

HP Network Node Manager i Software

For the Windows[®] and Linux[®] operating systems

Software Version: NNMi 10.10

HP Network Node Manager i Software—HP Business Service Management/Universal CMDB Topology Integration Guide



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2008–2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

AMD is a trademark of Advanced Micro Devices, Inc.

Google™ is a registered trademark of Google Inc.

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

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

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

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

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

sFlow is a registered trademark of InMon Corp.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

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

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

November 2015

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/>).

Available Product Documentation

For a complete list of the documentation that is available for NNMi, see the *HP Network Node Manager i Software Documentation List*. This document is available on the HP manuals web site. Use this file to track additions to and revisions within the NNMi documentation set for this version of NNMi. Click a link to access a document on the HP manuals web site.

Also available on the HP manuals web site are .zip files of the complete documentation set for NNMi, NNMi Premium, and NNMi Ultimate. Access these documentation packages from the *HP Network Node Manager i Software Documentation List* or directly from the HP manuals web site.

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

<https://softwaresupport.hp.com>

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

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

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

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

Support

Visit the HP Software Support Online web site at:

<https://softwaresupport.hp.com>

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

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

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

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

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

To find more information about access levels, go to:

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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this web site is:

<http://h20230.www2.hp.com/sc/solutions/index.jsp>

Contents

HP Business Service Management Overview	7
Comparison of Approaches to Integrating NNMi with HP BSM Operations Management	7
HP NNMi–HP BSM Operations Management Integration.....	9
NNMi Integrated with HPOM Integrated with HP BSM Operations Management	10
NNMi Visualizations in BSM.....	10
HP Business Service Management and HP Universal CMDB.....	11
HP NNMi–HP BSM/UCMDB Topology Integration	12
Value	12
Integrated Products	13
Documentation.....	13
Enabling the HP NNMi–HP BSM/UCMDB Integration to Synchronize Topology to the UCMDB System	13
Enabling the HP NNMi–HP BSM/UCMDB Topology Integration.....	15
Configuring Single Sign-On Between NNMi and BSM or UCMDB	17
Configure NNMi for the Proper Source Character Encoding for SNMP Agents	18
Enabling the Find BSM/UCMDB Impacted CIs Feature	19
Using the HP NNMi–HP BSM/UCMDB Topology Integration	20
Network Topology Views	23
Layer 2 Topology View	23
Service Health Views.....	27
OMi Health Perspectives.....	28
Additional NNMi Functionality Provided by the Integration	29
Running the BSM or UCMDB Impact Analysis from the NNMi Console	29
Changing the HP NNMi–HP BSM/UCMDB Topology Integration Configuration.....	29
Disabling the HP NNMi–HP BSM/UCMDB Topology Integration.....	29
Troubleshooting the HP NNMi–HP BSM/UCMDB Topology Integration.....	30
Interface Labels Appear as MAC Addresses in the BSM User Interface	30
Duplicate CIs for Managed Nodes in the RTSM.....	30
Application Failover and the HP NNMi–HP BSM/UCMDB Topology Integration	30
HP NNMi–HP BSM/UCMDB Topology Integration Configuration Form Reference	30
NNMi Management Server Connection	31
BSM Gateway Server or UCMDB Server Connection	31
Configuration Item Topology Filter	32
Node Topology Filter.....	33
HP BSM Operations Management	35
HP NNMi–HP BSM Operations Management Integration	35
Value	36
Integrated Products	36
Documentation.....	37

Enabling the HP NNMi—HP BSM Operations Management Integration	37
Configuring NNMi to Close Incidents After the Corresponding BSM Events are Closed	41
Using the HP NNMi—HP BSM Operations Management Integration	42
Configuration Item Identifiers.....	43
Health Indicators.....	43
Default Policy Conditions.....	43
Customizing Policy Conditions	44
More Information.....	44
Changing the HP NNMi—HP BSM Operations Management Integration.....	45
Update the SNMP Trap Policy Conditions for New NNMi Traps	45
Change the Configuration Parameters.....	45
Disabling the HP NNMi—HP BSM Operations Management Integration.....	46
Troubleshooting the HP NNMi—HP BSM Operations Management Integration	46
BSM Operations Management Event Browser Contains No Forwarded Incidents	46
BSM Operations Management Event Browser Contains Only Some Forwarded Incidents	49
NNMi—HPOM Agent Destination Form Reference (BSM Operations Management Integration).....	49
BSM Connector Connection	50
BSM Operations Management Integration Content	51
BSM Connector Destination Status Information.....	53
NNMi Visualizations Within HP Business Service Management	55
MyBSM Portal	55
NNMi Components Available in MyBSM.....	56
Viewing the NNMi Components in MyBSM	56
Configuring an SSL Connection to BSM	57
NNMi Data Available from BSM End User Management Reports.....	63
End User Management Reports with Drilldown to NNMi.....	63
Configuring Drilldown to NNMi Data	64
Enabling NNMi Visualizations from BSM	64
Comparing Methods of Integrating NNMi with BSM/UMCDB	67
NNMi - CI Attribute Mapping	71
NNMi Environment Variables	79
Environment Variables Used in This Document	79
Other Available Environment Variables	79

HP Business Service Management Overview

The HP 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.

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

- [Comparison of Approaches to Integrating NNMi with HP BSM Operations Management](#) on page 7
- [HP NNMi—HP BSM Operations Management Integration](#) on page 9
- [NNMi Integrated with HPOM Integrated with HP BSM Operations Management](#) on page 10
- [NNMi Visualizations in BSM](#) on page 10

Comparison of Approaches to Integrating NNMi with HP BSM Operations Management

[Table 1](#) compares the HP NNMi—HP BSM Operations Management with the HP NNMi—HPOM integration.

See [HP NNMi—HP BSM Operations Management Integration](#) on page 9 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 and HPOM

Comparison Item	Direct Integration with the BSM Connector	Indirect Integration Through HPOM
Instruction text	<p>Events cannot contain instructional text. To make instructional text available, create a tool to launch user-defined instructions as a URL. (You would need to create external documentation for this tool.)</p> <p>If BSM is installed with the Monitoring Automation component, you can do the following:</p> <ol style="list-style-type: none"> 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: <p>Windows:</p> <ul style="list-style-type: none"> — <code><BSM_Root_Directory>\opr\bin\ConfigExchange.bat -username <username> -password <password> uploadOM -input <policy header file></code> <p>OR</p> <ul style="list-style-type: none"> — <code><BSM_Root_Directory>\opr\bin\ConfigExchange.bat -username <username> -password <password> -uploadOM -input <dir in which the policy header file is located></code> <p>— where:</p> <ul style="list-style-type: none"> — <username> is the BSM user name — <password> is the BSM user password <p>Linux:</p> <ul style="list-style-type: none"> — <code><BSM_Root_Directory>\opr\bin\ConfigExchange -username <username> -password <password> uploadOM -input <policy header file></code> <p>OR</p> <ul style="list-style-type: none"> — <code><BSM_Root_Directory>\opr\bin\ConfigExchange -username <username> -password <password> -uploadOM -input <dir in which the policy header file is located></code> <p>— where:</p> <ul style="list-style-type: none"> — <username> is the BSM user name — <password> is the BSM user password <p>The SNMP trap policy on the BSM Connector OM Agent is imported to the BSM server.</p> <p>Also see Enabling the HP NNMi—HP BSM Operations Management Integration on page 37</p>	Events can contain instruction text.

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

Comparison Item	Direct Integration with the BSM Connector	Indirect Integration Through HPOM
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.
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 HP 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.	<ul style="list-style-type: none"> • The agent implementation of the HP NNMi—HPOM integration is unidirectional. • The web services implementations of the HP NNMi—HPOM integration provides bidirectional event handling.

HP NNMi—HP BSM Operations Management Integration

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

The BSM Connector can be on the NNMi management server or on a separate server.

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 HP 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 43.

For more information, see [HP NNMi—HP BSM Operations Management Integration](#) on page 35.

NNMi Integrated with HPOM Integrated with HP 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 HP 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*.

NNMi Visualizations 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. For more information, see [MyBSM Portal](#) on page 55.
- NNMi console views launched from events in the BSM Operations Management event browser. For more information, see [Using the HP NNMi—HP BSM Operations Management Integration](#) on page 42.

HP Business Service Management and HP Universal CMDB

For NNMi 10.00 or later, it is recommended to use the HP NNMi–HP BSM/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) software provides 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/UCMDB](#) on page 67.

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

This chapter contains the following topics:

- [HP NNMi–HP BSM/UCMDB Topology Integration](#)
- [Enabling the HP NNMi-HP BSM/UCMDB Integration to Synchronize Topology to the UCMDB System](#)
- [Enabling the HP NNMi–HP BSM/UCMDB Topology Integration](#)
- [Configuring Single Sign-On Between NNMi and BSM or UCMDB](#)
- [Configure NNMi for the Proper Source Character Encoding for SNMP Agents](#)
- [Enabling the Find BSM/UCMDB Impacted CIs Feature](#)
- [Using the HP NNMi–HP BSM/UCMDB Topology Integration](#)
- [Network Topology Views](#)
- [Additional NNMi Functionality Provided by the Integration](#)

- [Changing the HP NNMi–HP BSM/UCMDB Topology Integration Configuration](#)
- [Disabling the HP NNMi–HP BSM/UCMDB Topology Integration](#)
- [Troubleshooting the HP NNMi–HP BSM/UCMDB Topology Integration](#)
- [Application Failover and the HP NNMi–HP BSM/UCMDB Topology Integration](#)
- [HP NNMi–HP BSM/UCMDB Topology Integration Configuration Form Reference](#)

HP NNMi–HP BSM/UCMDB Topology Integration

The HP NNMi–HP BSM/UCMDB Topology integration populates NNMi topology into either the BSM 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.
- Path health views available from the BSM Real User Monitor (RUM).
- Using the agent implementation of the HP 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 43.
- Using the agent implementation of the HP 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 HP NNMi–HP BSM/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
- UCMDB



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

- NNMi 10.10

NNMi and BSM or UCMDB must be installed on separate computers. The NNMi management server and the BSM 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.

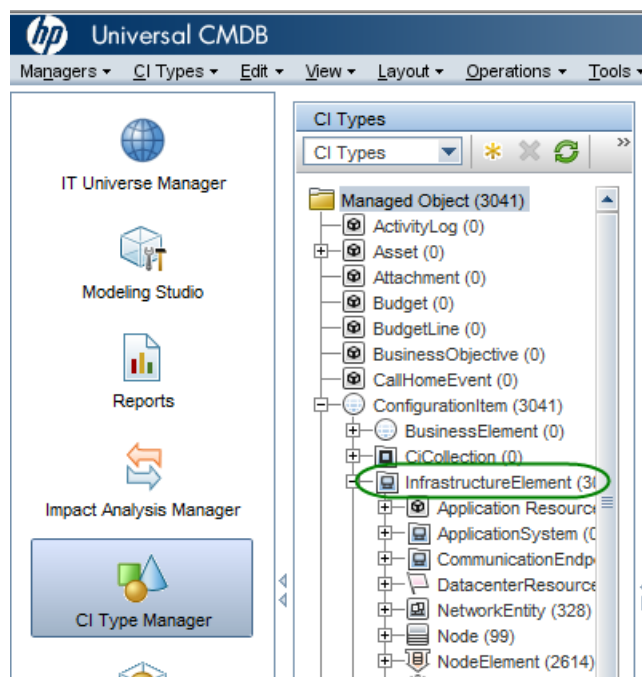
Enabling the HP NNMi-HP BSM/UCMDB Integration to Synchronize Topology to the UCMDB System

You must enable the HP NNMi-HP BSM/UCMDB integration to synchronize topology to the UCMDB system by adding the **monitored by** attribute in the CI Type model of UCMDB for certain CI types.

Note: This synchronization does not apply to the BSM/RTSM.

- 1 Open the UCMDB console.
- 2 Select **CI Type Manager**.

3 Expand **ConfigurationItem>Infrastructure Element**:



- 4 Navigate to the **Attributes** tab.
- 5 Click **+** (Add).
- 6 In the **Add Attribute** dialog, enter the following values:
 - a **Attribute Name:** `monitored_by`
 - b **Display Name:** `Monitored By`
- 7 In the **Attribute Type** section
 - a Select **Primitive**
 - b Select **list of strings**
- 8 Click **OK**.

Enabling the HP NNMi–HP BSM/UCMDB Topology Integration



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 HP NNMi–HP BSM/UCMDB Topology integration. If you want NNMi information in both databases, do *both* of the following in any order:

- Configure the HP NNMi–HP BSM/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:
<http://h20230.www2.hp.com/selfsolve/manuals>

Best practice

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

- 1 *Prerequisite:* Verify that the BSM 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 *Prerequisite:* Make sure that you have enabled the integration to synchronize topology to the UCMDB system by adding the **monitored by** attribute in the CI Type model of UCMDB for certain CI types. See [Enabling the HP NNMi–HP BSM/UCMDB Integration to Synchronize Topology to the UCMDB System](#).
- 3 *Optional.* Update the RTSM or UCMDB model for interfaces to set the interface display label to prefer interface name over MAC address:
 - a In the BSM or UCMDB user interface, open the **CI Type Manager** page (**Admin > 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
```
- 4 In the NNMi console, open the **HP NNMi–HP BSM/UCMDB Topology Integration Configuration** form (**Integration Module Configuration > HP BSM/UCMDB Topology**).
- 5 Select the **Enable Integration** check box to make the remaining fields on the form available.
- 6 Enter the information for connecting to the NNMi management server. For information about these fields, see [NNMi Management Server Connection](#) on page 31.

- 7 Enter the information for connecting to the BSM gateway server or the UCMDB server. For information about these fields, see [BSM Gateway Server or UCMDB Server Connection](#) on page 31.
- 8 *Optional:* Select **Only synchronize managed objects** if you want to exclude unmanaged CIs and unconnected interfaces from the integration.
- 9 *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 32.
- 10 *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 33.
- 11 *Optional:* Adjust the **Topology Synchronization Interval** hours to increase the period between full topology synchronizations.

The HP NNMi–HP BSM/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 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.

- 12 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 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.

- 13 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.



If you cannot connect to the NNMi management server, and suspect a problem with certificates, see *Working with Certificates for NNMi* in the *NNMi 10.10 Deployment Reference*.

- 14 Make sure that single sign-on is configured in both BSM or UCMDB and NNMi with the same initialization string values. For information about configuring the initialization string values in BSM, see *Authentication Wizard* in the *BSM Platform Administration Guide*. 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 SSL Connection to BSM](#) on page 57.
- 15 To display NNMi data in BSM and to access the NNMi components in MyBSM, complete the steps shown in [Enabling NNMi Visualizations from BSM](#) on page 64.

- 16 You can view NNMi data in MyBSM and EUM, as described in [NNMi Components Available in MyBSM](#) on page 56 and [End User Management Reports with Drilldown to NNMi](#) on page 63.

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

Configuring Single Sign-On Between NNMi and BSM 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 to HP 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.

BSM initialization string

Locate the BSM initialization string as follows:

- 1 Access the JMX console for BSM at:
`http://<BSM_hostname>:<BSM_JMX_port>/jmx-console/`
- 2 Select **service=LW-SSO Configuration** (under Topaz).
The initialization string is the value of the **InitString** parameter.
- 3 If you change the value of the **InitString** parameter, click **Apply Changes**.

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 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
```

- 3 If you change the value of the `initString` parameter shown in [step 2](#), run the following command to commit the changes:

```
nnmssso.ovpl -reload
```

Configure NNMi for the Proper Source Character Encoding for SNMP Agents

Node reconciliation in UCMDB and BSM Topology often depends on string matching of values provided by different data providers. In some cases, the values NNMi sends to BSM/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.

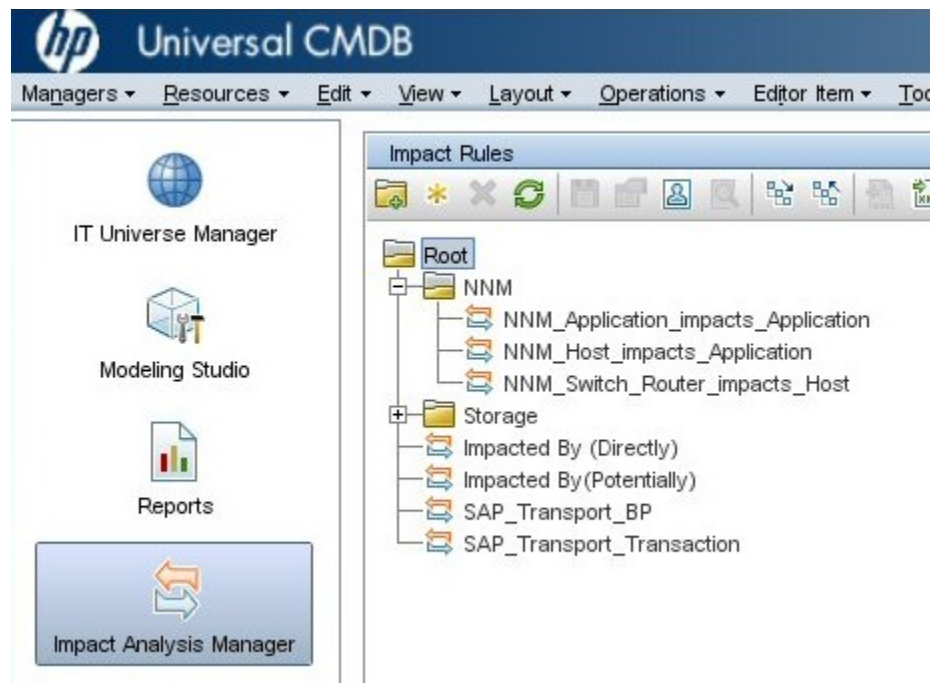
For more information, see "Configuring Character Set Encoding Settings for NNMi" in the *NNMi Deployment Reference*.

Enabling the Find BSM/UCMDB Impacted CIs Feature

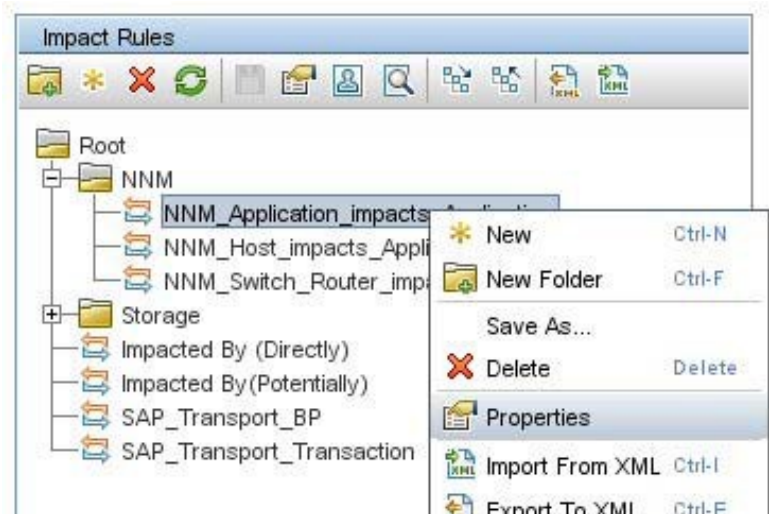
To enable the **Find BSM/UCMDB impacted CIs** feature in the NNMi-BSM integration, you must add the rules provided by NNMi to the NNMi Rule bundle using the **Impact Analysis Manager** as follows:

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/NNMi** folder:

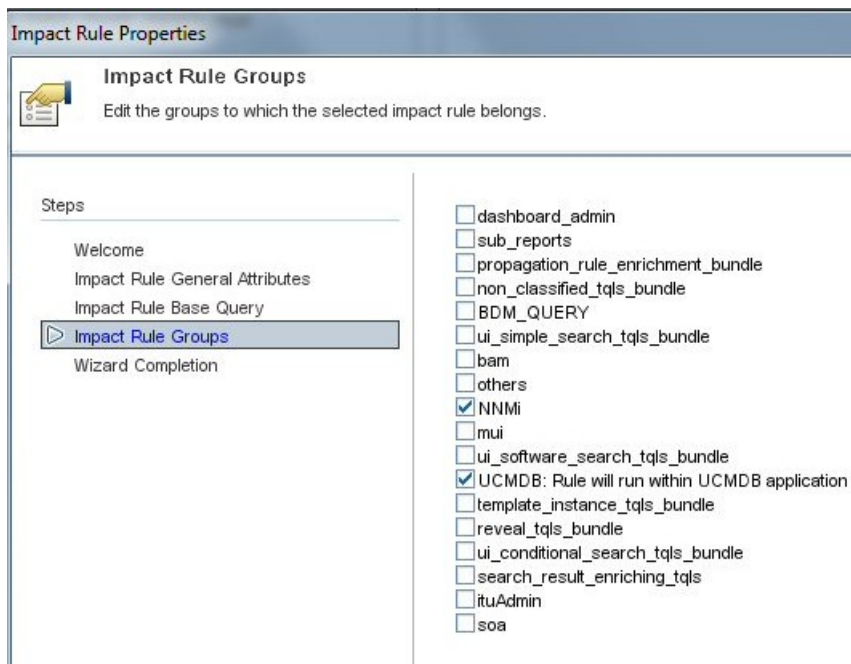


- 3 For each rule listed:
 - a Right-click the rule and select **Properties**:



- 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 HP NNMi–HP BSM/UCMDB Topology Integration](#):



Using the HP NNMi–HP BSM/UCMDB Topology Integration

The HP NNMi–HP BSM/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 33.
- 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 or UCMDB.
- InfrastructureElement > NodeElement > HardwareBoard

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



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 32.

- 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 or UCMDB.

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



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 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



A single node can have multiple nodes roles. NNMi uses the node's **Device Category** and the node's capabilities to determine which **NodeRole** or **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.capability.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 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](#) for the mapping of NNMi attributes to the equivalent CI attributes for each CI type.

The HP NNMi–HP BSM/UCMDB Topology integration forwards NNMi information and updates to the BSM 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 CI aging settings to delete CIs that have not been updated for a set period of time.



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 HP NNMi–HP BSM/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 9.1x 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 (OMi).

Layer 2 Topology View

You can modify the Layer 2 by NNMi view in BSM 9.1x to work with the topology created by the BSM – NNMi topology integration. One way to do this is as follows:

- 1 Open the Layer 2 by NNMi view and save it as **Layer 2 by NNMi 9.10**.
- 2 Modify the **Layer 2 by NNMi 9.10** view as follows:
 - a Delete the **Net Device CI Type**, and in its place add another **Node CI Type**.
 - b Add a Composition relationship between this new **Node CI** and its **Interface CI**.
 - c Re-establish the folding rule (fold Interface under Node).
 - d For the **Node CI**, specify that the **NodeRole** attribute must contain **lan_switch** or **router** to restrict the results to network devices.
 - e (Optional) You can further restrict the results by specifying the Node CI name(s) to match in order to view the equivalent of a Layer 2 Neighbor view.

The following two figures show the results, comparing an NNMi 9.10 Layer 2 Neighbor View with the equivalent Layer 2 by NNMi 9.10 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

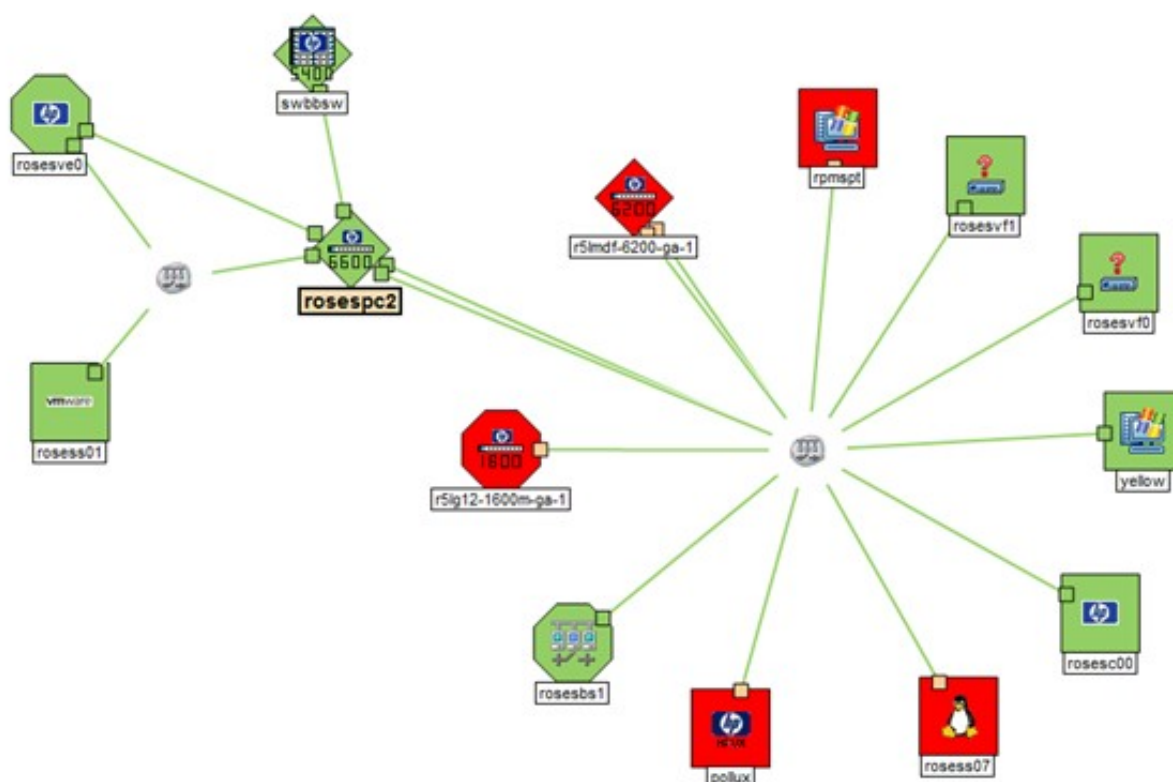


Figure 2 BSM 9.1x Layer 2 by NNMi 9.10 view

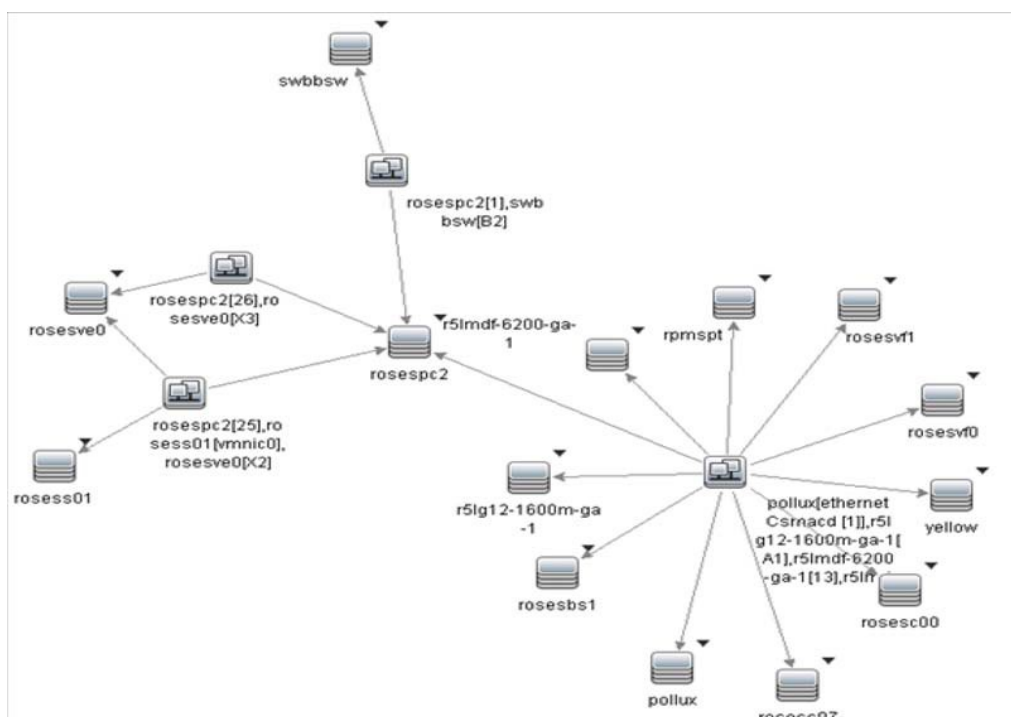
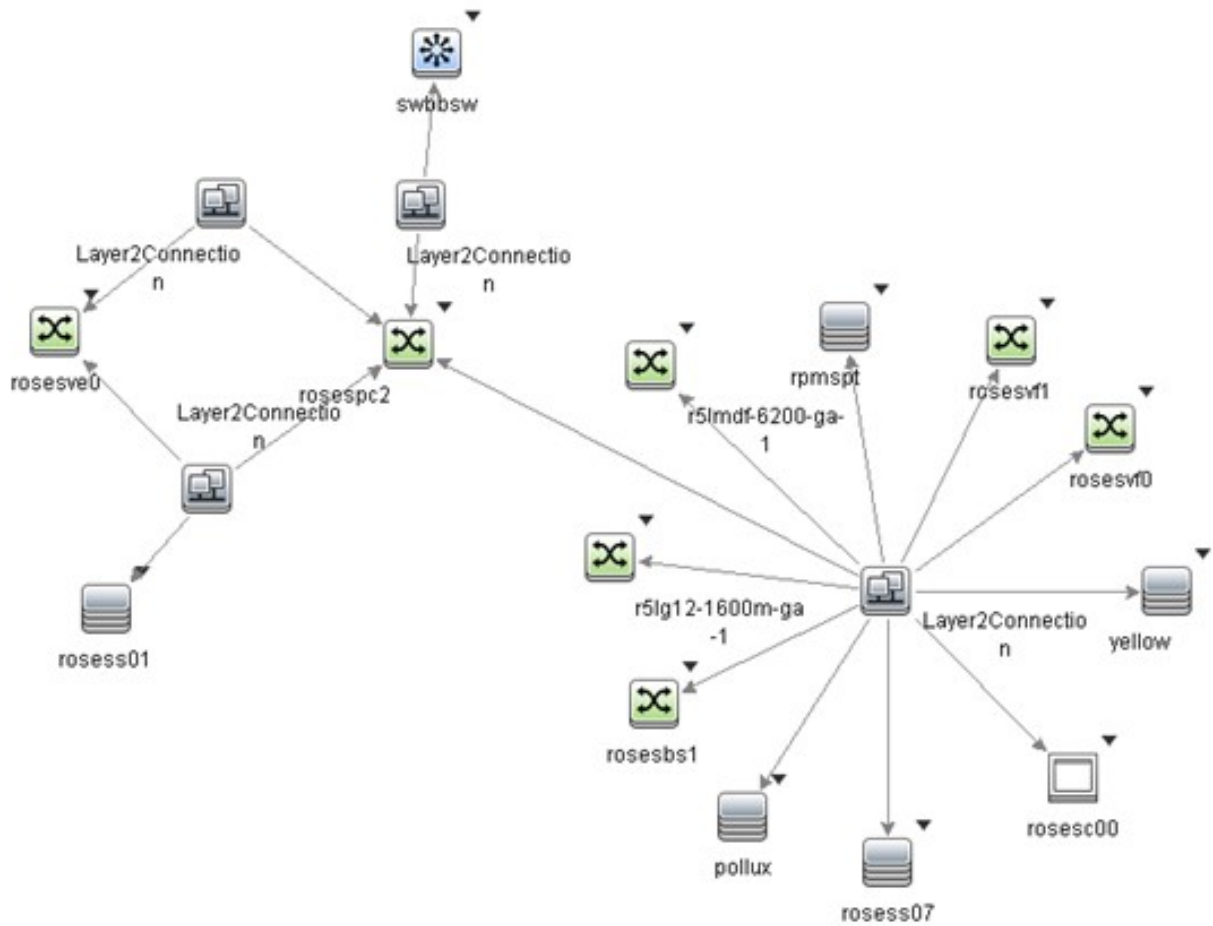


Figure 3 UCMDB 9.03 Layer 2 by NNMi view

This type of view (Layer 2 by NNMi 9.10) 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](#) 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

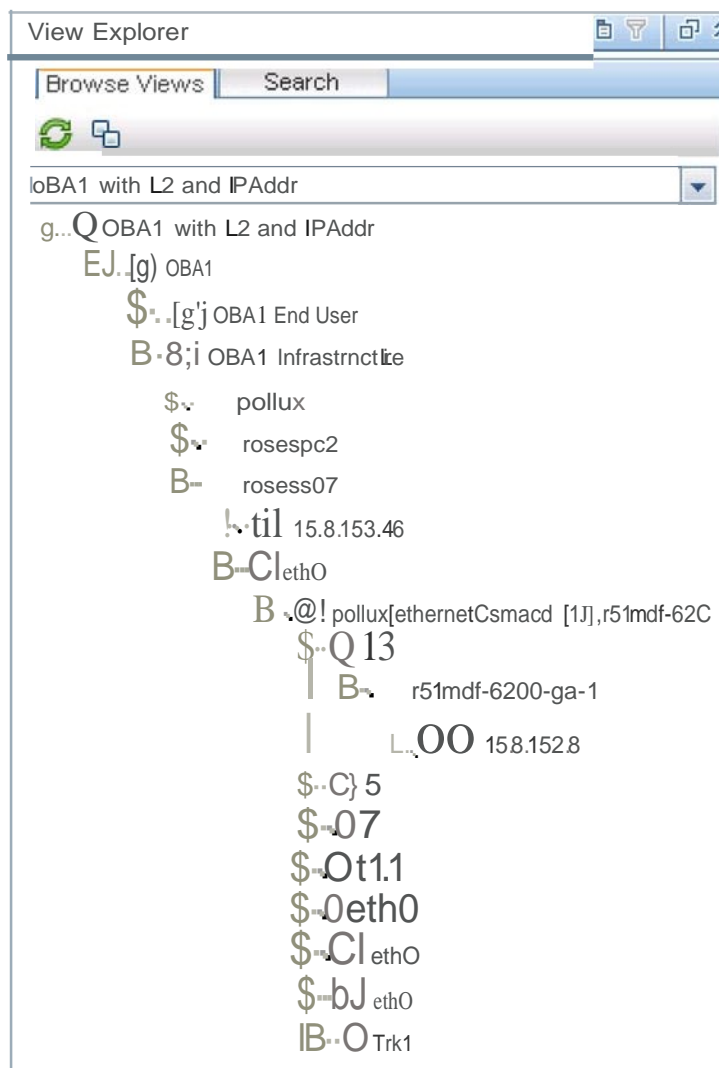
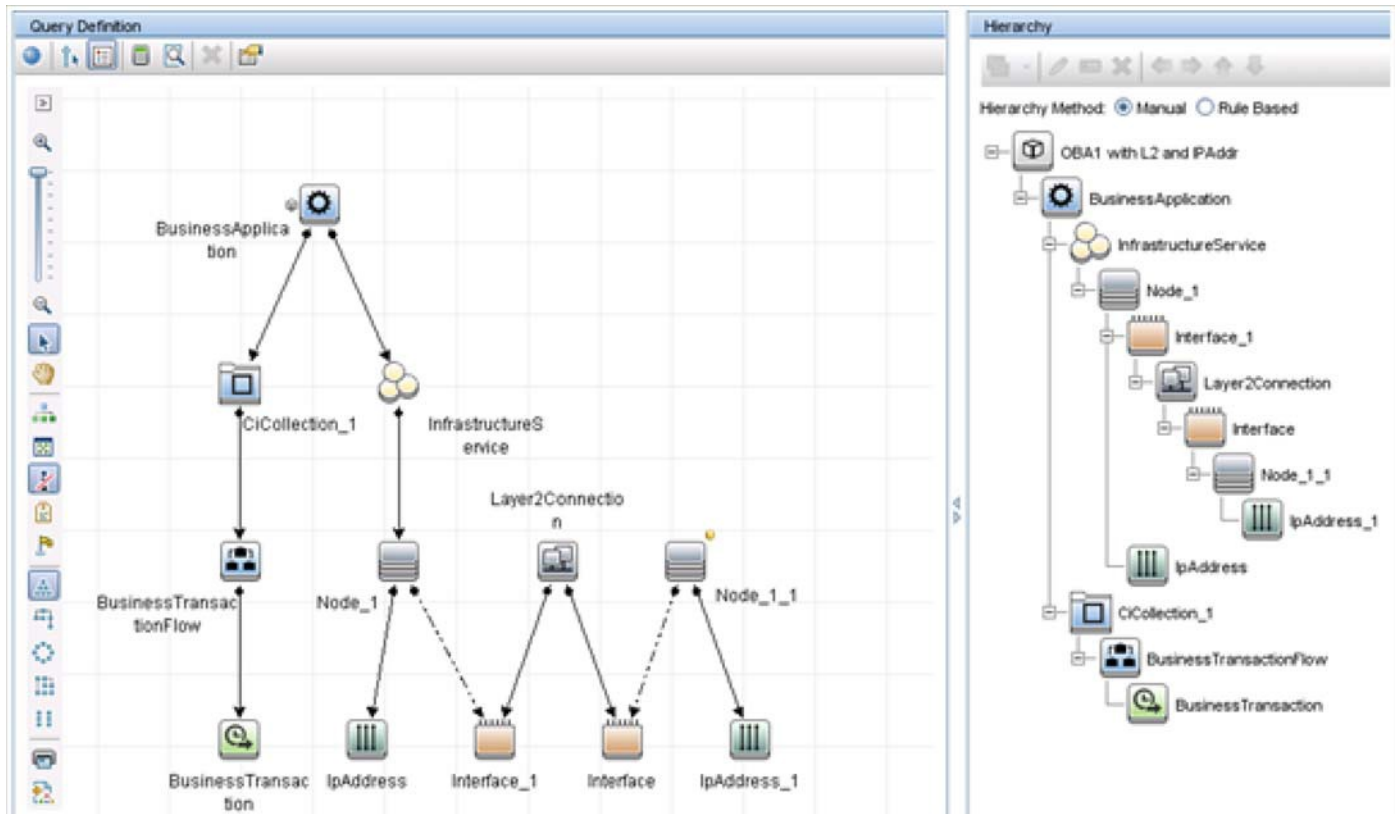


Figure 5 View Definition:

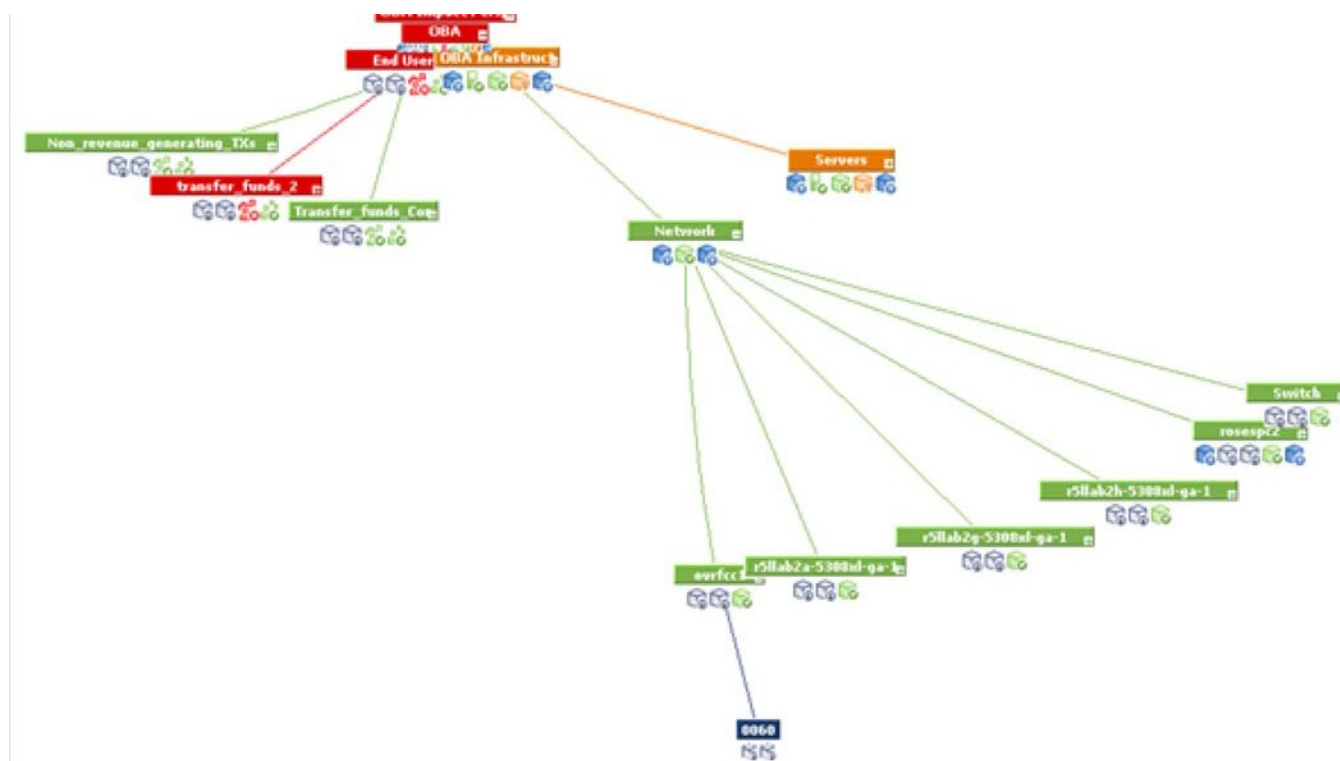


Service Health Views

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 HP NNMi–HP BSM/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 or UCMDB Impact Analysis from the NNMi Console


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

Enabling the HP NNMi–HP BSM/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 HP NNMi–HP BSM/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 [HP NNMi–HP BSM/UCMDB Topology Integration Configuration Form Reference](#) on page 30.
- 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.

 The changes take effect immediately.

Disabling the HP NNMi–HP BSM/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.

 The changes take effect immediately.

Troubleshooting the HP NNMi–HP BSM/UCMDB Topology Integration

This section contains the following topics:

- [Interface Labels Appear as MAC Addresses in the BSM User Interface](#) on page 30
- [Duplicate CIs for Managed Nodes in the RTSM](#) on page 30

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 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 HP NNMi–HP BSM/UCMDB Topology Integration

If the NNMi management server participates in NNMi application failover, the HP NNMi–HP BSM/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 server.

HP NNMi–HP BSM/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 or UCMDB. This form is available from the **Integration Module Configuration** workspace.



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](#) on page 31
- [BSM Gateway Server or UCMDB Server Connection](#) on page 31
- [Node Topology Filter](#) on page 33

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](#) on page 31 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	<p>The connection protocol specification.</p> <ul style="list-style-type: none"> • 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. <p>The integration selects the port for connecting to the NNMi console based on this specification.</p>
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 user must have the NNMi Administrator or Web Service Client role.
NNMi Password	The password for the specified NNMi user.

BSM Gateway Server or UCMDB Server Connection

[Table 3](#) lists the parameters for connecting to the BSM gateway server or the UCMDB server to communicate with the BSM RTSM or the UCMDB database. Coordinate with the BSM or UCMDB administrator to determine the appropriate values for this section of the configuration.



References to BSM in the configuration form apply to either the BSM gateway server or the UCMDB server.

Table 3 BSM Gateway Server Information

BSM Gateway Server or UCMDB Server Parameter	Description
BSM SSL Enabled	<p>The connection protocol specification for connecting to BSM or UCMDB.</p> <ul style="list-style-type: none"> • If BSM or UCMDB is configured to use HTTPS, select the BSM SSL Enabled check box. • If BSM 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 <i>Working with Certificates for NNMi</i> in the <i>NNMi 10.10 Deployment Reference</i>.
BSM Host	The fully-qualified domain name of the BSM gateway server or the UCMDB server.
BSM Port	<p>The port for connecting to BSM or UCMDB.</p> <p>If you are using the default BSM configuration, use the default http port 80 for BSM or the default http port 8080 for UCMDB.</p> <p>The default https port is 443 for BSM and UCMDB.</p>
BSM RTSM User	The user name for the BSM administrator.
BSM RTSM Password	The password of the above user.

Configuration Item Topology Filter

By default, the HP NNMi–HP BSM/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 HP NNMi–HP BSM/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:

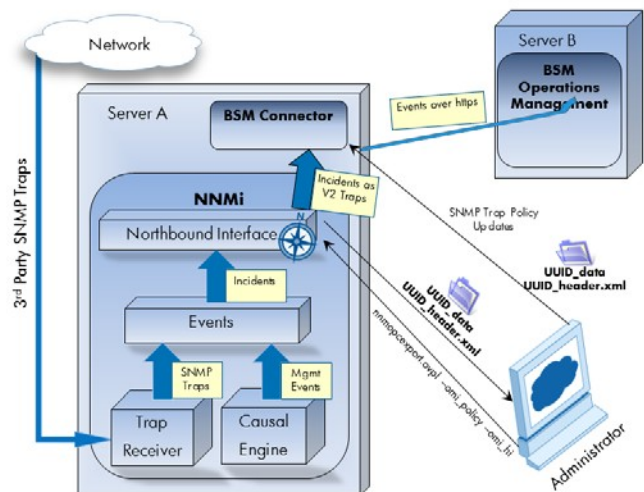
- If the node is connected to one or more nodes in the topology filter node group, the integration forwards the information about that node to BSM or UCMDB.
- If the node is not connected to any of the nodes in the topology filter node group, the integration ignores that node.

Table 4 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	<p>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.</p> <p>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.</p> <p>If you do not specify a topology filter node group, the HP NNMi–HP BSM/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.</p>
Additional Connections Node Group	<p>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.</p> <p>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.</p> <p>If you specify a topology filter node group and specify an additional connections node group, the HP NNMi–HP BSM/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.</p> <p>If you specify a topology filter node group but do not specify an additional connections node group, the HP NNMi–HP BSM/UCMDB Topology integration forwards information about the nodes and interfaces in the topology filter node group only.</p> <p>If you do not specify a topology filter node group, the HP NNMi–HP BSM/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 Connections Node Group field.</p>

HP BSM Operations Management



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

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

This chapter contains the following topics:

- [HP NNMi—HP BSM Operations Management Integration](#) on page 35
- [Enabling the HP NNMi—HP BSM Operations Management Integration](#) on page 37
- [Configuring NNMi to Close Incidents After the Corresponding BSM Events are Closed](#) on page 41
- [Using the HP NNMi—HP BSM Operations Management Integration](#) on page 42
- [Changing the HP NNMi—HP BSM Operations Management Integration](#) on page 45
- [Disabling the HP NNMi—HP BSM Operations Management Integration](#) on page 46
- [Troubleshooting the HP NNMi—HP BSM Operations Management Integration](#) on page 46
- [NNMi—HPOM Agent Destination Form Reference \(BSM Operations Management Integration\)](#) on page 49

HP NNMi—HP BSM Operations Management Integration

The HP NNMi—HP 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 HP BSM Operations Management event browser.

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

The BSM Connector can be on the NNMi management server or on a separate server.

The HP NNMi—HP BSM Operations Management integration also provides for accessing the NNMi console from within the BSM Operations Management event browser.



This chapter describes the direct integration between NNMi and the BSM Operations Management event browser.

The HP NNMi—HP 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 HP NNMi—HP BSM Operations Management integration consists of the following components:

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

Value

The HP NNMi—HP BSM Operations Management integration provides event consolidation in the BSM Operations Management event browser for the network management, system management, and application management domains, so that users of the BSM Operations Management 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 event browser.
- Access to the NNMi console from the BSM Operations Management 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 Manager i license



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

- NNMi 10.10 on the Windows or Linux operating system only

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

The BSM Connector must be installed *after* NNMi installation. The BSM Connector can be on the NNMi management server computer or on a separate computer. 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 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*

Enabling the HP NNMi—HP BSM Operations Management Integration

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



When NNMi integrates with the HP Business Service Management (BSM) topology database, the HP NNMi—HP BSM Operations Management 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 43.

To enable the HP NNMi—HP BSM Operations Management 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.



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 HP NNMi—HP BSM Operations Management Integration](#) on page 42.

- c If you want to forward the NNMi severity information (that is, if you performed [step b](#) on page 39), 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:

- 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, configure the BSM Connector integration with BSM as described in the *BSM Application Administration Guide*.



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 [step 1](#) 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 [step 4](#) (for the BSM Connector) and [step 5](#) (for NNMi) of this procedure.



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 [step b](#). 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
```



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 [step 3](#) 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 [step 3](#) of this procedure.
For information about these fields, see [BSM Connector Connection](#) on page 50.
- e Specify the sending options. Select the **HTTP** option for the **NNMi Console Access** field.
For information about these fields, see [BSM Operations Management Integration Content](#) on page 51.
- 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 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 user must have BSM RTSM or UCMDDB administrative privileges.

The SNMP trap policy on the BSM Connector OM Agent is imported to the BSM 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 HP BSM Operations Management.

- 1 Copy the **OMBackSync.pl** script to the correct location:

Windows: Copy %ovdatadir%\conf\nnm\backsync\OMBackSync.pl to %ovdatadir%\conf\backsync\OMBackSync.pl

Linux: Copy /var/opt/OV/conf/nnm/backsync/OMBackSync.pl to /var/opt/OV/conf/backsync/OMBackSync.pl

- 2 Modify the OMBackSync.pl script. Use the following example as a guide to modify the script parameters:

```
my $nnmi_server = 'localhost';
my $nnmi_port   = <http port used to access NNMi>;
my $nnmi_user   = '<administrator user name>';
my $nnmi_pass   = '<administrator password>';
my $logfilepath = OV_DATA_DIR.'/log/OMBacksync-NNMi.log';
my $verbosity   = 2
```

- 3 Edit the OMBackSync.pl script and search for the following line:

END

Remove all of the text from **END** to the end of the script in the OMBackSync.pl script. Make sure to save your work.

- 4 *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**

- 5 Run the following command to restart the ombacksync process: **ovc -restart ombacksync**.

- 6 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 HP BSM Operations Management as it detects alerts being acknowledged.




If you reinstall NNMi 10.10, you must reinstall the BSM Connector and repeat [step 1](#) on page 41 through [step 6](#) on page 41.



If you reinstall the BSM Connector, you must repeat [step 1](#) on page 41 through [step 6](#) on page 41. Reinstalling the BSM Connector overwrites the OMBackSync.pl script that you copied and modified in [step 1](#) on page 41 through [step 3](#) on page 41, and you will lose all of your changes. To avoid this problem, create a backup copy of the OMBackSync.pl script before you reinstall the BSM Connector.

- 7 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*.

8 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 HP NNMi—HP BSM Operations Management 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 HP BSM Operations Management. The HP NNMi—HP BSM Operations Management integration provides a two-way flow of NNMi management events and SNMP traps to and from BSM and the BSM Operations Management event browser. The NNMi SNMP trap policy determines how the BSM Operations Management 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.



NNMi sends only one copy of each management event or SNMP trap to the BSM Connector. This behavior is different from that of the NNM 6.x/7.x integration with HPOM.

View the forwarded NNMi incidents in the BSM Operations Management event browser. Menu commands in the BSM Operations Management 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 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 HP Business Service Management (BSM) and HP Universal CMDB Software (HP 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 HP UCMDB, NNMi shares CI information with BSM or HP UCMDB for the devices that NNMi manages. In this case, the HP NNMi—HP BSM Operations Management integration can associate incidents regarding NNMi-managed devices with BSM or HP UCMDB CIs. The SNMP trap policy conditions enable this association.

For information about the integrations with BSM and HP UCMDB, see [HP Business Service Management and HP Universal CMDB](#) on page 11.

Health Indicators

Because the NNMi SNMP trap policy file was created with the `-omi_hi` option to `nmopcxport.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 page 43.
 - The events created from these traps include health indicators described in [Health Indicators](#) on page 43.
- 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 page 43.
 - 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 event browser receives SNMP traps directly from devices that NNMi manages, the BSM Operations Management event browser receives device traps. You can set the policies to correlate SNMP traps from NNMi with those that the BSM Operations Management 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 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 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 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 event browser.
- Correlation notification traps
 - The BSM Connector logs the events created from these traps. They do not appear in the BSM Operations Management event browser.
 - The BSM Connector processes the NNMi correlation traps to replicate NNMi incident correlation in the BSM Operations Management 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 HP NNMi—HP BSM Operations Management 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 HP NNMi—HP BSM Operations Management integration, see the *BSM Operations Management Extensibility Guide*.

Changing the HP NNMi—HP BSM Operations Management Integration

This section contains the following topics:

- [Update the SNMP Trap Policy Conditions for New NNMi Traps](#) on page 45
- [Change the Configuration Parameters](#) on page 45

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.



If the BSM Connector configuration includes multiple policy conditions for one NNMi incident, messages appear in the BSM Operations Management 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 49.

- 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 HP NNMi—HP BSM Operations Management 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 HP NNMi—HP BSM Operations Management Integration

This section contains the following topics:

- [BSM Operations Management Event Browser Contains No Forwarded Incidents on page 46](#)
- [BSM Operations Management Event Browser Contains Only Some Forwarded Incidents on page 49](#)

BSM Operations Management Event Browser Contains No Forwarded Incidents



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 [step 1](#):
 - If the agent configuration is as expected, continue with [step 3](#) of this procedure.
 - If the `SNMP_SESSION_MODE` parameter is not set correctly, repeat [step 4](#) on page 39 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 [step 3](#) on page 38 through [step 5](#) on page 39, 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 [step 1](#) 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 `nmopcxport.ovpl` in [step 1](#) on page 37.

- 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.



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**.)



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](#) on page 50
- [BSM Operations Management Integration Content](#) on page 51
- [BSM Connector Destination Status Information](#) on page 53

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

BSM Connector Connection

Figure 5 on page 50 lists the parameters for configuring the connection to the BSM Connector.

Table 5 BSM Connector Connection Information

Field	Description
Host	<p>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.</p> <p>The integration supports the following methods for identifying the BSM Connector host:</p> <ul style="list-style-type: none"> • 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. • Other Do not use this option. <p>NOTE: If the NNMi management server participates in NNMi application failover, see <i>Application Failover and the NNMi Northbound Interface</i> in the <i>NNMi Northbound Interface</i> chapter of the <i>NNMi Deployment Reference</i>.</p>
Port	<p>The UDP port where the BSM Connector receives SNMP traps.</p> <p>Enter the port number specific to the BSM Connector. This value is the port that you identified in step 3 on page 38.</p> <p>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 <code>SNMP_TRAP_PORT</code> variable.</p> <p>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.</p>
Community String	<p>A read-only community string for the BSM Connector to receive traps.</p> <p>For the HP NNMi—HP BSM Operations Management integration, use the default value, which is <code>public</code>.</p>

BSM Operations Management Integration Content

Table 6 on page 51 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	<p>The incident forwarding sending options.</p> <ul style="list-style-type: none"> • Management 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. <p>For more information, see the <i>NNMi Northbound Interface</i> chapter of the <i>NNMi Deployment Reference</i>.</p>
Lifecycle State Changes	<p>The incident change notification sending options.</p> <ul style="list-style-type: none"> • 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 PROGRESS, 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.

Table 6 BSM Operations Management Integration Content Configuration Information (cont'd)

Field	Description
Correlations	<p>The incident correlation sending options.</p> <ul style="list-style-type: none"> • None NNMi does not notify the BSM Connector of incident 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	<p>The incident deletion sending options.</p> <ul style="list-style-type: none"> • 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	<p>The connection protocol specification in the URL for browsing to the NNMi console from the BSM Operations Management 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).</p> <p>The integration requires an HTTP connection to the NNMi console. Select the HTTP option.</p>
Incident Filters	<p>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.*).</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • None NNMi sends all events to the BSM Connector. This is the default configuration. • Include 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. <p>Specify the incident filter:</p> <ul style="list-style-type: none"> • 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 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 Within HP Business Service Management

The HP 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.

This chapter contains the following topics:

- [MyBSM Portal](#) on page 55
- [Configuring an SSL Connection to BSM](#) on page 57
- [NNMi Data Available from BSM End User Management Reports](#) on page 63
- [Enabling NNMi Visualizations from BSM](#) on page 64

For information about NNMi console views launched from events in the BSM Operations Management event browser, see [Using the HP NNMi—HP BSM Operations Management Integration](#) on page 42.

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.



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](#) on page 56. 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 its 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](#) on page 64.
- 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 or UCMDB](#) on page 17.

- 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 HP NNMi–HP BSM/UCMDB Topology Integration](#) on page 15.



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*.

Configuring an SSL Connection to BSM

To configure an SSL connection to BSM, follow these steps:

- 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
```



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 [step 1](#) to a temporary directory on the BSM gateway server. In the remaining commands, this file is shown as residing on the BSM gateway server in the following location:
 - *Windows:* `<drive>:\bsm_temp\nnmicert`
 - *Linux:* `/bsm_tmp/nnmicert`

- 4 On the BSM 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_tmp\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_tmp\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 certificates into the NNMi management server, complete the following steps:

- a Run the following command on the BSM 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 keystore certificate is stored in the specified keystore file.

- b Run the following command on the BSM 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 truststore certificate is stored in the specified truststore file.

- c Copy the keystore file created in [step a](#) and 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 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 uses a self-signed certificate (not a certificate authority (CA) signed certificate). To merge the BSM 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 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 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 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 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](#) lists the End User Management reports that provide drilldown to NNMi data. [Table 8](#) 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 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.

Table 8 End User Management Reports with Drilldown to NNMi (cont'd)

End User Management Report	Source and Destination Machines
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](#) on page 64.
- 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 or UCMDB](#) on page 17.
- 3 If you have not already done so, configure NNMi to push topology information to the RTSM as described in [Enabling the HP NNMi–HP BSM/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

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

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

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

- 1 In the BSM user interface, open the **Infrastructure Settings** page (**Admin > Platform > 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/UMCDB

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: <ul style="list-style-type: none"> • Host is Route. • Host is Virtual. • NodeModel. • PrimaryDnsName. 	Node CI attributes populated by Probe but not by BSM method: <ul style="list-style-type: none"> • Description (populated from Device Profile Description) Node CI attributes with different values from BSM method: <ul style="list-style-type: none"> • 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 Label is set to the Layer 2 Connection Name as shown in NNMi.	Layer 2 Connection CI attribute Display Label is hard-coded to "Layer2Connection". Other CIs with different attributes when populated by Probe: <ul style="list-style-type: none"> • 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.

NNMi - CI Attribute Mapping

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

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

Figure 7 NNMi Node - Node CI Attribute Mapping

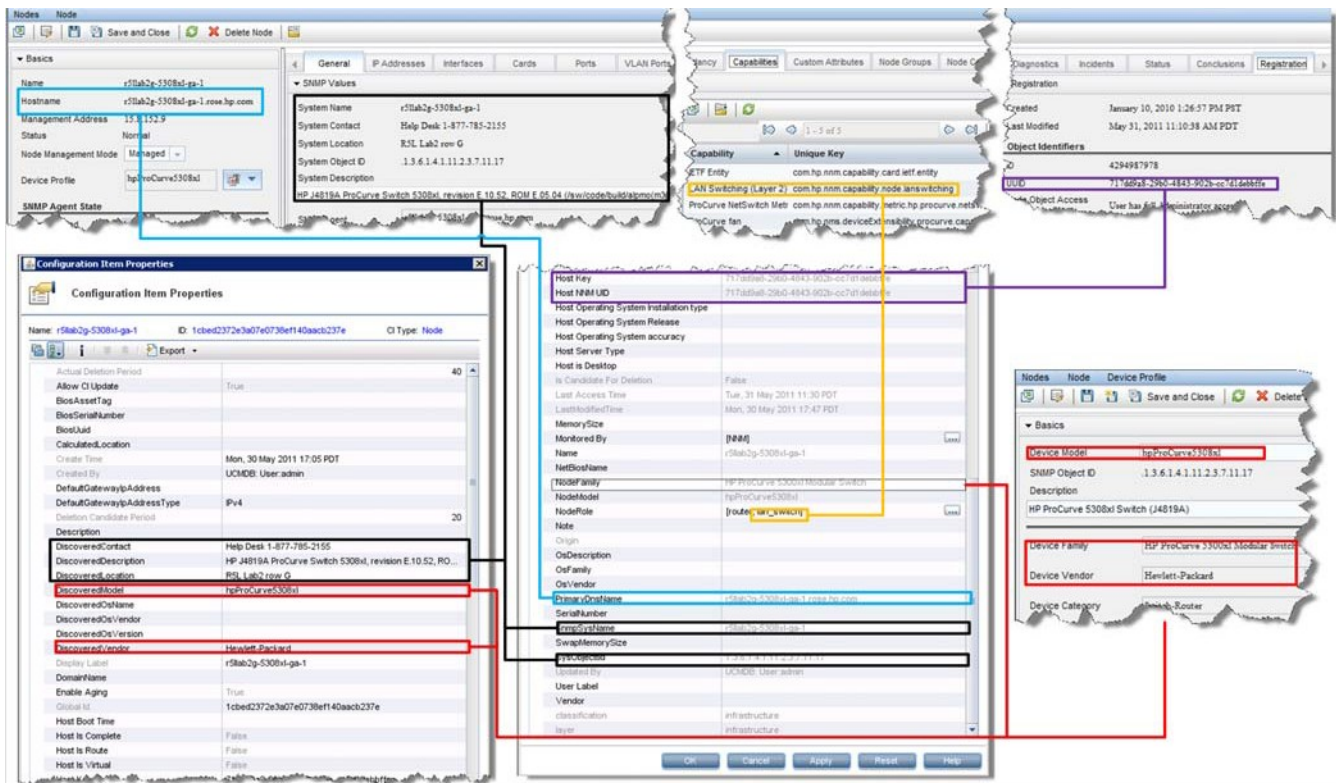


Figure 8 NNMi Interface • Interface CI Attribute Mapping

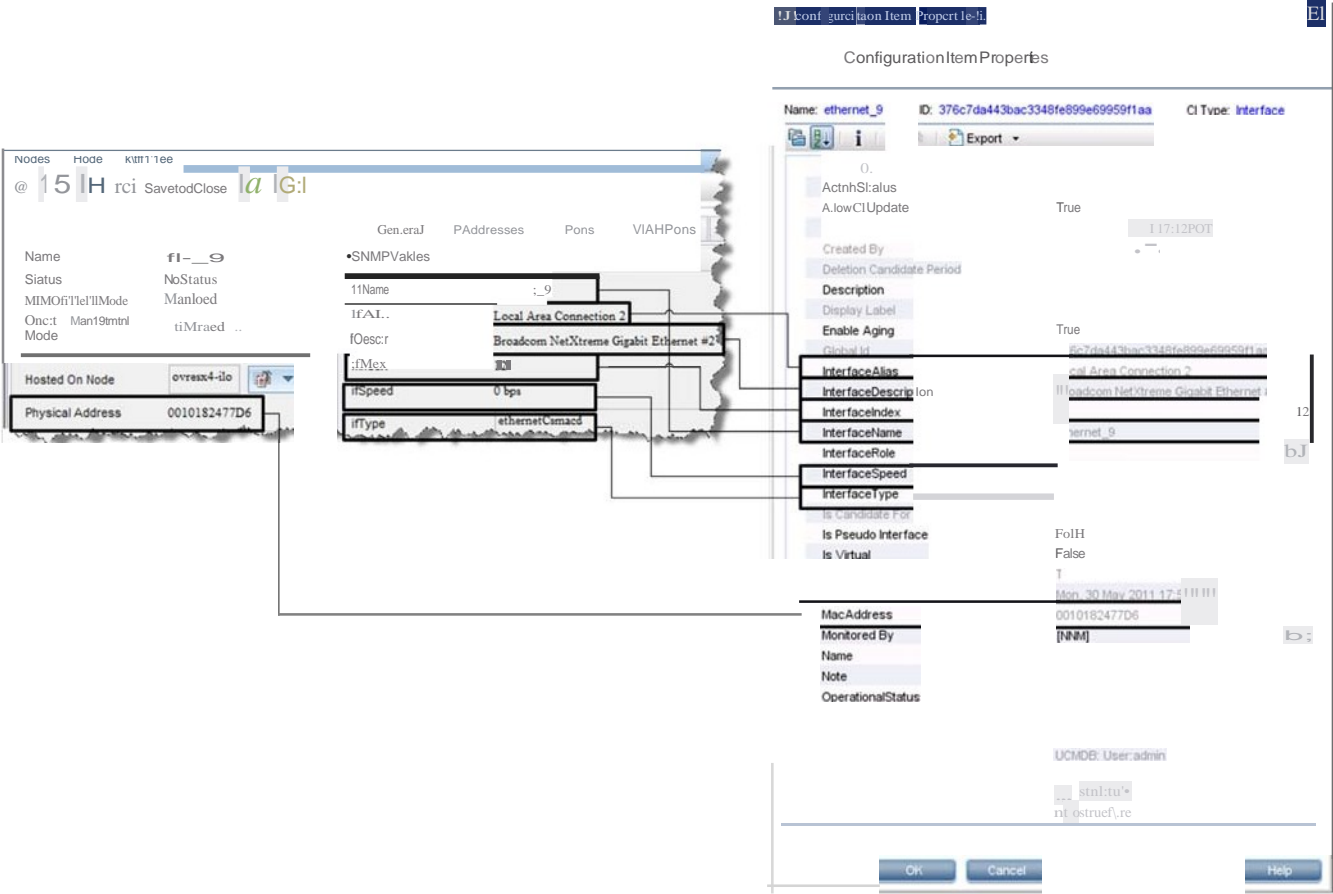


Figure 9 NNMi IP Address •IpAddress CI Attribute Mapping

PAddresses	PAddress
IQ 	{1 SaveandClose IC E;;J
Basics	
Address	ISSIS3.12
Prefix Length	21
Status	No Status
Management Mode	Managed
Object Management Mode	Inherited
P Address State	
State	NotPoled
State last Modified	Mon=May 10, 2010 1:26:16 P.O.I
In Interface	OEFAULT_VUN
Hosted On Node	r3-phps... OS
In Subn	ISSIS20F21

Configuration Item Properties	
Name:	15.85312 D: dc19fec2c3ef3438e202d49c5261ef9f Cl Type: IpAddress
AllowCle	True
Ao.to<ativeOnsName	Mon 3U ilay 2011 1713PDT UCIAOe User 8dmrn
Oescripllon	153.12
Enable Aging	True
IP DHCP Oomai N:wne	
IR Broadcast	
IP Network Address	
IP Network Class	
IP Network Mask	
IPNetwork Type	
IP Probe Name	
IpAddressProperty	
IpAddressType	
IpAddressVlWe	00:0000:0000:0000:ffff:0f08:990c
IsManaged	True
Is Virtual	False
MoNored B	'!NA
Name	15.8.153.12
Note	
User Label	DefaultDomain UCMDB: User:admin
layer	network infrastructure

Figure 10 NNMi IP Subnet -IpSubnet CI Attribute Mapping

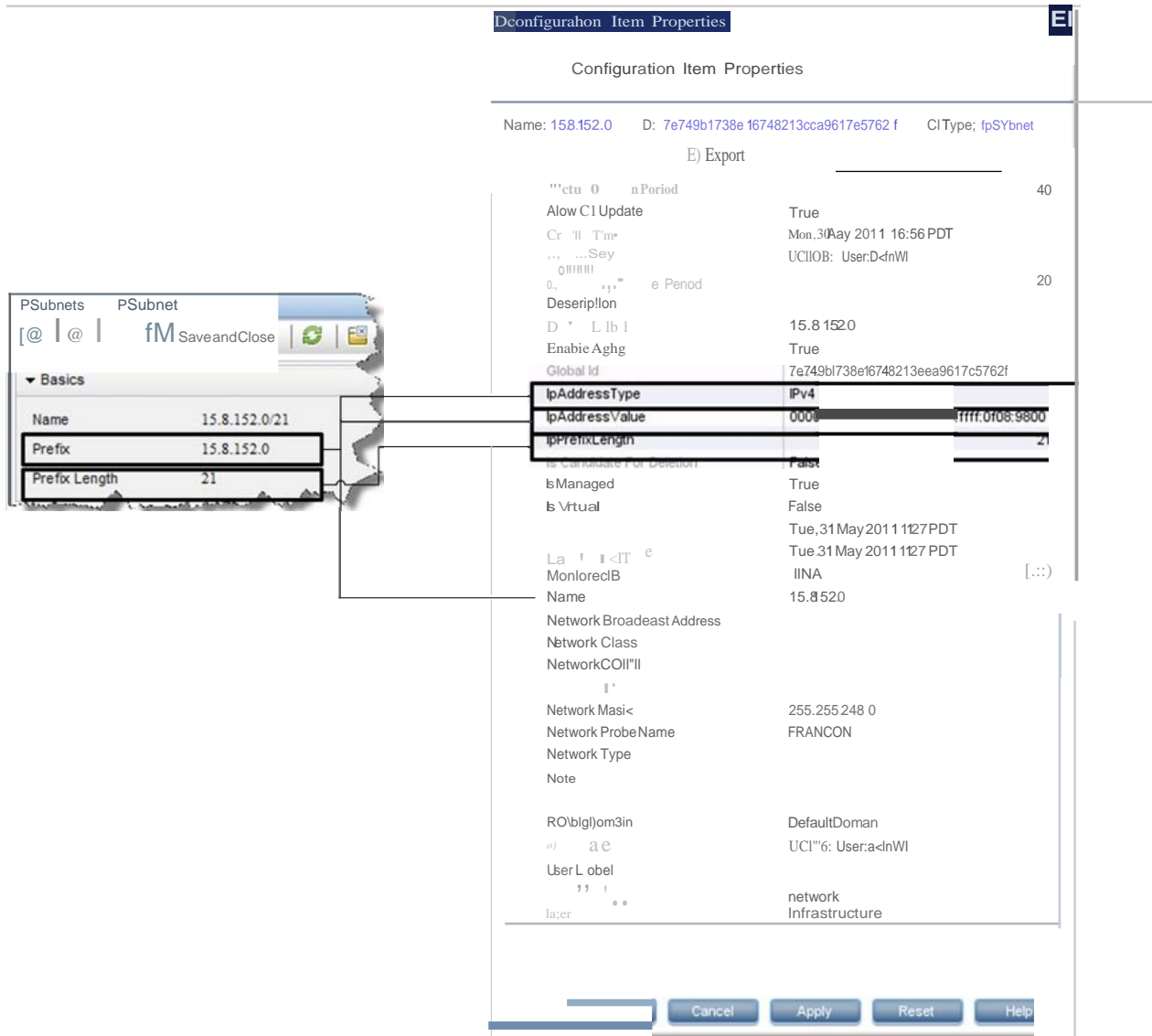


Figure 11 NNMi Card HardwareBoard CI Attribute Mapping

Configuration Item Properties

Name: c ID: Oafb09afe12d860Se7ff7495clb03479 CItemType: HardwareBoard

12] ElExport • 40

Actu; O... tionPe 40

Allow CI Update Tru6

BoardIndex C

Created By Mbn, 30 May 2011 17:41 PDT

Description UCH06: useadmin 20

EnableA C

Firmware/versloo K.11 2

GI Oafb09afe12d860Se7117495clb03479

HardwareBoardIdex

HardwareVersion

For Deletion false

Is Virtual false

Tue, 31 May 2011 12:28 PDT

Mort() (ed B Tue, 31 May 2011 12:28 PDT

Name C

SerialNumber SG915ATcr.Mi

SoftwareVersion

ledB UCH06: Useadmin

Userlabel infrastructure

layer infrastructure

Cancel Apply Reset Help

NOdes NOde Card

@I |ErJ |rj

Save and Close CJ

• Basics

Name C

HostedOnNode

Status Normal

Management MMode Managed

DhclManagement MMode Inherited

Hosted On Card

Redundant Group

Card State

Administrative State U11..

General Ports Daughter Card

• Basics

ModelName

Type hpSwitchModuleJ8702A

Serial Number SG915AT0WH

Firmware Version K.11.12

Hardware Version

Software Version K.12.62

Index C

Physical Index 39

Description

Curve J87 • 24p G • zlfJody •

Figure 12 NNMi Port • PhysicalPort CI Attribute Mapping

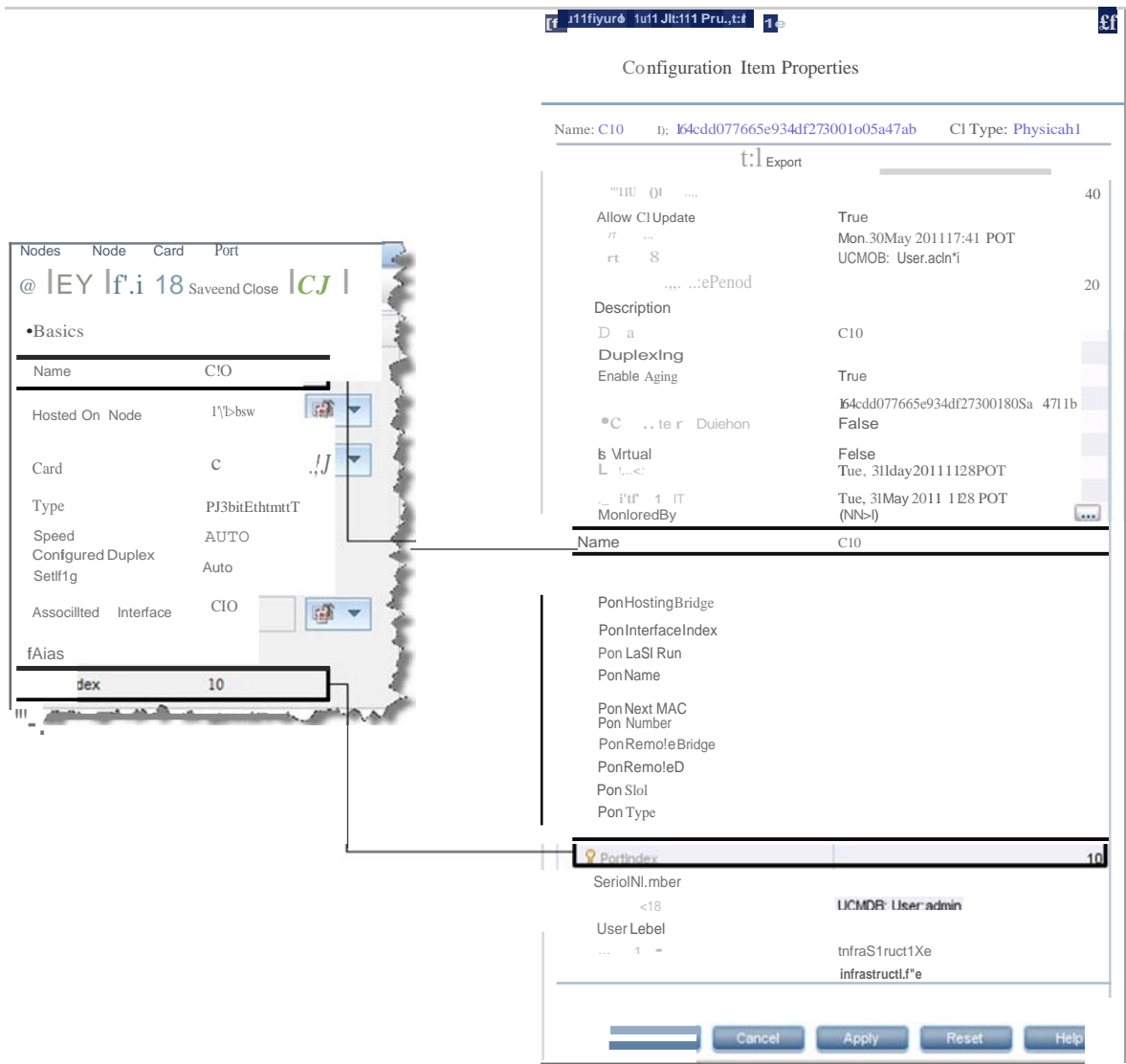
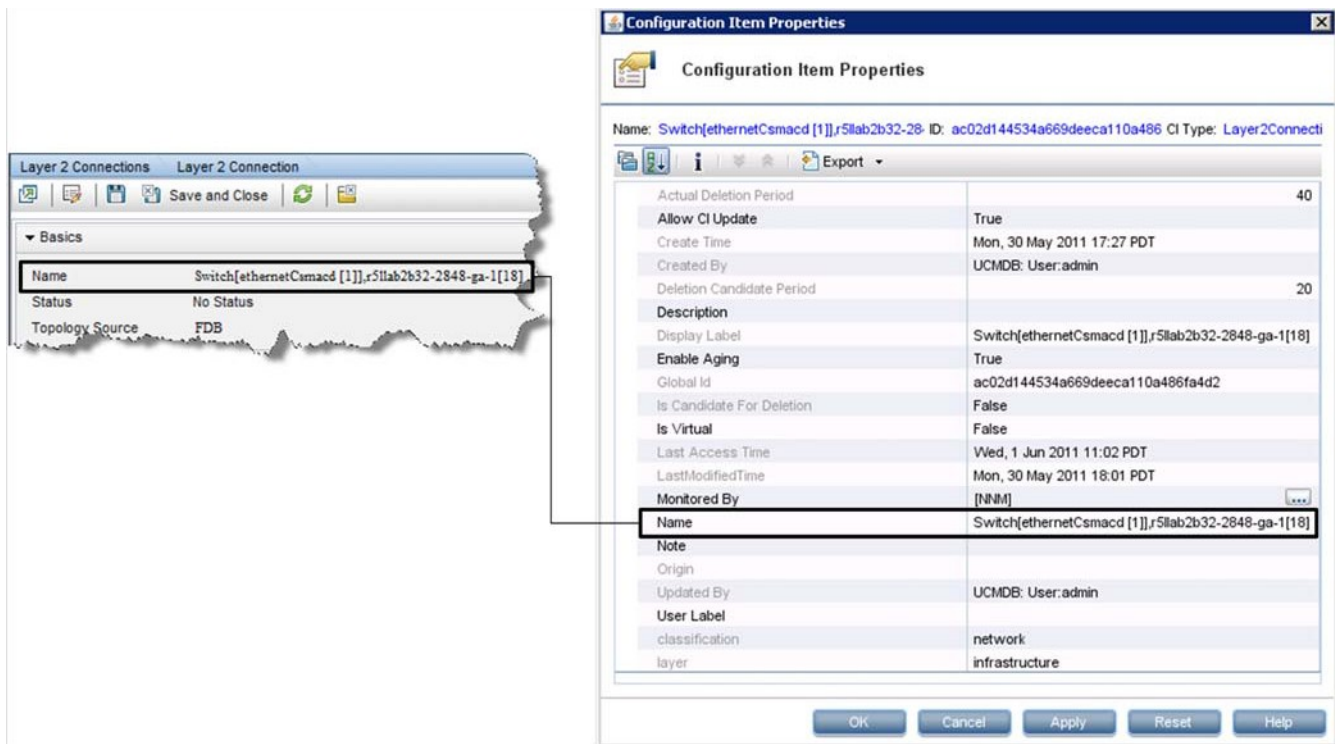


Figure 13 NNMi Layer 2 Connection - Layer2Connection CI Attribute Mapping



NNMi Environment Variables

HP 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](#)
- [Other Available Environment Variables](#)

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



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



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](#) on page 79.

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 10](#) (Windows) or [Table 11](#) (Linux) to get to commonly used NNMi file locations.

Table 10 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
%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 11 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	:
\$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

We appreciate your feedback!

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

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

Product name and version: NNMi 10.10

Document title: *HP Network Node Manager i Software—HP Business Service Management Integration Guide, November 2015*

Feedback: