Run the following command on the BSM or OMi gateway server:" on the previous page and the `truststore` file created in "Run the following command on the BSM or OMi gateway server:" on the previous page to a temporary directory on the NNMi management server. In the remaining commands, these files are shown as residing on the NNMi management server in the following locations:

   - *Windows*:
     `<drive>:\nnmi_temp\keystore`
     `<drive>:\nnmi_temp\truststore`,
   - *Linux*:
     `/nnmi_tmp/keystore`
     `/nnmi_tmp/truststore`

d. To merge the keystore certificate, run the following command on the NNMi management server:

   - *Windows*:
     ```
     keytool.exe -import -alias hpcert -keystore
     %NnmDataDir%\shared\nnm\certificates\nnm.keystore
     -storepass nnmkeypass -file <drive>:\nnmi_temp\keystore
     ```
   - *Linux*:
     ```
     keytool -import -alias hpcert -keystore
     $NnmDataDir/shared/nnm/certificates/nnm.keystore
     -storepass nnmkeypass -file /nnmi_tmp/keystore
     ```

e. To merge the truststore certificate, run the following command on the NNMi management server:

   - *Windows*:
     ```
     keytool.exe -import -alias clientcert -keystore
     %NnmDataDir%\shared\nnm\certificates\nnm.truststore
     -storepass ovpass -file <drive>:\nnmi_temp\truststore
     ```
   - *Linux*:
     ```
     keytool -import -alias clientcert -keystore
     $NnmDataDir/shared/nnm/certificates/nnm.truststore
     -storepass ovpass -file /nnmi_tmp/truststore
     ```

f. Complete this step only if BSM or OMi uses a self-signed certificate (not a certificate authority (CA) signed certificate). To merge the BSM or OMi keystore certificate into the NNMi truststore, run the following command on the NNMi management server:

  - *Windows*:
    ```
    keytool.exe -import -alias <bsm_selfsigned_cert> -keystore
    %NnmDataDir%\shared\nnm\certificates\nnm.truststore
    -storepass ovpass -file <drive>:\temp\keystore
    ```
  - *Linux*:
    ```
    keytool -import -alias <bsm_selfsigned_cert> -keystore
    $NnmDataDir/shared/nnm/certificates/nnm.truststore
    -storepass ovpass -file /tmp/keystore
    ```

g. Complete this step only if BSM or OMi uses one or more certificate authority (CA) signed certificates (not a self-signed certificate). Import the CA root certificate, as well as any CA intermediate certificates, into the NNMi trust store.

   Import each CA certificate separately. For example, to import the CA root certificate and one CA intermediate certificate, run the following commands on the NNMi management server:

  - *Windows*:
    ```
    keytool.exe -import -alias <bsm_ca_root_cert> -keystore
    %NnmDataDir%\shared\nnm\certificates\nnm.truststore
    -storepass ovpass -file <drive>:\temp\keystore
    ```

  -
    ```
    keytool.exe -import -alias <bsm_ca_intermediate_cert>
    -keystore %NnmDataDir%\shared\nnm\certificates\
    nnm.truststore -storepass ovpass -file <drive>:\temp\keystore
    ```
  - *Linux*:
    ```
    keytool -import -alias <bsm_ca_root_cert> -keystore
    $NnmDataDir/shared/nnm/certificates/nnm.truststore
    -storepass ovpass -file /tmp/keystore
    ```

  -
    ```
    keytool -import -alias <bsm_ca_intermediate_cert> -keystore
    $NnmDataDir/shared/nnm/certificates/nnm.truststore
    -storepass ovpass -file /tmp/keystore
    ```

10. *Optional*: Run the following command sequence on the NNMi management server:

    a. `ovstop`

    b. `ovstart`

11. *Optional*: Run the following commands on both the NNMi management server and the BSM or OMi gateway server. Compare the outputs to make sure the keystore certificates reside\ on both servers:

    - *NNMi management server*:
      - *Windows*:
        ```
        keytool.exe -list -keystore
        %NnmDataDir%\shared\nnm\certificates\nnm.keystore
        -storepass nnmkeypass
        ```

- *Linux*: `keytool -list -keystore $NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass`

- *BSM or OMi gateway server*:
  - *Windows*: `keytool.exe -list -keystore <drive>:\HPBSM\odb\conf\security\server.keystore -storepass hppass`
  - *Linux*: `keytool -list -keystore /opt/HP/BSM/odb/conf/security/server.keystore -storepass hppass`

12. *Optional*: Run the following commands on both the NNMi management server and the BSM or OMi gateway server. Compare the outputs to make sure the truststore certificates reside on both servers:
    - *NNMi management server*:

      Use the -v option to print the certificate in readable format. This option includes the date range for certificate validity.
      - *Windows*: `keytool.exe -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.truststore -storepass ovpass -v`
      - *Linux*: `keytool -list -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass -v`
    - *BSM gateway server*:
      - *Windows*: `keytool.exe -list -keystore <drive>:\HPBSM\odb\conf\security\server.truststore -storepass hppass -v`
      - *Linux*: `keytool -list -keystore /opt/HP/BSM/odb/conf/security/server.truststore -storepass hppass -v`
13. Check the date range to verify the certificate is still valid.

NNMi Data Available from BSM End User Management Reports

If you have configured a link in to an NNMi management server, BSM users can drill down from some of the End User Management reports to NNMi data. In NNMi, you can see Path View (trace route) information between a source (client) machine and destination (server) machine, which can help you identify the root cause of network problems and pinpoint common network problems.

BSM users can also use URL tools to launch the NNMi console for further analyzing incoming events in NNMi.

End User Management Reports with Drilldown to NNMi

"Table 8 End User Management Reports with Drilldown to NNMi" below lists the End User Management reports that provide drilldown to NNMi data. "Table 8 End User Management Reports with Drilldown to NNMi" below also describes the relevant source and destination machines for which trace route data is displayed. For more information about any report type, see *Analysis Reports* in the *BSM User Guide.*

Table 8 End User Management Reports with Drilldown to NNMi

End User Management Report	Source and Destination Machines
Action Over Time Report	The source and destination IP addresses with the worst network time for the selected action. If more than one action is included in the filter, the first action is used.
Action Raw Data Report	The source and destination IP addresses with the worst network time for the selected action.
RUM Action Summary Report	The source and destination IP addresses with the worst network time for the selected action.
RUM End User Group Over Time Report	The source and destination IP addresses for the request-response with the worst network time in the selected application. If more than one end-user group is included in the filter, the first end-user group is used. **NOTE:** You can drill down to NNMi from this report only when it is generated for TCP applications, or Web applications with TCP data.
RUM End User Group Summary Report	The source and destination IP addresses for the request-response with the worst network time from the selected application. **NOTE:** To drill down from this report to NNMi, the report must be generated for TCP

Table 8 End User Management Reports with Drilldown to NNMi, continued

End User Management Report	Source and Destination Machines
	applications or web applications with TCP data.
RUM Tier Summary Report	The source and destination IP addresses for the request-response with the worst network time in the selected application.
RUM Transaction Summary Report	The source and destination IP addresses with the worst network time for the selected transaction.
Session Details Report	The action server and session client IP addresses.
Tiers Over Time Report	The source and destination IP addresses for the request-response with the worst network time in the selected application.
Transaction Over Time Report	The source and destination IP addresses with the worst network time for the selected transaction. If more than one transaction is included in the filter, the first transaction is used.

Configuring Drilldown to NNMi Data

To enable drilldown from End User Management reports to NNMi data, follow these steps:

1. If you have not already done so, configure a connection from BSM to NNMi as described in "Enabling NNMi Visualizations from BSM or OMi" on the next page.
2. If you have not already done so, enable single sign-on between BSM and NNMi as described in "Configuring Single Sign-On Between NNMi and BSM, OMi, or UCMDB" on page 18.
3. If you have not already done so, configure NNMi to push topology information to the RTSM as described in "Enabling the HPE NNMi–HPE BSM/OMi/UCMDB Topology Integration" on page 15.
4. *Optional*. On the BSM server, install and configure the HPOprInf infrastructure content pack.

   For information, see the BSM Operations Management Extensibility Guide.

Enabling NNMi Visualizations from BSM or OMi

Configure a connection from BSM to NNMi to view the following data:

- NNMi components in MyBSM
- NNMi components in My Workspace in OMi
- Drilldown to NNMi from End User Management reports

To configure the connection from BSM or OMi to NNMi, follow these steps:

1. *For BSM.* In the BSM user interface, open the **Infrastructure Settings** page (**Admin > Platform > Setup and Maintenance > Infrastructure Settings**).

   For OMi. In the OMi user interface, open the **Infrastructure Settings** page (**Administration > Setup and Maintenance > Infrastructure Settings**).
2. Select **Foundations**, and then select **Integrations with other applications**.
3. In the **HP NNM** table, locate and modify the following parameters:
   - **HP NNM Integration URL**: the URL for accessing the NNMi console. Use the correct URL in the following form:
     <protocol> ://<fully_qualified_domain_name>:<port_number>

     <protocol> represents either http or https.

     <fully_qualified_domain_name> represents the official fully-qualified domain name (FQDN) of the NNMi management server.

     <port_number> is the port for connecting to the NNMi console, as specified in the following file:

     - *Windows*: `%NnmDataDir%\conf\nnm\props\nms-local.properties`
     - *Linux*: `$NnmDataDir/conf/nnm/props/nms-local.properties`

     For non-SSL connections, use the value of `nmsas.server.port.web.http` (formerly called `jboss.http.port`), which is `80` or `8004` by default (depending on the presence of another web server when NNMi was installed).

     For SSL connections, use the value of `nmsas.server.port.web.https` (formerly called `jboss.https.port`), which is `443` by default.

   - **HP NNMi User name**: the user name for connecting to the NNMi web services. This user must have the NNMi Administrator or Web Service Client role.

   - **HP NNMi User password**: the password for the specified NNMi user name.

Comparing Methods of Integrating NNMi with BSM/UMCDB

The following table provides a summary comparison of the two methods.

Table 9 Method Comparison for Integrating NNMi with BSM/UCMDB

NNMi-BSM Topology "Push" Integration	Probe-based "Pull" Integration ("Layer 2 by NNM" Discovery Job)
Can filter objects to sync from NNMi to BSM based on NNMi Node Group.	Currently no ability to filter NNMi objects to sync into BSM.
Performs incremental discovery and scheduled full topology sync.	Performs full topology sync only.
Creates all NNMi nodes as Node CIs *.	Creates NNMi nodes as various CI types (Router, Switch, Switch Router, Chassis, Computer, ATM Switch, Firewall, Load Balancer, and Printer).
Creates these other CIs: Interface, IpAddress, IpSubnet, Layer2Connection, HardwareBoard, and PhysicalPort.	Creates these other CIs: Interface, IpAddress, IpSubnet, Layer2Connection, HardwareBoard+, PhysicalPort+, and VLAN +.
Node CI attributes populated by BSM but not by Probe method: • Host is Route. • Host is Virtual. • NodeModel. • PrimaryDnsName.	Node CI attributes populated by Probe but not by BSM method: • Description (populated from Device Profile Description) Node CI attributes with different values from BSM method: • DiscoveredVendor (more user-friendly format in BSM method; for example "Hewlett-Packard" rather than "hewlettpackard"). • NodeFamily (more user-friendly format in BSM method). • Host NNM UID. • Host Key.
Layer 2 Connection CI attribute Display	Layer 2 Connection CI attribute Display

Table 9 Method Comparison for Integrating NNMi with BSM/UCMDB, continued

NNMi-BSM Topology "Push" Integration	Probe-based "Pull" Integration ("Layer 2 by NNM" Discovery Job)
Label is set to the Layer 2 Connection Name as shown in NNMi.	Label is hard-coded to "Layer2Connection". Other CIs with different attributes when populated by Probe: • HardwareBoard CI includes SoftwareVersion attribute. • PhysicalPort CI includes DuplexSetting and Port Name (same value as Name) attributes.
Can easily adapt the out-of-the-box Layer 2 Network view.	Out-of-the-box Layer 2 Network view.

+ NNMi 9 is required for these CIs to be created.

* Nodes are identified by the NodeRole attribute.

NOTE: UCMDB Content Pack 9 enhances NNMi integration support of large NNMi environments, allowing you to control the number of Layer2Connections, VLANs, and Nodes to get from NNMi per query.

Creating a New RTSM User

To create a new RTSM user for the HPE NNMi–HPE BSM/OMi/UCMDB Topology integration, follow these steps:

1. Open the UCMDB console.
2. Select **Security**.
3. Click **Users and Groups**.
4. Enter the user name and password.
5. For the roles association, select **Discovery and Integration Admin**.

Enter the new user name and password for the BSM RTSM user and password on the **HPE NNMi–HPE BSM/OMi/UCMDB Topology Integration Configuration** form.

NNMi - CI Attribute Mapping

The following diagrams show the mapping of NNMi object attributes to the equivalent CI attributes in BSM or OMi.

NOTE: The **Monitored By** attribute is set to include NNM for each of the CI types.

Table 10 NNMi Node - Node CI Attribute Mapping

NNMi Node Attribute	Node CI Attribute
Hostname	• PrimaryDnsName • Name
System Name	• SnmpSysName • Name
System Object ID	SysObjectId
System Contact	DiscoveredContact
System Location	DiscoveredLocation
System Description	DiscoveredDescription
Device Model	• NodeModel • DiscoveredModel
Device Vendor	DiscoveredVendor
Device Family	NodeFamily
Capabilities	NodeRole
PartitionID	BiosUuid
Capability: IP Forwarding (Layer 3)	Node Is Route
Capability: Virtual Machine	Node Is Virtual
UUID	• Host Key • Host NNM UID

Table 11 NNMi Interface - Interface CI Attribute Mapping

NNMi Interface Attribute	Interface CI Attribute
Physical Address	MacAddress
ifName	InterfaceName
ifAlias	InterfaceAlias
ifDescr	InterfaceDescription
ifIndex	InterfaceIndex
ifSpeed	InterfaceSpeed
ifType	InterfaceType

Table 12 NNMi IP Address - IpAddress CI Mapping

NNMi IP Address Attribute	IpAddress CI Attribute
Address	• IP Address • Name • IpAddressType • IpAddressValue

Table 13 NNMi IP Subnet IpSubnet CI Attribute Mapping

NNMi IP Subnet Attribute	IpSubnet CI Attribute
Prefix	• Name • IpAddressType • IpAddressValue
Prefix Length	IpPrefixLength

Table 14 NNMi Card - HardwareBoard CI Attribute Mapping

NNMi Card Attribute	HardwareBoard CI Attribute
Name	Name

Table 14 NNMi Card - HardwareBoard CI Attribute Mapping, continued

NNMi Card Attribute	HardwareBoard CI Attribute
Serial Number	SerialNumber
Firmware Version	FirmwareVersion
Hardware Version	HardwareVersion
Index	BoardIndex

Table 15 NNMi Port - PhysicalPort CI Attribute Mapping

NNMi Port Attribute	PhysicalPort CI Attribute
Name	Name
Port Index	PortIndex

Table 16 NNMi Layer 2 Connection - Layer2Connection CI Attribute Mapping

NNMi Layer 2 Connection Attribute	Layer2Connection CI Attribute
Name	Name

Table 17 NNMi VLAN - Vlan CI Attribute Mapping

VLAN Attribute	Vlan CI Attribute
Name	VLAN Name
VLAN Id	• Vlanid • Name

NNMi Environment Variables

HPE Network Node Manager i Software (NNMi) provides many environment variables that are available for your use in navigating the file system and writing scripts.

This appendix contains the following topics:

- "Environment Variables Used in This Document" below
- "Other Available Environment Variables" below

Environment Variables Used in This Document

This document primarily uses the following two NNMi environment variables to reference file and directory locations. This list shows the default values. Actual values depend on the selections that you made during NNMi installation.

- *Windows Server*:
  - `%NnmInstallDir%`: `<drive>\Program Files (x86)\HP\HP BTO Software`
  - `%NnmDataDir%`: `<drive>\ProgramData\HP\HP BTO Software`

  > **NOTE:** On Windows systems, the NNMi installation process creates these system environment variables, so they are always available to all users.

- Linux:
  - `$NnmInstallDir`: `/opt/OV`
  - `$NnmDataDir`: `/var/opt/OV`

  > **NOTE:** On Linux systems, you must manually create these environment variables if you want to use them.

Additionally, this document references some of the NNMi environment variables that you can source as part of your user log-on configuration on the NNMi management server. These variables are of the form `NNM_*`. For information about this extended list of NNMi environment variables, see "Other Available Environment Variables" below.

Other Available Environment Variables

NNMi administrators access some NNMi file locations regularly. NNMi provides a script that sets up many environment variables for navigating to commonly accessed locations.

To set up the extended list of NNMi environment variables, use a command similar to the following examples:

- Windows: "`C:\Program Files (x86)\HP\HP BTO Software\bin\nnm.envvars.bat`"
- Linux: `. /opt/OV/bin/nnm.envvars.sh`

After you run the command for your operating system, you can use the NNMi environment variables shown in "Table 18 Environment Variable Default Locations for the Windows Operating System" (Windows) or "Table 19 Environment Variable Default Locations for Linux Operating Systems" (Linux) to get to commonly used NNMi file locations.

Table 18 Environment Variable Default Locations for the Windows Operating System

Variable	Windows (example)
%NNM_BIN%	C:\Program Files (x86)\HP\HP BTO Software\bin
%NNM_CONF%	C:\ProgramData\HP\HP BTO Software\conf
%NNM_DATA%	C:\ProgramData\HP\HP BTO Software\
%NNM_DB%	C:\ProgramData\HP\HP BTO Software\shared\nnm\databases
%NNM_JAVA%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\hpsw\bin\java.exe
%NNM_JAVA_DIR%	C:\Program Files (x86)\HP\HP BTO Software\java
%NNM_JAVA_PATH_SEP%	;
%NNM_JBOSS%	C:\Program Files (x86)\HP\HP BTO Software\nmsas
%NNM_JBOSS_DEPLOY%	C:\Program Files (x86)\HP\HP BTO Software\nmsas\server\nms\deploy
%NNM_JBOSS_LOG%	C:\ProgramData\HP\HP BTO Software\log\nnm
%NNM_JBOSS_SERVERCONF%	C:\Program Files (x86)\HP\HP BTO Software\nmsas\server\nms
%NNM_JRE%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\hpsw
%NNM_LOG%	C:\ProgramData\HP\HP BTO Software\log

Table 18 Environment Variable Default Locations for the Windows Operating System, continued

Variable	Windows (example)
%NNM_LRF%	C:\ProgramData\HP\HP BTO Software\shared\nnm\lrf
%NNM_PRIV_LOG%	C:\ProgramData\HP\HP BTO Software\log
%NNM_PROPS%	C:\ProgramData\HP\HP BTO Software\shared\nnm\conf\props
%NNM_SHARED_CONF%	C:\ProgramData\HP\HP BTO Software\shared\nnm\conf
%NNM_SHARE_LOG%	C:\ProgramData\HP\HP BTO Software\log
%NNM_SNMP_MIBS%	C:\Program Files (x86)\HP\HP BTO Software\misc\nnm\snmp-mibs
%NNM_SUPPORT%	C:\Program Files (x86)\HP\HP BTO Software\support
%NNM_TMP%	C:\ProgramData\HP\HP BTO Software\tmp
%NNM_USER_SNMP_MIBS%	C:\ProgramData\HP\HP BTO Software\shared\nnm\user-snmp-mibs
%NNM_WWW%	C:\ProgramData\HP\HP BTO Software\shared\nnm\www

Table 19 Environment Variable Default Locations for Linux Operating Systems

Variable	Linux
$NNM_BIN	/opt/OV/bin
$NNM_CONF	/var/opt/OV/conf
$NNM_DATA	/var/opt/OV
$NNM_DB	/var/opt/OV/shared/nnm/databases
$NNM_JAVA	/opt/OV/nonOV/jdk/hpsw/bin/java
$NNM_JAVA_DIR	/opt/OV/java
$NNM_JAVA_PATH_SEP	:

Table 19 Environment Variable Default Locations for Linux Operating Systems, continued

Variable	Linux
$NNM_JBOSS	/opt/OV/nmsas
$NNM_JBOSS_DEPLOY	/opt/OV/nmsas/server/nms/deploy
$NNM_JBOSS_LOG	/var/opt/OV/log/nnm
$NNM_JBOSS_SERVERCONF	/opt/OV/nmsas/server/nms
$NNM_JRE	/opt/OV/nonOV/jdk/hpsw
$NNM_LOG	/var/opt/OV/log
$NNM_LRF	/var/opt/OV/shared/nnm/lrf
$NNM_PRIV_LOG	/var/opt/OV/log
$NNM_PROPS	/var/opt/OV/shared/nnm/conf/props
$NNM_SHARED_CONF	/var/opt/OV/shared/nnm/conf
$NNM_SHARE_LOG	/var/opt/OV/log
$NNM_SNMP_MIBS	/opt/OV/misc/nnm/snmp-mibs
$NNM_SUPPORT	/opt/OV/support
$NNM_TMP	/var/opt/OV/tmp
$NNM_USER_SNMP_MIBS	/var/opt/OV/shared/nnm/user-snmp-mibs
$NNM_WWW	/var/opt/OV/shared/nnm/www

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 Business Service Management/Universal CMDB Topology Integration Guide (Network Node Manager i Software 10.20)

Just add your feedback to the email and click send.

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

We appreciate your feedback!

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.