Hewlett Packard
Enterprise

HPE Network Node Manager i Software

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

Network Node Manager i Software - HP Operations Manager Integration Guide

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

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. HPE 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 HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Oracle Technology — Notice of Restricted Rights

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

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

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

AMD is a trademark of Advanced Micro Devices, Inc.

Google™ is a registered trademark of Google Inc.

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

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

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

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

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

sFlow is a registered trademark of InMon Corp.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

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

This product includes software developed by the Visigoth Software Society (http://www.visigoths.org/).

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=.

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

Support

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

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

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

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

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

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

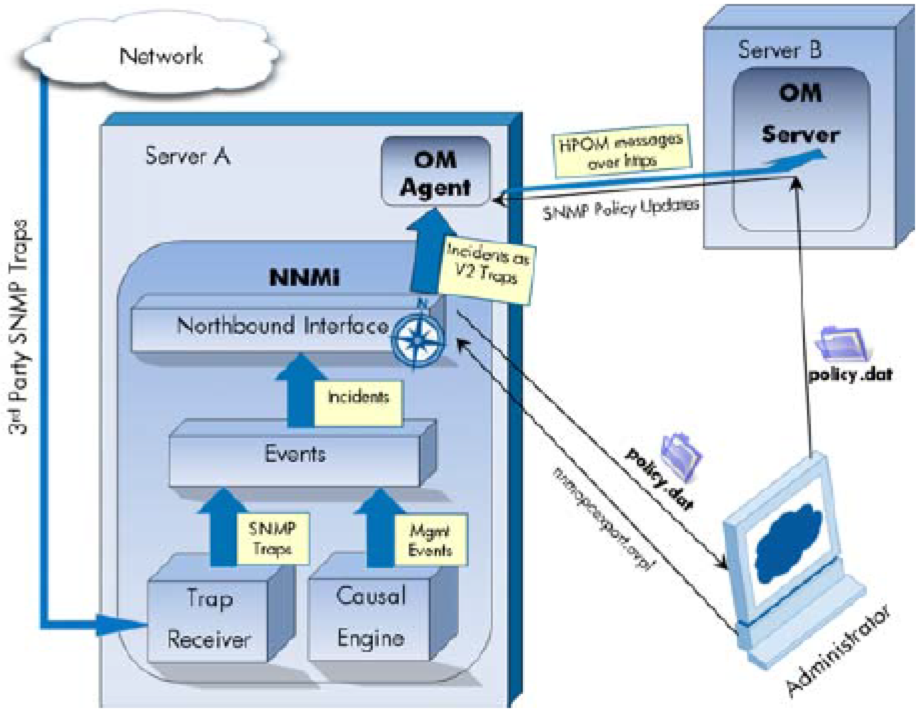
HPE Software Integrations, Solutions and Best Practices

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

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

Contents

HP Operations Manager



HP Operations Manager (HPOM) provides comprehensive event management; proactive performance monitoring; and automated alerting, reporting, and graphing for management operating systems, middleware, and application infrastructure. HPOM consolidates events from a wide range of sources into a single view.

For information about purchasing HPOM, contact your HPE sales representative.

This chapter describes the available integrations:

- "Network Node Manager i Software - HP Operations Manager Integration Guide (Agent Implementation)" below
- "HPE NNMi—HPOM Integration (Web Services Implementation)" on page 32

Network Node Manager i Software - HP Operations Manager Integration Guide (Agent Implementation)

The agent implementation of the HPE NNMi—HPOM integration is the preferred solution for integrating HPOM with NNMi.

If the agent and the web services implementations of the HPE NNMi—HPOM integration both forward messages to the same HPOM management server, you might not see all messages from both implementations in the HPOM active messages browser. For this reason, HPE does not support running both implementations of the HPE NNMi—HPOM integration from one NNMi management server to the same HPOM management server concurrently.

This section contains the following topics:

- "About the HPE NNMi—HPOM Integration (Agent Implementation)" below
- "Enabling the HPE NNMi—HPOM Integration (Agent Implementation)" on page 10
- "Configuring NNMi to Forward HPE ArcSight Logger Syslog Messages " on page 14
- "Using the HPE NNMi—HPOM Integration (Agent Implementation)" on page 17
- "Changing the HPE NNMi—HPOM Integration Configuration (Agent Implementation)" on page 20
- "Disabling the HPE NNMi—HPOM Integration (Agent Implementation)" on page 21
- "Troubleshooting the HPE NNMi—HPOM Integration (Agent Implementation)" on page 22
- "HPE NNMi—HPOM Agent Destination Form Reference (Agent Implementation)" on page 25

About the HPE NNMi–HPOM Integration (Agent Implementation)

The agent implementation of the HPE NNMi—HPOM integration forwards NNMi management events as SNMPv2c traps to an HPE Operations agent on the NNMi management server. The agent filters the NNMi traps and forwards them to the HPOM active messages browser. The agent configuration determines the HPOM management server receiving the forwarded incident.

If you transfer all of your SNMP trap handling from HPOM to NNMi (due to license issues, scalability, or other reasons), and you have invested in HPOM policies, you might want to consider trap forwarding as an alternative to the HPE NNMi—HPOM integration. Note that trap forwarding does not provide any NNMi Incident enrichment when processing traps. For more information, see *Trap and Incident Forwarding* in the NNMi Deployment Reference. Another option is to use the nnmopcexport.ovpl script to read the NNMi management event and SNMP trap configurations and export these configurations into an HPOM policies file. You could then continue to use the HPE NNMi—HPOM integration using these policies. For more information, see the *nnmopcexport.ovpl* reference page, or the Linux manpage.

The HPE NNMi—HPOM integration can also forward the SNMP traps that NNMi receives to the agent.

The HPE NNMi—HPOM integration also provides for accessing the NNMi console from within HPOM.

The agent implementation of the HPE NNMi—HPOM 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 agent implementation of the HPE NNMi—HPOM integration consists of the following components:

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

Value

The HPE NNMi—HPOM integration provides event consolidation in the HPOM active messages browser for the network management, system management, and application management domains, so that HPOM users can detect and investigate potential network problems.

The primary features of the integration are as follows:

- Automatic incident forwarding from NNMi to the HPE Operations agent. Forwarded incidents appear in the HPOM active messages browser.
- Access to the NNMi console from HPOM.
  - HPOM users can open the NNMi **Incident** form in the context of a selected message.
  - HPOM users can launch an NNMi view (for example, the Layer 2 Neighbor view) in the context of a selected message and node.
  - HPOM users can launch an NNMi tool (for example, status poll) in the context of a selected message and node.

Integrated Products

The information in this section applies to the following products:

- HPOM for Windows
- HPOM for Linux

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

- NNMi 10.20

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

The HPE Operations agent requires a license and must be installed on the NNMi management server computer *after* installing NNMi.

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 HPOM.

The HPOM documentation describes how to install and use the HPOM applications that access the NNMi console from the HPOM active messages browser.

- For HPOM for Windows, see the information for the NNMi Adapter in the HPOM help.
- For HPOM for Linux version 9.xx, see the *Integrating NNMi into HPOM* section in the *HPE Operations Manager for UNIX or Linux Administrator's Reference*.

Enabling the HPE NNMi–HPOM Integration (Agent Implementation)

It is recommended that an experienced HPOM administrator complete the procedure for enabling the agent implementation of the HPE NNMi—HPOM integration.

> **NOTE:** When NNMi integrates with the HPE Business Service Management (BSM) topology database, the agent implementation of the HPE NNMi—HPOM 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 17.

To enable agent implementation of the HPE NNMi—HPOM integration, follow these steps:

1. On the NNMi management server, generate an SNMP trap policy file:
   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" \
      -file NNMi_policy.dat
      ```

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

> **TIP:** If HPOM will forward the NNMi incidents to the HPE OMi event browser or to the BSM Operations Management event browser, also use the `-omi_hi` option to add health indicators to the management event policy conditions. For more information, see "Health Indicators" on page 18.

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

For information about the default policy conditions and customizing conditions, see "Using the HPE NNMi—HPOM Integration (Agent Implementation)" on page 17.

2. On the HPOM management server, configure HPOM to receive messages from NNMi:

   a. In the HPOM console, add a node for the NNMi management server

   b. Install the HPE Operations agent on the NNMi management server.

   c. Transfer the `NNMi_policy.dat` file created in "On the NNMi management server, generate an SNMP trap policy file:" on the previous page of this procedure from the NNMi management server to the HPOM management server.

      Import the `NNMi_policy.dat` file into HPOM.

      - *HPOM for Windows*: Use the `ImportPolicies` command.
      - HPOM for Linux version 9.x: Use the `opcpolicy` command.

   d. Deploy the `NNMi Management Events` policy to the NNMi managed node.

   e. In the HPOM console, add an external node to catch all forwarded NNMi incidents.

      For initial testing, set the node filter to `<*>.<*>.<*>.<*>` (for an IP filter) or `<*>` (for a name filter). After you validate the integration, restrict the external node filter to match your network.

      > **CAUTION:** If you do not set up an HPOM managed node for an NNMi incident source node, the HPOM management server discards all incidents regarding that node.

   For more information, see the following references:

   - *HPOM for Windows*:
     - *Configuring external nodes* in the HPOM help

- *HPOM for Linux*:
  - *HPE Operations Manager for UNIX HTTPS Agent Concepts and Configuration Guide*
  - *HPE Operations Manager for UNIX Concepts Guide*
  - *HPE Operations Manager for UNIX Administrator's Reference*
  - *HPE Operations Manager for UNIX Developer's Toolkit Developer's Reference*
  - *opcnode(1M)*, *opcbbcdist(1M)*, *opcragt(1M)*, *opccfgupl(1M)*, *opcpolicy(1M)* (version 9.xx)

3. Identify an available port for SNMP communications between NNMi and the HPE Operations agent.

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

   Because the HPE Operations agent is installed on the NNMi management server, this port number must be different from the port NNMi uses to receive SNMP traps.

   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 HPE Operations agent.

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

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

4. On the NNMi management server configure the HPE Operations agent with a custom port for receiving SNMP traps from NNMi by entering the following commands:

- Configure the agent:

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

- Restart the agent:

  ```
  ovc -restart opctrapi
  ```

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

5. On the NNMi management server, configure NNMi incident forwarding to the HPE Operations agent:

   a. In the NNMi console, open the **HPE 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 **HPE 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 HPE Operations agent on the NNMi management server. The trap destination port is the port that you identified in "Identify an available port for SNMP communications between NNMi and the HPE Operations agent." on the previous page of this procedure.

      For information about these fields, see "HPE Operations Agent Connection" on page 26.

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

      For information about these fields, see "HPOM Integration Content" on page 27.

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

      A new window opens, showing 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*. In HPOM, add the custom message attributes for NNMi incidents to the active messages browser. Follow the appropriate steps:

   - *HPOM for Windows*:
     - In the browser, right-click any column heading, then click **Options**.
     - In the **Enter Custom Message Attributes** list, select an attribute, then click **Add**.

- *HPOM for Linux*:
  - In the Java Interface Message Browser, right-click any column heading, and then click **Customize Message Browser Columns**.
  - On the **Custom** tab, select from the **Available Custom Message Attributes**, and then click **OK**.

Note the following information:

- Most of the custom message attributes for NNMi incidents begin with the text `nnm`.
- For the agent implementation of the HPE NNMi—HPOM integration, some interesting attributes for NNMi incidents are as follows:

  ```
  nnm.name
  nnm.server.name
  ```

  For information about other interesting CMAs, see "Using the HPE NNMi—HPOM Integration (Agent Implementation)" on page 17.
- To change the order the custom message attributes appear in the messages browser, drag a column heading to the new location.

7. *Optional*. On the HPOM management server, enable contextual launching of the NNMi views.
   - *HPOM for Windows*: Associate the NNMi source nodes with the NNMi Web Tools group.

     For information, see *Enable tools in the By Node tool group* in the HPOM help.

     > **TIP:** HPOM for Linux version 9.xx automatically installs the basic NNMi applications.

     For information, see the section on installing and configuring the HPE NNMi—HPOM integration in the *HPE Operations Manager for UNIX and Linux Administrator's Reference* (version 9.xx).

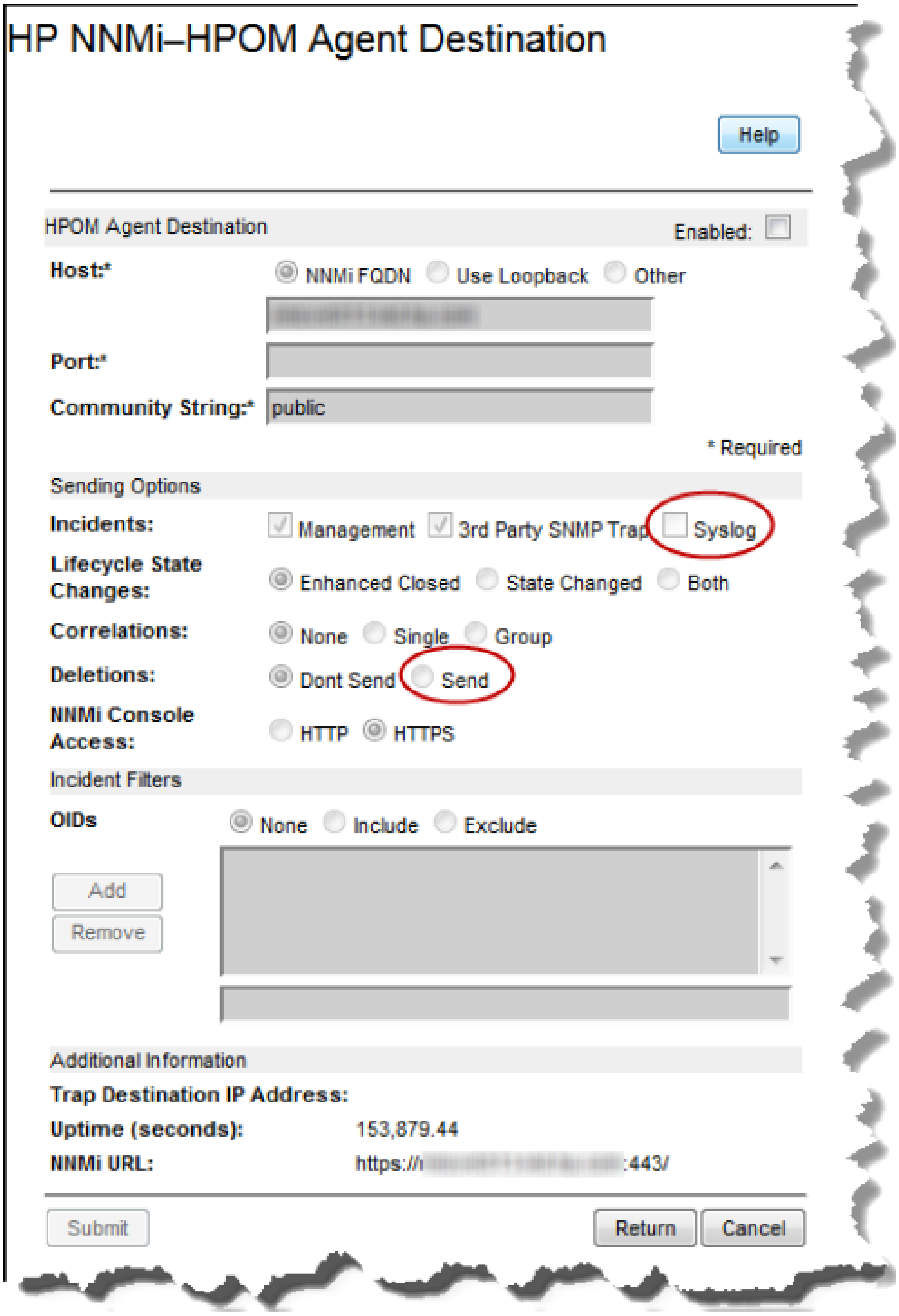
Configuring NNMi to Forward HPE ArcSight Logger Syslog Messages

You can configure NNMi to forward HPE ArcSight Logger Syslog messages to HPOM using NNMi's Northbound Interface. The result is in HPE ArcSight Logger Syslog messages being sent to HPOM management server.

To configure the HPE NNMi—HPOM (Agent Implementation) to forward Syslog messages to NNMi's Northbound Interface, do the following:

1. Review the information in the "HPE NNMi—HPOM Agent Destination Form Reference (Agent Implementation)" on page 25.
2. Follow the enabling instructions shown in "Enabling the HPE NNMi—HPOM Integration (Agent Implementation)" on page 10.
3. From the NNMi console, click **Integration Module Configuration** > **HPOM**. NNMi opens the **HPE NNMi—HPOM Integration Selection** screen.
4. Click the **HPOM agent implementation**.
5. Click **Edit**.
6. Modify the form to match the highlighted fields shown in "Figure 1 Important Fields" on the next page. Completing the following configuration steps are important:
   - In the **Incidents** Field, select the **Syslog** check box.
   - In the **Deletions** Field, select the **Send** check box.

Figure 1 Important Fields



HP NNMi–HPOM Agent Destination

HPOM Agent Destination — Enabled: □

Host:* ● NNMi FQDN ○ Use Loopback ○ Other

[redacted]

Port:*

Community String:* public

* Required

Sending Options

Incidents: ☑ Management ☑ 3rd Party SNMP Trap □ Syslog

Lifecycle State Changes: ● Enhanced Closed ○ State Changed ○ Both

Correlations: ● None ○ Single ○ Group

Deletions: ● Dont Send ○ Send

NNMi Console Access: ○ HTTP ● HTTPS

Incident Filters

OIDs ● None ○ Include ○ Exclude

Additional Information

Trap Destination IP Address:

Uptime (seconds): 153,879.44

NNMi URL: https://[redacted]:443/

7. Configure HPOM to include an SNMP trap policy that matches traps with the OID for `nnmiSyslog` incidents. The `nnmiSyslog` incident OID to listen for is .1.3.6.1.4.1.11.2.17.19.2.0.4000.

After completing "Review the information in the "HPE NNMi—HPOM Agent Destination Form Reference (Agent Implementation)" on page 25." on page 15 through "Configure HPOM to include an SNMP trap policy that matches traps with the OID for nnmiSyslog incidents. The nnmiSyslog incident OID to listen for is .1.3.6.1.4.1.11.2.17.19.2.0.4000." on the previous page, the HPOM management server will be able to receive HPE ArcSight Logger Syslog messages.

> NNMi takes varbinds from the `ArcSightEvent` trap (OID is .1.3.6.1.4.1.11937.0.1) and forwards these varbinds northbound in another trap (from the **`hp-nnmi-nbi.mib`**). You can see the trap's Custom Incident Attributes (CIAs) by viewing the 20th varbind (`nnmiIncidentCias`) in the comma-separated list from the `nnmiSyslog` incident (OID is .1.3.6.1.4.1.11.2.17.19.2.0.4000).

Using the HPE NNMi–HPOM Integration (Agent Implementation)

The agent implementation of the HPE NNMi—HPOM integration provides a one-way flow of NNMi management events and SNMP traps to the HPE Operations agent. The SNMP trap policy conditions determine how HPOM treats and shows the incoming traps. For example, you can change a policy condition to include the value of a trap custom message attribute (CMA) in the message text.

View the forwarded NNMi incidents in the HPOM active messages browser. HPOM menu commands provide access to NNMi views in the context of the selected message. Information embedded in each message supports this cross-navigation:

- The `nnmi.server.name` and `nnmi.server.port` CMAs in the message identify the NNMi management server.
- The `nnmi.incident.uuid` CMA identifies the incident in the NNMi database.

The original source object appears in the **Object** column of the HPOM active messages browser and in the `nnm.source.name` CMA. (In the web services implementation of the HPE NNMi—HPOM integration, the original source object is only available in `nnm.source.name` CMA.)

Configuration Item Identifiers

In HPE Business Service Management (BSM) and HPE Universal CMDB Software (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 UCMDB, NNMi shares CI information with BSM or UCMDB for the devices that NNMi manages. In this case, the agent implementation of the HPE NNMi—HPOM integration can associate incidents regarding NNMi-managed devices with BSM or UCMDB CIs. The SNMP trap policy conditions enable this association.

For information about the integrations with BSM and UCMDB, see the *NNMi—HPE Business Service Management Integration Guide*.

Health Indicators

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

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 messages created from NNMi management events appear in the HPOM active messages browser.
  - These traps include the CI information described in "Configuration Item Identifiers" on the previous page.
  - The messages created from these traps might include health indicators described in "Health Indicators" above.
- 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 messages created from third-party traps appear in the HPOM active messages browser.
  - These traps include the CI information described in "Configuration Item Identifiers" on the previous page.
  - The messages created from these traps do not include health indicators.

    - If you configure the integration to forward all received SNMP traps and the HPOM management server receives SNMP traps directly from devices that NNMi manages, HPOM receives duplicate device traps. You can set the policies to correlate SNMP traps from NNMi with those that HPOM receives directly from managed devices.

- Syslog messages
    - NNMi forwards ArcSight Syslog messages to the northbound application using the NorthBound Integration module.
      NNMi begins forwarding incidents as soon as you enable the destination.
- EventLifecycleStateClosed traps
    - The HPE Operations agent logs the messages created from these traps. Generally, they do not appear in the HPOM active messages browser.
    - The NNMi SNMP trap policy file causes the HPE Operations agent to acknowledge the message that corresponds to the closed NNMi incident in the HPOM active messages browser.
- LifecycleStateChangeEvent traps
    - The NNMi SNMP trap policy file does not include conditions for processing these traps. The HPE Operations agent does not forward these traps to the HPOM active messages browser.
- EventDeleted traps
    - The NNMi SNMP trap policy file does not include conditions for processing these traps. The HPE Operations agent does not forward these traps to the HPOM active messages browser.
- Correlation notification traps
    - The HPE Operations agent logs the messages created from these traps. They do not appear in the HPOM active messages browser.
    - These traps have no impact on the HPOM active messages browser.

Customizing Policy Conditions

To customize the default policy conditions, edit the conditions on the HPOM management server, and then re-deploy the policy to the HPE Operations agent on the NNMi management server. For more information, see the following reference:

- *HPOM for Windows*: *SNMP Interceptor Policies* (version 9.0x) in the HPOM help
- *HPOM for Linux* (version 9.xx): *HPE Operations Manager for UNIX and Linux Concepts Guide*

More Information

For more information about the agent implementation of the HPE NNMi—HPOM integration, see the following references:

- For descriptions of the trap types that the integration sends to the HPE Operations agent, see the *NNMi Northbound Interface* chapter of the NNMi Deployment Reference.
- For information about the format of the traps that NNMi sends to the HPE Operations agent, see the `hp-nnmi-nbi.mib` file.
- For detailed information about using the HPE NNMi—HPOM integration, see the HPOM documentation.
  - *HPOM for Windows*: See *Agent implementation of the NNMi Adapter* in the HPOM help.
  - *HPOM for Linux*: See the section on installing and configuring the HPE NNMi—HPOM integration in the *HPE Operations Manager for UNIX and Linux Administrator's Reference* (version 9.xx).

Changing the HPE NNMi–HPOM Integration Configuration (Agent Implementation)

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` script 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.

   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. Transfer the new SNMP trap policy file from the NNMi management server to the HPOM management server, and then import it into HPOM.
3. On the HPOM management server, deploy the new policy to the NNMi managed node.

Alternatively, you can re-create the SNMP trap policy file for all NNMi management events and SNMP traps. If you take this approach, importing the new policy file into HPOM overwrites any existing policy customizations.

Change the Configuration Parameters

To change the integration configuration parameters, follow these steps:

1. In the NNMi console, open the **HPE NNMi—HPOM 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 "HPE NNMi—HPOM Agent Destination Form Reference (Agent Implementation)" on page 25.
5. Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Disabling the HPE NNMi–HPOM Integration (Agent Implementation)

No SNMP trap queuing occurs while a destination is disabled.

To discontinue the forwarding of NNMi incidents to the NNMi Operations agent, follow these steps:

1. In the NNMi console, open the **HPE 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 HPOM documentation.

Troubleshooting the HPE NNMi–HPOM Integration (Agent Implementation)

Launch of the NNMi Console from the HPOM Java GUI Console Fails

Launch of the NNMi console from the HPOM console fails, and the following error message appears in the web browser:

```
The page cannot be displayed
```

This problem occurs because of an incorrectly constructed NNMi URL by the Java GUI.

To resolve this problem, manually correct URL of the NNMi console in the address bar of the browser.

Here is the format of the URL of the NNMi console:

https://*<NNMi_FQDN>***:***<port>***/nnm**

or

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

In this instance, *<NNMi_FQDN>* is the fully qualified domain name of the NNMi management server; *<port>* is the HTTPS or HTTP port of NNMi.

HPOM Active Messages Browser Does Not Receive Any Forwarded Incidents

> **Tip:** In the following procedure, the `OVBIN` environment variable refers to the `bin` directory for the HPE Operations agent commands, which defaults to the following value:
>
> - *Windows*: `<drive>\Program Files (x86)\HP\HPE BTO Software\bin`
> - *Linux*: `/opt/OV/bin`

If the HPOM active messages browser does not contain any incidents from NNMi, follow these steps:

1. On the NNMi management server, verify the HPE Operations agent configuration:
   - *Windows* NNMi management server:

     `%OVBIN%\ovconfget eaagt`

   - *Linux* NNMi management server:

     `$OVBIN/ovconfget eaagt`

The command output should include the following information:

- *Windows*: `SNMP_SESSION_MODE=NNM_LIBS`
- *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 **HPE NNMi—HPOM Agent Destination** form.

2. Evaluate the HPE Operations agent configuration by considering the results from "On the NNMi management server, verify the HPE Operations agent configuration:" on the previous page:
   - If the HPE Operations agent configuration is as expected, continue with "On the NNMi management server, verify that the HPE Operations agent is running:" below of this procedure.
   - If the `SNMP_SESSION_MODE` parameter is not set correctly, repeat "On the NNMi management server configure the HPE Operations agent with a custom port for receiving SNMP traps from NNMi by entering the following commands:" on page 12 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 **HPE NNMi—HPOM Agent Destination** form, repeat "Identify an available port for SNMP communications between NNMi and the HPE Operations agent." on page 12 through "On the NNMi management server, configure NNMi incident forwarding to the HPE Operations agent:" on page 13, as appropriate, until the `ovconfget` command returns the expected results.
3. On the NNMi management server, verify that the HPE Operations agent is running:
   - *Windows* NNMi management server:

     ```
     %OVBIN%\ovc -status
     ```
   - *Linux* NNMi management server:

     ```
     $OVBIN/ovc -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 HPE Operations agent:

   ```
   ovc -restart opctrapi
   ```
4. On the NNMi management server, verify that the HPE Operations agent is listening on the expected SNMP trap port:

a. Run the following command:
   - *Windows*: **`netstat -an | findstr <custom_port>`**
   - *Linux*: **`netstat -an | grep <custom_port>`**

     Where *`<custom_port>`* is the value of `SNMP_TRAP_PORT` from "On the NNMi management server, verify the HPE Operations agent configuration:" on page 22 of this procedure.

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

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

   ```
   ovc -restart opctrapi
   ```

5. On the HPOM management server, verify the external node filter for the NNMi management server node.

   The HPOM management server must be configured to accept incidents from the devices that NNMi manages. HPOM ignores any forwarded incident from an NNMi source node that is not configured as a managed node or included in an external node filter, as described in "On the HPOM management server, configure HPOM to receive messages from NNMi:" on page 11.

6. On the NNMi management server, verify that the SNMP trap policy file for NNMi has been deployed to the HPE Operations agent on the NNMi management server:
   - *Windows* NNMi management server:

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

   - *Linux* NNMi management server:

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

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

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

   The value of the `Name` field is the name of the SNMP trap policy file from the -`template` option to `nnmopcexport.ovpl` in "On the NNMi management server, generate an SNMP trap policy file:" on page 10.

7. Verify that the HPE Operations agent is receiving traps:

   a. Verify that the HPE Operations agent can send messages to the HPOM management server.

   b. Enable tracing of the HPE Operations agent to determine whether the traps arrive at the HPE Operations agent.

   For information about troubleshooting the HPE Operations agent, see the following reference:

- *HPOM for Windows*: HPOM help
- *HPOM for Linux*: *HPE Operations Manager for UNIX and Linux HTTPS Agent Concepts and Configuration Guide*

8. Verify that NNMi is forwarding management events to the HPE Operations agent.

   For more information, see the *Troubleshooting the NNMi Northbound Interface* Chapter of the NNMi Deployment Reference.

HPOM Active Messages Browser Does Not Receive Some Forwarded Incidents

If one or more NNMi incidents do not appear in the HPOM active messages browser, follow these steps:

1. On the NNMi management server verify that the SNMP trap policy does not suppress the trap.
2. On the HPOM management server, verify the external node filter for the NNMi management server node.

   The HPOM management server must be configured to accept incidents from the devices that NNMi manages. HPOM ignores any forwarded incident from an NNMi source node that is not configured as a managed node or included in an external node filter, as described in "On the HPOM management server, configure HPOM to receive messages from NNMi:" on page 11.
3. On the HPOM management server, verify that HPOM is running.

   If the HPOM management server shuts down, the HPE Operations agent queues received traps. The HPE Operations agent forwards the queued traps when the HPOM management server becomes available.

   If the HPE Operations agent shuts down, the forwarded traps are lost. NNMi does not resend traps.
4. 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.

HPE NNMi–HPOM Agent Destination Form Reference (Agent Implementation)

The **HPE NNMi—HPOM Agent Destination** form contains the parameters for configuring communications between NNMi and the NNMi Operations agent. This form is available from the **Integration Module Configuration** workspace. (On the **HPE**

NNMi—HPOM Integration Selection form, click **HPOM agent implementation**. Click **New**, or select a destination, and then click **Edit**.)

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

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

- "HPE Operations Agent Connection" below
- "HPOM Integration Content" on the next page
- "HPE Operations Agent Destination Status Information" on page 30

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

HPE Operations Agent Connection

"Table 1 HPE Operations Agent Connection Information" below lists the parameters for configuring the connection to the HPE Operations agent. To configure the parameters explained in "Table 1 HPE Operations Agent Connection Information" below, make changes to the **HPOM Agent Destination** options on the **HPE NNMi—HPOM Agent Destination** form

Table 1 HPE Operations Agent Connection Information

Field	Description
Host	The fully-qualified domain name (preferred) or the IP address of the NNMi management server. The HPE Operations agent receives SNMP traps from NNMi on this server. The integration supports the following methods for identifying the HPE Operations agent host: • **NNMi FQDN** NNMi manages the connection to the HPE Operations agent on the NNMi management server 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.

Table 1 HPE Operations Agent Connection Information, continued

Field	Description
	NOTE: If the NNMi management server participates in NNMi application failover, see the *NNMi Deployment Reference* for information about the impact of application failover on the integration module.
Port	The UDP port where the HPE Operations agent receives SNMP traps. Enter the port number specific to the HPE Operations agent. This value is the port that you identified in "Identify an available port for SNMP communications between NNMi and the HPE Operations agent." on page 12. To determine the port, run the **`ovconfget eaagt`** command on the NNMi management server. The trap port is the value of the `SNMP_TRAP_PORT` variable. **NOTE:** This port number must be different from the port NNMi uses to receive SNMP traps, as set in the **SNMP Port** field on the **Communication Configuration** form in the NNMi console.
Community String	A read-only community string for the HPE Operations agent to receive traps. For the HPE NNMi—HPOM integration, use the default value, which is `public`.

HPOM Integration Content

"Table 2 HPOM Integration Content Configuration Information" below lists the parameters for configuring the content NNMi sends to the HPE Operations agent. To configure the parameters explained in "Table 2 HPOM Integration Content Configuration Information" below, make selections to the **Sending Options** on the **HPE NNMi—HPOM Agent Destination** form.

Table 2 HPOM Integration Content Configuration Information

Field	Description
Incidents	The incident forwarding specification. • **Management**

Table 2 HPOM Integration Content Configuration Information, continued

Field	Description
	NNMi forwards only NNMi-generated management events to the HPE Operations agent. - **SNMP 3rd Party Trap** NNMi forwards only SNMP traps that NNMi receives from managed devices to the HPE Operations agent. - **Syslog** NNMi forwards ArcSight Syslog messages to the northbound application using the NorthBound Integration module. NNMi begins forwarding incidents as soon as you enable the destination. For more information, see the *NNMi Northbound Interface* chapter of the NNMi Deployment Reference.
Lifecycle State Changes	The incident change notification specification. - **Enhanced Closed** NNMi sends an incident closed trap to the HPE Operations agent 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 HPE Operations agent for each incident that changes to the IN PROGRESS, COMPLETED, or CLOSED lifecycle state. - **Both** NNMi sends an incident closed trap to the HPE Operations agent for each incident that changes to the CLOSED lifecycle state. Additionally, the integration sends an incident lifecycle state changed trap to the HPE Operations agent for each incident that changes to the IN PROGESS, COMPLETED, or CLOSED lifecycle state. **NOTE:** In this case, each time an incident changes to the CLOSED lifecycle state, the integration sends two notification traps: an incident closed trap and an incident lifecycle state changed trap.

Table 2 HPOM Integration Content Configuration Information, continued

Field	Description
	For more information, see *Incident Lifecycle State Change Notifications* in the NNMi Deployment Reference.
Correlations	The incident correlation notification specification. • **None** NNMi does not notify the HPE Operations agent 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. For more information, see *Incident Lifecycle State Change Notifications* in the NNMi Deployment Reference.
Deletions	The incident deletion specification. • **Don’t Send** NNMi does not notify the HPE Operations agent when incidents are deleted in NNMi. This is the default configuration. • **Send** NNMi sends a deletion trap to the HPE Operations agent for each incident that is deleted in NNMi. For more information, see *Incident Deletion Notifications* in the NNMi Deployment Reference.
NNMi Console Access	The connection protocol specification in the URL for browsing to the NNMi console from the HPOM message browser. The traps that NNMi sends to the HPE Operations agent include the NNMi URL in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). The integration requires an HTTP connection to the NNMi console. Select the **HTTP** option.

Table 2 HPOM Integration Content Configuration Information, continued

Field	Description
Incident Filters	A list of object identifiers (OIDs) the integration uses to filter the events sent to the HPE Operations agent. Each filter entry can be a valid numeric OID (for example, .1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9) or OID prefix (for example, .1.3.6.1.6.3.1.1.5.*). Select one of the following options: • **None** NNMi sends all events to the HPE Operations agent. 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. Specify the incident filter: • To add a filter entry, enter the text in the lower text box, and then click **Add**. • To delete a filter entry, select that entry from the list in the upper box, and then click **Remove**. For more information, see *Event Forwarding Filter* in the NNMi Deployment Reference.

HPE Operations Agent Destination Status Information

"Table 3 HPE Operations Agent Destination Status Information" below lists the read-only status information for the HPE Operations agent. This information is useful for verifying that the integration is working correctly.

Table 3 HPE Operations Agent Destination Status Information

Field	Description
Trap Destination IP Address	The HPE Operations agent destination host name resolves to this IP address. This value is unique to this HPE Operations agent destination.

Table 3 HPE Operations Agent Destination Status Information, continued

Field	Description
Uptime (seconds)	The time (in seconds) since the northbound component was last started. The traps that NNMi sends to the HPE Operations agent 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 HPE Operations agent 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.

HPE NNMi–HPOM Integration (Web Services Implementation)

The agent implementation of the HPE NNMi—HPOM integration is the preferred solution for integrating HPOM with NNMi.

If the agent and the web services implementations of the HPE NNMi—HPOM integration both forward messages to the same HPOM management server, you might not see all messages from both implementations in the HPOM active messages browser. For this reason, HPE does not support running both implementations of the HPE NNMi—HPOM integration from one NNMi management server to the same HPOM management server concurrently.

This section contains the following topics:

- "About the HPE NNMi—HPOM Integration (Web Services Implementation)" below
- "Enabling the HPE NNMi—HPOM Integration (Web Services Implementation)" on page 35
- "Using the HPE NNMi—HPOM Integration (Web Services Implementation)" on page 40
- "Changing the HPE NNMi—HPOM Integration Configuration (Web Services Implementation)" on page 42
- "Disabling the HPE NNMi—HPOM Integration (Web Services Implementation)" on page 42
- "Troubleshooting the HPE NNMi—HPOM Integration (Web Services Implementation)" on page 43
- "HPE NNMi—HPOM Web Services Integration Configuration Form Reference" on page 48

About the HPE NNMi–HPOM Integration (Web Services Implementation)

The web services implementation of the HPE NNMi—HPOM integration forwards NNMi incidents to the HPOM active messages browser. The integration synchronizes incidents between NNMi and HPOM. It also provides for accessing the NNMi console from within HPOM.

The HPE NNMi—HPOM integration supports a “many-to-many” arrangement. Each NNMi management server can forward incidents to multiple HPOM management servers. Likewise, each HPOM management server can receive incidents from multiple

NNMi management servers. The integration interprets the unique identifier of an incident to determine the source NNMi management server.

The HPE NNMi—HPOM integration consists of the following components:

- **HPE NNMi—HPOM Integration Module**

  The HPE NNMi—HPOM integration module forwards incidents from NNMi to HPOM. It is installed and configured on the NNMi management server.
- **HPE Operations Manager Incident Web Service**

  HPOM uses the HPE Operations Manager Incident Web Service (IWS) to receive the incidents that are forwarded from NNMi.
- **HPOM applications for contextual access of the NNMi console**

  HPOM provides applications for accessing forms, views, and tools in the NNMi console. For example, you can open an NNMi incident directly from the HPOM active messages browser. The specific application determines the context the NNMi console opens to. You need to configure the applications before you can use them.

Value

The HPE NNMi—HPOM integration provides event consolidation in the HPOM active messages browser for the network management, system management, and application management domains, so that HPOM users can detect and investigate potential network problems.

The primary features of the integration are as follows:

- Automatic incident forwarding from NNMi to HPOM.
  - Forwarded incidents appear in the HPOM active messages browser.
  - You can create filters that limit the incidents NNMi forwards.
- Synchronization of Incident updates between NNMi and HPOM as described in the following table.

Trigger	Result
In HPOM, the message is acknowledged.	In NNMi, the corresponding incident’s lifecycle state is set to Closed.
In HPOM, the message is unacknowledged.	In NNMi, the corresponding incident’s lifecycle state is set to Registered.
In NNMi, the incident’s lifecycle state is set to Closed.	In HPOM, the corresponding message is acknowledged.

Trigger	Result
In NNMi, the incident's lifecycle state is changed from Closed to any other state.	In HPOM, the corresponding message is unacknowledged.

- Access to the NNMi console from HPOM.
  - HPOM users can open the NNMi **Incident** form in the context of a selected message.
  - HPOM users can launch an NNMi view (for example, the Layer 2 Neighbor view) in the context of a selected message and node.
  - HPOM users can launch an NNMi tool (for example, status poll) in the context of a selected message and node.
  - When HPOM is consolidating NNMi incidents from multiple NNMi management servers, the integration interprets the unique identifier of each incident to access the correct NNMi management server.

Integrated Products

The information in this section applies to the following products:

- HPOM for Windows
- HPOM for Linux

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

- NNMi 10.20

NNMi and HPOM must be installed on separate computers. The NNMi management server and the HPOM management 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 both products.

Documentation

This chapter describes how to configure NNMi to communicate with HPOM.

The HPOM documentation describes how to configure HPOM to communicate with NNMi. It also describes how to use the HPE NNMi—HPOM integration.

- For HPOM for Windows, see the information for the NNMi Adapter in the HPOM help.
- HPOM for Linux version 9.xx, see the *Integrating NNMi into HPOM* section in the *HPE Operations Manager for UNIX and Linux Administrator's Reference*.

Enabling the HPE NNMi–HPOM Integration (Web Services Implementation)

This section describes the procedure for enabling the HPE NNMi—HPOM integration. For each NNMi management server and each HPOM management server that you want to include in the integration, complete the appropriate steps in the procedure for the version of HPOM that you are using.

HPOM for Windows

1. On the NNMi management server, configure NNMi incident forwarding to HPOM:
   a. In the NNMi console, open the **HPE NNMi—HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
   b. Click **web services implementation**.
   c. On the **HPE NNMi—HPOM Web Services Integration Configuration** form, select the **Enable Integration** check box to make the remaining fields on the form available.
   d. Enter the information for connecting to the NNMi management server.

      > **NOTE:** The integration requires an HTTP connection to the NNMi console. Leave the **NNMi SSL Enabled** check box cleared.

      For information about these fields, see "NNMi Management Server Connection" on page 48.
   e. Enter the information for connecting to the HPOM management server.

      For information about these fields, see "HPOM Management Server Connection" on page 49.
   f. Enter values for the following fields:
      - **Forward Only**
      - **Holding period (minutes)**
      - **Incident Filter**

      For information about these fields, see "Integration Behavior" on page 51.
   g. If you want NNMi to forward incidents to multiple HPOM management servers, click **Add another HPOM server**, and then enter the information for the next HPOM management server in the HPOM fields.

      The information for the first server appears in the **Additional HPOM Servers** list.
   h. Click **Submit** at the bottom of the form.

      A new window opens, showing a status message. If the message indicates a problem with connecting to the HPOM management server, re-open the **HPE**

NNMi—HPOM Web Services Integration Configuration form (or press **ALT+LEFT ARROW** in the message window), and then adjust the values for connecting to the HPOM management server as suggested by the text of the error message.

2. In HPOM, configure the NNMi adapter for connecting to the NNMi management server as described in *Configure the NNMi Management Server Name and Port* of the HPOM help.
3. In HPOM, add a managed node for each NNMi node that will be named as a source node in the NNMi incidents that are forwarded to this HPOM management server. Also add a managed node for each NNMi management server that will forward incidents to this HPOM management server.

   Alternatively, you can create one external node to catch all forwarded NNMi incidents. For initial testing, set the node filter to `<*>.<*>.<*>.<*>` (for an IP filter) or `<*>` (for a name filter). After you validate the integration, restrict the external node filter to match your network.

   For more information, see *Configuring NNMi Management Server Nodes* in the HPOM help.

   > **CAUTION:** If you do not set up an HPOM managed node for an NNMi incident source node, the HPOM management server discards all incidents regarding that node.

4. *Optional*. In HPOM, add the custom message attributes for NNMi incidents to the active messages browser:
   a. In the browser, right-click any column heading, and then click **Options**.
   b. In the **Enter Custom Message Attributes** list, select an attribute, and then click **Add**.
      - The custom message attributes for NNMi incidents begin with the text `nnm`.
      - For the web services implementation of the HPE NNMi—HPOM integration, the most interesting attributes for NNMi incidents are as follows:

        ```
        nnm.assignedTo
        nnm.category
        nnm.emittingNode.name
        nnm.source.name
        ```
      - To change the order the custom message attributes appear in the messages browser, drag a column heading to the new location.
5. *Optional*. In HPOM, enable contextual launching of the NNMi views by associating the NNMi source nodes with the NNMi Web Tools group.

   For more information, see *Enable tools in the By Node tool group* in the HPOM help.

HPOM for Linux

1. On the NNMi management server, configure NNMi incident forwarding to HPOM:
   a. In the NNMi console, open the **HPE NNMi—HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
   b. Click **web services implementation**.
   c. On the **HPE NNMi—HPOM Web Services Integration Configuration** form, select the **Enable Integration** check box to make the remaining fields on the form available.
   d. Enter the information for connecting to the NNMi management server.

      > **NOTE:** The integration requires an HTTP connection to the NNMi console. Leave the **NNMi SSL Enabled** check box cleared.

      For information about these fields, see "NNMi Management Server Connection" on page 48.
   e. Enter the information for connecting to the HPOM management server.

      For information about these fields, see "HPOM Management Server Connection" on page 49.
   f. Enter values for the following fields:
      - **Forward Only**
      - **Holding period (minutes)**
      - **Incident Filter**

      For information about these fields, see "Integration Behavior" on page 51.
   g. If you want NNMi to forward incidents to multiple HPOM management servers, click **Add another HPOM server**, and then enter the information for the next HPOM management server in the HPOM fields.

      The information for the first server appears in the **Additional HPOM Servers** list.
   h. Click **Submit** at the bottom of the form.

      A new window opens, showing a status message. If the message indicates a problem with connecting to the HPOM server, re-open the **HPE NNMi—HPOM Web Services Integration Configuration** form (or press **ALT+LEFT ARROW** in the message window), and then adjust the values for connecting to the HPOM management server as suggested by the text of the error message.
   i. Click **Submit** at the bottom of the form.
2. In HPOM, add a managed node for each NNMi node that will be named as a source node in the NNMi incidents that are forwarded to this HPOM management server. Also add a managed node for each NNMi management server that will forward

incidents to this HPOM management server.

Alternatively, you can create one external node to catch all forwarded NNMi incidents. For initial testing, set the node filter to `<*>.<*>.<*>.<*>` (for an IP filter) or `<*>` (for a name filter). After you validate the integration, restrict the external node filter to match your network.

For more information, see the *HPE Operations Manager for UNIX and Linux Administrator's Reference*.

> **CAUTION:** If you do not set up an HPOM managed node for an NNMi incident source node, the HPOM management server discards all incidents regarding that node.

3. *Optional*. In HPOM, add the custom message attributes for NNMi incidents to the active messages browser:
   a. In the Java Interface Message Browser, right-click any column heading, and then click **Customize Message Browser Columns**.
   b. On the **Custom** tab, select from the **Available Custom Message Attributes**, and then click **OK**.
      - The custom message attributes for NNMi incidents begin with the text `nnm`.
      - For the web services implementation of the HPE NNMi—HPOM integration, the most interesting attributes for NNMi incidents are as follows:

        ```
        nnm.assignedTo
        nnm.category
        nnm.emittingNode.name
        nnm.source.name
        ```
      - To change the order the custom message attributes appear in the messages browser, drag a column heading to the new location.
4. *Optional*. On the HPOM management server, prepare the HPOM applications for accessing the NNMi console.
   a. *Required*. Install the basic set of NNMi applications.

      > **TIP:** HPOM version 9.00 or higher automatically installs the basic NNMi applications.

   b. *Optional*. Install additional NNMi applications.

   For information, see the section on installing and configuring the HPE NNMi—HPOM integration in the *HPE Operations Manager for UNIX and Linux Administrator's Reference* (version 9.xx).

Configuring an HTTPS Connection

To configure an SSL connection to HPOM, follow the steps documented in this topic.

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

1. Log on to the HPOM management server, and then generate one of the following certificates:
   - A self-signed HPOM certificate

     > **Note:** For an NNMi management server with the PKCS #12 format-based certificate scheme, you must use a 2048-bit self-signed HPOM certificate.

     To generate a self-signed HPOM certificate:

     i. Log on to the HPOM management server as root or administrator.

     ii. Stop the HPOM processes by running the following command:
       - *On Windows:* **%ovinstalldir%\bin\ovc -stop**
       - *On UNIX/Linux:* **/opt/OV/bin/ovc -stop**

     iii. Delete the existing `tomcat.certificate` file from the following directory:
       - *On Windows:* `%ovdatadir%\certificates\tomcat\b`
       - *On UNIX/Linux:* `/var/opt/OV/certificates/tomcat/b`

     iv. Regenerate the `tomcat.certificate` file by running the following command:

       > **Note:** Omit **-keysize "2048"** from the command if NNMi uses the JKS format-based certificate scheme.

       - *On Windows:* **%ovinstalldir%\nonOV\jre\b\bin\keytool -genkey -alias ovtomcatb -keyalg "RSA" -keysize "2048" -validity "7200" -dname "***<distinguished_name>***" -keypass changeit -storepass changeit -keystore %ovdatadir%\certificates\tomcat\b\tomcat.keystore**
       - *On UNIX/Linux:* **/opt/OV/nonOV/jre/b/bin/keytool -genkey -alias ovtomcatb -keyalg "RSA" -keysize "2048" -validity "7200" -dname "***<distinguished_name>***" -keypass changeit -storepass changeit -keystore /var/opt/OV/certificates/tomcat/b/tomcat.keystore**

       In this instance, *<distinguished_name>* is the distinguished name of the HPOM management server.

     v. Generate a new certificate by running the following command:
       - *On Windows:* **%ovinstalldir%\nonOV\jre\b\bin\keytool -exportcert -alias ovtomcatb -keystore %ovdatadir%\certificates\tomcat\b\tomcat.keystore -storepass changeit -file** *<hostname>***.cer**

- *On UNIX/Linux:* **/opt/OV/nonOV/jre/b/bin/keytool -exportcert -alias ovtomcatb -keystore /var/opt/OV/certificates/tomcat/b/tomcat.keystore -storepass changeit -file** <*hostname*>**.cer**

  In this instance, <*hostname*>is the host name of the HPOM management server.

vi. Start the HPOM processes by running the following command:

- *On Windows:* **%ovinstalldir%\bin\ovc -start**
- *On UNIX/Linux:* **/opt/OV/bin/ovc -start**

- A CA-signed certificate

2. Transfer the certificate to the NNMi management server.
3. Import the certificate to the NNMi truststore by running the following command:
   - On a system with the PKCS #12 format-based certificate scheme:
     - *On Windows:* **%nnminstalldir%\bin\nnmkeytool.ovpl -import -truststore %NnmDataDir%\shared\nnm\certificates\nnm-trust.p12 -storetype PKCS12 -alias** <*alias*> **-storepass ovpass -file** <*filename*>
     - *On Linux:* **/opt/OV/bin/nnmkeytool.ovpl -import -truststore /var/opt/OV/shared/nnm/certificates/nnm-trust.p12 -storetype PKCS12 -alias** <*alias*> **storepass ovpass -file** <*filename*>
   - On a system with the JKS format-based certificate scheme:
     - *On Windows:* **%nnminstalldir%\nonOV\jdk\hpsw\bin\keytool -import -truststore %NnmDataDir%\shared\nnm\certificates\nnm.truststore -storetype JKS -alias** <*alias*> **-storepass ovpass -file** <*filename*>
     - *On Linux:* **/opt/OV/nonOV/jdk/hpsw/bin/keytool -import -truststore /var/opt/OVshared/nnm/certificates/nnm.truststore -storetype JKS -alias** <*alias*> **-storepass ovpass -file** <*filename*>

   In this instance, <*filename*> is the full path (including the file name) to the newly created HPOM certificate; <*alias*> is the alias of the HPOM certificate.

   See the *Managing Certificates* section in the *NNMi Deployment Reference* for more information about PKCS #12 and JKS certificates.

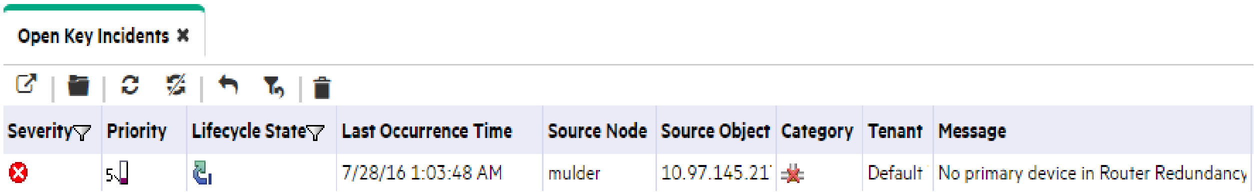
Using the HPE NNMi–HPOM Integration (Web Services Implementation)

Usage Example

"Figure 2 Interface Down Incident in NNMi Console" on the next page shows an interface down incident in the NNMi console. The information in the **Source Object** and

Message columns together describe the situation.

Figure 2 Interface Down Incident in NNMi Console

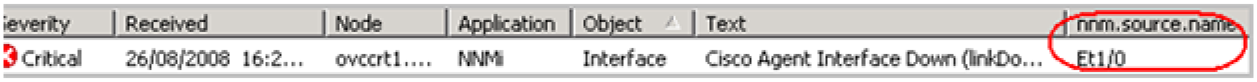


Severity	Priority	Lifecycle State	Last Occurrence Time	Source Node	Source Object	Category	Tenant	Message
⊗	5		7/28/16 1:03:48 AM	mulder	10.97.145.21		Default	No primary device in Router Redundancy

"Figure 3 Forwarded Incident in HPOM for Windows" below shows the NNMi incident as received by HPOM for Windows. "Figure 4 Forwarded Incident in HPOM for Linux" below shows the NNMi incident as received by HPOM for Linux. The **nnm.source.name** and **Text** columns are equivalent to the **Source Object** and **Message** columns in the NNMi console.

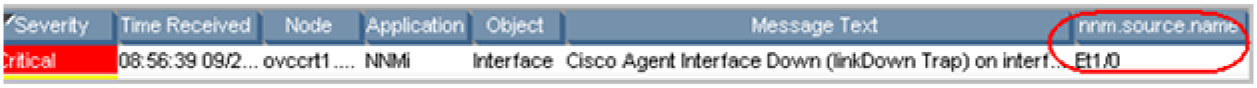
> **NOTE:** You must enable the display of the **nnm.source.name** custom message attribute column as described in "HPOM for Windows" on page 35 (for HPOM for Windows) and in "HPOM for Linux" on page 37 (for HPOM for Linux).

Figure 3 Forwarded Incident in HPOM for Windows



everity	Received	Node	Application	Object	Text	nnm.source.name
Critical	26/08/2008 16:2...	ovccrt1....	NNMi	Interface	Cisco Agent Interface Down (linkDo...	Et1/0

Figure 4 Forwarded Incident in HPOM for Linux



Severity	Time Received	Node	Application	Object	Message Text	nnm.source.name
ritical	08:56:39 09/2...	ovccrt1....	NNMi	Interface	Cisco Agent Interface Down (linkDown Trap) on interf...	Et1/0

A Normal Situation: Unknown MSI Condition

The HPOM server receives forwarded NNMi incidents through MSI (not a regular trap policy). In the HPOM message browser, the format of the message source is **MSI** followed by the name of the MSI interface. The condition name corresponds to the `condition_id` field in the message, which is unset because there is no associated policy.

- *HPOM for Windows*: The policy type is empty.
- *HPOM for Linux*: The message source is of the format: **MSI: <*MSI_Interface*>: Unknown Condition**.

More Information

For detailed information about using the HPE NNMi—HPOM integration, see the HPOM documentation.

- *HPOM for Windows*: See the topics about the NNMi adapter in the HPOM help.
- *HPOM for Linux*: See the section on installing and configuring the HPE NNMi—HPOM integration in the *HPE Operations Manager for UNIX and Linux Administrator's Reference* (version 9.xx).

> **NOTE:** In the HPOM messages browser, the details for a forwarded NNMi incident are available as custom message attributes.

Changing the HPE NNMi–HPOM Integration Configuration (Web Services Implementation)

1. In the NNMi console, open the **HPE NNMi—HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **web services implementation**.
3. Modify the values as appropriate.
   - If you know the syntax of the entries in the Incident Filter and Additional HPOM Servers lists, you can modify the entries directly.
   - If you do not know the syntax for a list item, delete that entry and then re-enter it.

   For information about the fields on this form, see "HPE NNMi—HPOM Web Services Integration Configuration Form Reference" on page 48.
4. Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Disabling the HPE NNMi–HPOM Integration (Web Services Implementation)

For All HPOM Management Servers

To discontinue the forwarding of NNMi incidents to all HPOM management servers, follow these steps:

1. In the NNMi console, open the **HPE NNMi—HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **web services implementation**.

3. 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.

If necessary, repeat this process for all NNMi management servers.

For One HPOM Management Server

To discontinue the forwarding of NNMi incidents to only one of the HPOM management servers, follow these steps:

1. In the NNMi console, open the **HPE NNMi—HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **web services implementation**.
3. In the **Additional HPOM Servers** list, edit the text to delete the entry (or entries) for the HPOM management server to disconnect from the integration.

   CAUTION: Clicking **Clear** removes all HPOM servers from the list.

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

   The changes take effect immediately.

Troubleshooting the HPE NNMi–HPOM Integration (Web Services Implementation)

HPOM Integration (Web Service Implementation) Fails

If HPOM and NNMi are configured to use the HTTPS protocol and if the HPOM-NNMi integration fails, follow these steps:

1. Log on to the NNMi management server as root or administrator.
2. Stop NNMi by running the following command:
   - *On Windows:* **%nnminstalldir%\bin\ovstop -c**
   - *On Linux:* **/opt/OV/bin/ovstop -c**
3. Take a backup of the following file:
   - *On Windows:* `%nnmdatadir%\conf\nnm\java.security`
   - *On Linux:* `/var/opt/OV/conf/nnm/java.security`
4. Replace the above file with a copy of the following file:

- *On Windows:* `%nnminstalldir%\newconfig\HPNmsServStgs\Windows\java.security`
- *On Linux:* `/opt/OV/newconfig/HPNmsServStgs/Windows/java.security`

5. Start NNMi by running the following command:
   - *On Windows:* **%nnminstalldir%\bin\ovstart -c**
   - *On Linux:* **/opt/OV/bin/ovstart -c**

HPOM Does Not Receive Any Forwarded Incidents

NOTE: If the integration has worked successfully in the past, it is possible that some aspect of the configuration, for example, the NNMi or HPOM user password, has changed recently. You might want to update the integration configuration as described in "Changing the HPE NNMi—HPOM Integration Configuration (Web Services Implementation)" on page 42, before walking through this entire procedure.

1. In the NNMi console, open the **HPE NNMi—HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **web services implementation**.

   For information about the fields on this form, see "HPE NNMi—HPOM Web Services Integration Configuration Form Reference" on page 48.
3. Check the status of the integration, in the **HPE NNMi—HPOM Web Services Integration Configuration** form, by clicking **Submit** at the bottom of the form (without making any configuration changes).

   A new window opens, showing a status message.
   - If the message indicates success, the problem is most likely that HPOM is not configured to accept incidents from the devices that NNMi manages. HPOM ignores any forwarded incident from an NNMi source node that is not configured as a managed node in HPOM, and then test the integration as described in this procedure.
   - If the message indicates a problem with connecting to the HPOM server, NNMi and HPOM are not able to communicate. Continue with the next step of this procedure.
4. Verify the accuracy and access level of the HPOM credentials by logging in to the HPOM console and opening the HPOM active messages browser:
   - *HPOM for Windows*: Log on to the computer as the **HPOM User** from the **NNMi–HPOM Web Services Integration Configuration** form, and then start the HPOM console.

The user name is in the format *<Windows_domain>**<username>*.

- *HPOM for Linux*: Log on to the HPOM console with the credentials for the **HPOM User** from the **NNMi–HPOM Web Services Integration Configuration** form.

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

5. Verify that the connection to the HPOM management server is configured correctly:
   a. In a web browser, enter the following URL:

      ***<protocol>*://*<omserver>*:*<port>*/opr-webservice//Incident.svc?wsdl**

      Where the variables are related to values on the **HPE NNMi—HPOM Web Services Integration Configuration** form as follows:
      - If the **HPOM SSL Enabled** check box is selected, *<protocol>* is `https`.
      - If the **HPOM SSL Enabled** check box is cleared, *<protocol>* is `http`.
      - *<omserver>* is the value of **HPOM Host**.
      - *<port>* is the value of **HPOM Port**.

   b. When prompted, enter the credentials for the **HPOM User** from the **HPE NNMi—HPOM Web Services Integration Configuration** form.

      The resulting web page is an XML file that describes the IWS.
      - If the XML file appears, the connection to the HPOM management server is configured correctly. Continue with "Verify that the connection to NNMi is configured correctly:" below.
      - If you see an error message, the connection to the HPOM management server is not configured correctly. Contact the HPOM administrator to verify the information you are using to connect to the HPOM web service. Continue to troubleshoot the connection to HPOM until you see the XML file.

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

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

   a. In a web browser, enter the following URL:

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

      Where the variables are related to values on the **HPE NNMi—HPOM Web Services Integration Configuration** form as follows:
      - If the **NNMi SSL Enabled** check box is selected, *<protocol>* is `https`.

        > **Tip:** If the **NNMi SSL Enabled** check box is selected, verify that the KeyManager process is running by entering the following command:

```
ovstatus -v ovjboss
```

- If the **NNMi SSL Enabled** check box is cleared, *<protocol>* is `http`.
- *<NNMiserver>* is the value of **NNMi Host**.

  > **TIP:** Use the fully-qualified domain name or the IP address of the NNMi management server. Do not use `localhost`.

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

  > **TIP:** To verify the NNMi ports for HTTP or HTTPS, check the `nms-local.properties` file, as described in "HPOM Does Not Receive Any Forwarded Incidents" on page 44.

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

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

   > **NOTE:** You cannot log on to the NNMi console as a user with the Web Service Client role.

c. Verify the values of the **NNMi User** and **NNMi Password**.

   - If the **NNMi User** listed on the **HPE NNMi—HPOM Web Services Integration Configuration** form has the Administrator role and you were able to connect to the NNMi console with this user name, then re-enter the corresponding password on the **HPE NNMi—HPOM Web Services Integration Configuration** form.
   - If the **NNMi User** listed on the **HPE NNMi—HPOM Web Services Integration Configuration** form has the Web Service Client role, contact the NNMi administrator to verify the values of **NNMi User** and **NNMi Password**.

   Passwords are hidden in the NNMi console. If you are not sure what password to specify for an NNMi user name, ask the NNMi administrator to reset the password.

7. Update the **HPE NNMi—HPOM Web Services Integration Configuration** form with the values that you used for successful connections in the last two steps of this procedure.

   For more information, see "HPE NNMi—HPOM Web Services Integration Configuration Form Reference" on page 48.

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

9. If the status message still indicates a problem with connecting to the HPOM server, do the following:
   a. Clear the web browser cache.
   b. Clear all saved form or password data from the web browser.
   c. Close the web browser window completely, and then re-open it.
   d. Repeat the last two steps of this procedure.
10. Test the configuration by generating an incident on the NNMi management server and determining whether it reaches the HPOM management server.

    Alternatively, change the lifecycle state of an NNMi management event to OPEN. (If the lifecycle state is currently OPEN, change the lifecycle state to CLOSED and then back to OPEN.)

HPOM Does Not Receive Some Forwarded Incidents

Verify the HPOM nodes and the incident filter.

The HPOM management server must be configured to accept incidents from the devices that NNMi manages. HPOM ignores any forwarded incident from an NNMi source node that is not configured as a managed node in HPOM.

If the NNMi source node is configured as a managed node in HPOM, verify the incident filter configuration on the **HPE NNMi—HPOM Web Services Integration Configuration** form. Then test the filter by generating an incident on the NNMi management server and determine whether it reaches the HPOM management server.

NNMi Incident Information Is Not Available in the HPOM Messages Browser

The important information from NNMi incidents is passed to HPOM as custom message attributes. Add one or more custom messages attributes for NNMi incidents as described in HPOM for Windows and in HPOM for Linux.

NNMi and HPOM Are Not Synchronized

If either of the management servers becomes unreachable, the incidents in the NNMi incident views and the HPOM active messages browser might become mismatched. The HPE NNMi—HPOM integration can re-synchronize the incidents as described here.

- If an HPOM management server becomes unavailable to the HPE NNMi—HPOM integration module, the integration module periodically checks for the availability of that HPOM management server and resumes incident forwarding when a connection can be re-established. When the connection to the HPOM management server is available, the integration module forwards any incidents that might have been missed while the HPOM management server was down.

- If the NNMi management server is unavailable when an HPOM user acknowledges or unacknowledges a forwarded incident, NNMi does not receive the change of state. NNMi and HPOM might show different states for this incident.

The Integration Does Not Work Through a Firewall

Ensure that the NNMi management server can directly address the HPOM IWS by host and port.

HPE NNMi–HPOM Web Services Integration Configuration Form Reference

The **HPE NNMi—HPOM Web Services Integration Configuration** form contains the parameters for configuring communications between NNMi and HPOM. This form is available from the **Integration Module Configuration** workspace. (On the **HPE NNMi—HPOM Integration Selection** form, click **web services implementation**.)

> **NOTE:** Only NNMi users with the Administrator role can access the **HPE NNMi—HPOM Web Services Integration Configuration** form.

The **HPE NNMi—HPOM Web Services Integration Configuration** form collects information for the following general areas:

- "NNMi Management Server Connection" below
- "HPOM Management Server Connection" on the next page
- "Integration Behavior" on page 51
- "Incident Filters" on page 52

To apply changes to the integration configuration, update the values on the **HPE NNMi—HPOM Web Services Integration Configuration** form, and then click **Submit**.

NNMi Management Server Connection

"Table 4 NNMi Management Server Connection Information" on the next page 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 4   NNMi Management Server Connection Information

Field	Description
NNMi SSL Enabled	The connection protocol specification for connecting to the NNMi console. The integration requires an HTTP connection to the NNMi console. Leave the **NNMi SSL Enabled** check box cleared.
NNMi Host	The fully-qualified domain name of the NNMi management server. This field is pre-filled with the hostname that was used to access the NNMi console. Verify that this value is the name returned by the **`nnmofficialfqdn.ovpl -t`** command run on the NNMi management server.
NNMi Port	The port for connecting to the NNMi console. This field is pre-filled with the port that the jboss application server uses for communicating with 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` Use the value of `nmsas.server.port.web.http`, which is `80` or `8004` by default (depending on the presence of another web server when NNMi was installed).
NNMi User	The user name for connecting to the NNMi web services. This user must have the NNMi Administrator or Web Service Client role. **NOTE:** The password for this user name is passed in clear text. Best practice: Create and use an `NNMiIntegration` user account with the Web Service Client role.
NNMi Password	The password for the specified NNMi user.

HPOM Management Server Connection

"Table 5   HPOM Management Server Connection Information" on the next page lists the parameters for connecting to the web service on the HPOM management server.

Coordinate with the HPOM administrator to determine the appropriate values for this section of the configuration.

Table 5 HPOM Management Server Connection Information

HPOM Server Parameter	Description
HPOM SSL Enabled	The connection protocol specification. • If HPOM is configured to use HTTPS, select the **HPOM SSL Enabled** check box. This is the default configuration. • If HPOM is configured to use HTTP, clear the **HPOM SSL Enabled** check box.
HPOM Host	The fully-qualified domain name of the HPOM management server. Verify that this name is resolvable from the NNMi management server by using the `nslookup` or `ping` command. If DNS is questionable, use the IP address of the HPOM management server. If possible, use the `traceroute` command to verify the network path from the NNMi management server to the HPOM management server.
HPOM Port	The port for connecting to the HPOM web service. To determine the port number to specify, do the following on the HPOM management server: • *HPOM for Windows*: Examine the port settings in the IIS Manager, which is available from the **Start** menu, for example, **Start > Administrative Tools > Internet Information Services (IIS) Manager**. • HPOM for *Linux*: Run the following command: **`ovtomcatbctl -getconf`** This field is pre-filled with the value `443`, which is the default port for SSL connections to HPOM for Windows. For SSL connections to HPOM for Linux, the default port is 8443 or 8444.
HPOM User	A valid HPOM user account name with the HPOM Administrator role. This user must be permitted to view the HPOM active messages browser and the HPOM incident

Table 5 HPOM Management Server Connection Information, continued

HPOM Server Parameter	Description
	web service WSDL. *Windows only*: On the Windows operating system, HPOM works through Microsoft Internet Information Services (IIS) to authenticate user credentials. Specify a Windows user in the format `<Windows_domain>\<username>`. Best Practice: • *HPOM for Windows*: Specify a user who is a member of the `HP-OVE-ADMINS` user group. (Verify group membership in the Local Users and Groups area of the Microsoft Management Console, which is available from **Control Panel > Administrative Tools > Computer Management**.) • *HPOM for Linux*: Use the `opc_adm` user account.
HPOM Password	The password for the specified HPOM user.

Integration Behavior

"Table 6 Integration Behavior Information" below lists the parameters that describe the integration behavior. Coordinate with the NNMi administrator to determine the appropriate values for this section of the configuration.

Table 6 Integration Behavior Information

Field	Description
Forward Only	The behavior specification for the HPE NNMi—HPOM integration module. By default, the integration module forwards incidents to and receives incident acknowledgements from the HPOM management servers identified on the **HPE NNMi—HPOM Web Services Integration Configuration** form. You can disable the receipt of incident acknowledgements. • For one-way communication (forward incidents to HPOM but ignore incident acknowledgements from HPOM), select the **Forward Only** check box. • For two-way communication, leave the **Forward Only** check box cleared. This is the default behavior.

Table 6 Integration Behavior Information, continued

Field	Description
Holding period (minutes)	The number of minutes to wait before forwarding the configured incidents to HPOM. If an incident is closed during this time (for example, an SNMPLinkUp incident cancels an SNMPLinkDown incident), HPOM never receives that incident. If you want NNMi to forward incidents immediately, enter the value `0`. The default value is 5 minutes.
Incident Filter	A filter based on NNMi incident attributes that limits incident forwarding. The default filter (`nature=ROOTCAUSE origin=MANAGEMENTSOFTWARE`) specifies all root cause incidents that are generated by NNMi. You can modify this filter to change the incidents forwarded to HPOM. **NOTE:** All text (attribute names and values) in the **Incident Filter** field is case-sensitive. For more information, see "Incident Filters" below.

Incident Filters

The incident filter is the combination of all entries in the **Incident Filter** list. Filter entries with the same attribute value expand the filter (logical OR). Filter entries with different attribute values restrict the filter (logical AND). All filter entries work together; you *cannot* create a filter of the format `(a AND b) OR c`. For example filter entries, see "Example Incident Filters" on page 54.

To create the incident filter, follow these steps:

1. In the NNMi console, open the **HPE NNMi—HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **web services implementation**.
3. To delete a filter entry, in the **Incident Filter** list, edit the text to delete the entry (or entries).

   CAUTION: Clicking **Clear** removes all filter entries from the list.

4. To add an incident filter entry:

   a. Select an attribute from the **name** list. For the supported attributes, see the table in "Enter a comparison value. The following table lists the supported attributes and the acceptable values for each attribute." on the next page.

b. Select the comparison operation to perform. Supported operators are:
   - =
   - !=
   - <
   - <=
   - >
   - >=

c. Enter a comparison value. The following table lists the supported attributes and the acceptable values for each attribute.

Attribute	Possible Values
name	Examine the incident configuration in the NNMi console to determine the available incident names.
nature	◦ ROOTCAUSE ◦ SECONDARYROOTCAUSE ◦ SYMPTOM ◦ SERVICEIMPACT ◦ STREAMCORRELATION ◦ INFO ◦ NONE
origin	◦ MANAGEMENTSOFTWARE ◦ MANUALLYCREATED ◦ SYMPTOM ◦ REMOTELYGENERATED ◦ SNMPTRAP ◦ SYSLOG ◦ OTHER
family	◦ com.hp.nms.incident.family.Address ◦ com.hp.nms.incident.family.Interface ◦ com.hp.nms.incident.family.Node ◦ com.hp.nms.incident.family.OSPF ◦ com.hp.nms.incident.family.HSRP ◦ com.hp.nms.incident.family.AggregatePort

Attribute	Possible Values
	◦ com.hp.nms.incident.family.Board ◦ com.hp.nms.incident.family.Connection ◦ com.hp.nms.incident.family.Correlation
category	◦ com.hp.nms.incident.category.Fault ◦ com.hp.nms.incident.category.Status ◦ com.hp.nms.incident.category.Config ◦ com.hp.nms.incident.category.Accounting ◦ com.hp.nms.incident.category.Performance ◦ com.hp.nms.incident.category.Security ◦ com.hp.nms.incident.category.Alert
severity	◦ NORMAL ◦ WARNING ◦ MINOR ◦ MAJOR ◦ CRITICAL

5. Repeat the previous step until all filter entries are defined.
6. Click **Submit** at the bottom of the form.

Example Incident Filters

Forward NodeDown Incidents from NNMi to HPOM

```
name=NodeDown
```

Forward NodeDown and InterfaceDown Incidents from NNMi to HPOM

```
name=NodeDown
name=InterfaceDown
```

Forward CiscoLinkDown Incidents from NNMi to HPOM

```
name=CiscoLinkDown
```

Forward NNMi Incidents with Severity of at least MINOR and nature of ROOTCAUSE or SERVICEIMPACT

```
severity=MINOR
severity=MAJOR
severity=CRITICAL
nature=ROOTCAUSE
nature=SERVICEIMPACT
```

Setting a Filter not to Filter Anything

HPE does not recommend configuring a blank filter to configure the integration for no filtering. Configuring a blank filter configures NNMi to send *ALL* events and traps using the web-service. Use the NNMi Northbound Interface to achieve that.

If you find you must configure NNMi to NOT filter any NNMi incidents, configure the filter as follows:

```
name!=nonsense
```

Incident Filter Limitations

Because all filter entries combine to create one incident filter for the NNMi management server, the following limitations apply:

- The HPE NNMi—HPOM integration processes the filtering of HPOM incident field values by treating the values as an alphabetic string. For example, you would normally expect a CRITICAL value to be greater than a MINOR value. However, as MINOR is greater than CRITICAL alphabetically, applying a filter such as `severity>=MINOR` results in only MINOR, NORMAL, and WARNING incidents being sent to the HPOMmessage browser. To forward incidents based on severity, you must explicitly include each severity to be forwarded using the `=` (equal) operator.
- The stated severity applies to all incidents. For example, to forward NodeDown incidents with a severity of MINOR or higher and InterfaceDown incidents with a severity of MAJOR, set the filter severity to `>=MINOR` and use HPOM logic to filter out the unwanted InterfaceDown messages.
- The incident filter does not provide a mechanism for limiting incident forwarding to specific source nodes. The HPOM managed node (or external node) configuration limits the forwarded incidents that HPOM accepts.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Network Node Manager i Software - HP Operations Manager Integration Guide (Network Node Manager i Software 10.20)

Just add your feedback to the email and click send.

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

We appreciate your feedback!

Glossary

A

AES

Advanced Encryption Standard

Anycast Rendezvous Point IP Address

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

Autonomous System

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

B

BGP

Border Gateway Protocol

C

Causal Engine

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

CBC

Cipher Block Chaining

CE

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

CRC

Cyclic Redundancy Check

Custom Node Collection

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

Custom Polled Instance

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

Custom User Groups

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

D

DES

Data Encryption Standard

E

EIGRP

Enhanced Interior Gateway Routing Protocol

EVPN

Ethernet Virtual Private Network.

G

global unicast address

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

H

HMAC

Hash-based Message Authentication Code

hops

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

HSRP

Hot Standby Router Protocol

hypervisor

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

I

IPv6 link-local address

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

ISIS

Intermediate System to Intermediate System Protocol

J

Jython

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

K

Key Incident

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

L

Layer 2

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

Layer 3

Refers to the Network layer of the multilayered communication model, Open Systems Interconnection (OSI). The Network layer is concerned with knowing the address of the neighboring nodes in the network, selecting routes and quality of service, and recognizing and forwarding incoming messages to local host domains. The router and switch-router are the devices that redirect data messages at the Layer 3 level. Everything in a subnet is connected at the Layer 3 (IP) level.

Link Aggregation

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

loopback address

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

M

MAC address

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

MAC addresses

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

MD5

Message-Digest algorithm 5

MIB file

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

MPLS

Multiprotocol Label Switching

multicast address

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

multiconnection

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

N

NAT

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

NIC

Network Interface Controller

NNMi Role

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

NNMi User Group

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

Node

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

O

OSPF

Open Shortest Path First Protocol

P

PE

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

private IP addresses

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

R

RAMS

HP Router Analytics Management System

routing prefixes

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

S

SHA

Secure Hash Algorithm

SNMP

Simple Network Management Protocol

SNMP Agent

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

SOAP

Simple Object Access Protocol

Split Link Aggregation

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

U

unique local address

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

Unmanaged

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

USM

User-based Security Model

UUID

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

V

virtual machine

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

VMware

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

VRRP

Virtual Router Redundancy Protocol

W

WAN Cloud

Layer 3 connectivity between your network and any MPLS networks.

Web Agent

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