

HP Network Node Manager and HP Performance Insight

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

Software Version: 5.41

Integration Guide

Document Release Date: November 2012
Software Release Date: November 2010



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2009-2012 Hewlett-Packard Development Company, L.P.

Trademark Notices

Windows® is US registered trademark of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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

Adobe® is a trademark of Adobe Systems Incorporated.

Acknowledgements

This product includes Xerces XML Java Parser software, which is Copyright (c) 1999 The Apache Software Foundation. All rights reserved.

This product includes JDOM XML Java Parser software, which is Copyright (C) 2000-2003 Jason Hunter & Brett McLaughlin. All rights reserved.

This product includes JClass software, which is (c) Copyright 1997, KL GROUP INC. ALL RIGHTS RESERVED.

This product includes J2TablePrinter software, which is © Copyright 2001, Wildcrest Associates (<http://www.wildcrest.com>)

This product includes Xalan XSLT Processor software, which is Copyright (c) 1999 The Apache Software Foundation. All rights reserved.

This product includes EXPAT XML C Processor software, which is Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper Copyright (c) 2001, 2002 Expat maintainers.

This product includes Apache SOAP software, which is Copyright (c) 1999 The Apache Software Foundation. All rights reserved.

This product includes O'Reilley Servlet Package software, which is Copyright (C) 2001-2002 by Jason Hunter, jhunter_AT_servlets.com. All rights reserved.

This product includes HTTPClient Package software, which is Copyright (C) 1991, 1999 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

This product includes Perl software, which is Copyright 1989-2002, Larry Wall. All rights reserved.

This product includes Skin Look And Feel software, which is Copyright (c) 2000-2002 L2FProd.com. All rights reserved.

This product includes nanoXML software, which is Copyright (C) 2000 Marc De Scheemaeker, All Rights Reserved.

This product includes Sixlegs PNG software, which is Copyright (C) 1998, 1999, 2001 Chris Nokleberg

This product includes cURL & libcURL software, which is Copyright (c) 1996 - 2006, Daniel Stenberg, <daniel@haxx.se>. All rights reserved.

This product includes Quartz - Enterprise Job Scheduler software, which is Copyright 2004-2005 OpenSymphony

This product includes Free DCE software, which is (c) Copyright 1994 OPEN SOFTWARE FOUNDATION, INC., (c) Copyright 1994 HEWLETT-PACKARD COMPANY, (c) Copyright 1994 DIGITAL EQUIPMENT CORPORATION, Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

This product includes DCE Threads software, which is Copyright (C) 1995, 1996 Michael T. Peterson

This product includes Jboss software, which is Copyright 2006 Red Hat, Inc. All rights reserved.

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

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

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

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

Or click the **New users - please register** link on the HP Passport login page.

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

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1	Introduction	9
	Overview	9
	Features and Benefits	9
	Configuration Points	10
	NNM Node Synchronization with HP Performance Insight	10
	NNM Interface Synchronization with HP Performance Insight	10
	NNM Trap Destination for HP Performance Insight Threshold Traps	10
	Launching HP Performance Insight Reports from NNM	11
	Sources of Additional Information	11
2	Installing the Integration Module	13
	Preinstallation Steps	13
	Installing the Integration Module on NNM	15
	Installing the Integration Module on NNM 7.5x	15
	Installing the Integration Module on NNMi 8.1x, 9.0x, or 9.10	15
	Installing Integration Components on PI	17
	Integrating Multiple NNM Servers with PI	21
	Automatic Scheduling of the NNM and PI Integration	21
	Post-Installation Steps	22
	Configuring an NNM Trap Destination for PI Threshold Traps	22
	Configure an NNM Trap Destination on UNIX	22
	Configure an NNM Trap Destination on Windows	23
	Configure Multiple NNM Trap Destinations	23
	Uninstalling the NNM and PI Integration Module	26
3	Verifying the Installation	27
	Verifying NNM Node Synchronization	27
	Verifying Report Launching	28

4	Launching Device-Specific Reports	29
	Launching Reports from NNM 7.x Server	29
	Launching Reports from the Native NNM Alarm Browser	29
	Launching Reports from NNM Dynamic Views	33
	Launching Reports from an NNM Map	34
	Launching Reports from NNMi 8.1x, 9.0x, or 9.10 Server	36
	Launching Reports from Inventory Workspace	36
	Launching Reports from Incidents Workspace	37
5	Troubleshooting	39
	Node Synchronization is not Working	39
	NNM devices are not being imported into PI from NNM through NNM Device Synchronization	39
	NNMi devices are not being imported into PI from NNMi through NNMi Device Synchronization	40
	Launched Reports Contain no Data	41
	NNM Device Sync Installation Fails	41
	NNM Device Sync Fails for Some of the NNM Node Sources	42
	Unable to Open NNM Event reports on Windows	42
	Additional Troubleshooting Resources	42
6	Reference	45
	The install.ovpl Script	45
	Index	47

1 Introduction

Overview

The NNM and PI Integration Module creates tight linkages between HP Network Node Manager (NNM) and HP Performance Insight (PI). By joining fault management with performance management, the Integration Module enhances problem diagnostic capabilities.

Features and Benefits

The following list outlines the features of the NNM and PI Integration Module and its benefits to you:

- It provides additional performance data from NNM, which contributes to faster and easier resolution of network-based service level problems.
- It shares and synchronizes detailed topology information between NNM and PI databases to better enable NNM and PI to monitor and manage your environment.
- It can forward PI threshold traps to a specified NNM management station (or set of NNM management stations).
- It enables you to launch PI reports directly from an NNM map or the NNM alarm browser. Reports display information pertinent to the node or alarm from which the action is invoked.
- It can integrate other NNM Smart Plug-in and HP Performance Insight products, such as the NNM Event Report Pack, to further enhance the management and monitoring of networks.

Configuration Points

NNM Node Synchronization with HP Performance Insight

The NNM node synchronization functionality resides on the PI core product. The initial node synchronization takes place after you run the NNM and PI integration wizard. For more information, see [Installing Integration Components on PI](#) on page 17.

If you want to synchronize the nodes at a later time, you can either run the NNM and PI integration wizard or automatically schedule the NNM and PI integration. For more information, see [Automatic Scheduling of the NNM and PI Integration](#) on page 21.

NNM Interface Synchronization with HP Performance Insight

The interface synchronization and NNM event reporting features are available with NNM Event Report Pack. For more information, see the NNM Event Report Pack documentation.

NNM Trap Destination for HP Performance Insight Threshold Traps

When PI report packs containing threshold packages are installed, such as MPLS VPN, PI can generate threshold traps specific to that package. The PI thresholds feature forwards PI-generated threshold traps to designated NNM management stations to display in the alarm browser. NNM places these threshold traps in the PI Threshold Alarms category of the NNM alarm browser.

During the installation of the Integration Module, a default trap destination is defined. You must modify this default configuration to point to the NNM management stations that will receive the threshold traps. For details, see [Configuring an NNM Trap Destination for PI Threshold Traps](#) on page 22.

Launching HP Performance Insight Reports from NNM

The NNM and PI Integration Module provides you with the capability to launch performance reports about nodes in NNM. Reports display information pertinent to the node or alarm from which the action is invoked.

You can launch PI performance reports from the following NNM user interfaces:

- From the NNM alarms browser. See [Launching Reports from the Native NNM Alarm Browser](#) on page 29.
- From Dynamic Views. See [Launching Reports from NNM Dynamic Views](#) on page 33.
- From NNM maps. See [Launching Reports from an NNM Map](#) on page 34.

Use the OVPI Report Launchpad window to view a list of reports based on the node information from a selected device or alarm. Then select and launch the desired report from the Report Launchpad window.

Sources of Additional Information

The following documents are sources for additional information:

- *NNM: Creating and Using Registration Files*
- *NNM: Managing Your Network*
- *PI: HP Performance Insight Administration Guide*
- *PI: HP Performance Insight Guide to Building and Viewing Reports*
- *PI: HP Performance Insight Installation and Upgrade Guide for Oracle Databases*
- *PI: HP Performance Insight Installation and Upgrade Guide for Sybase Databases*
- *PI Reporting Solutions: Interface Reporting Report Pack User Guide*
- *PI Reporting Solutions: Threshold and Event Generation Module User Guide*

2 Installing the Integration Module

Preinstallation Steps

- ▶ You must install the NNM integration components on the NNM server before installing the PI integration components on the PI server. The reason is that PI synchronizes the device list by accessing components on the NNM management station.

Before installing the Integration Module, you must follow these steps:

- 1 Verify that you have installed the following softwares and patches:

- HP Performance Insight 5.41
- HP Network Node Manger 7.x, NNMi 8.1x, NNMi 9.0x, or 9.10. If you have installed NNMi 8.1x, NNMi 9.0x, or 9.10, proceed to [step 3](#).
- The latest consolidated NNM patch

- ▶ Service packs and patches are available at:
<http://support.openview.hp.com/selfsolve/patches>

- 2 *Windows only*: Set the Write permission for the Internet Guest Account on the NNM server. To do so, follow these steps:

- a From the Control Panel window, double-click the **Administrative Tools** and then double-click **Computer Management**. The Computer Management window opens.
- b In the console tree, expand **Local Users and Groups**, and click **Users**.
- c Note down the name of the Internet Guest Account.
- d Navigate to the NNM installation directory. Locate the `tmp` directory and right-click and select **Sharing** or **Sharing and Security** from the submenu.

- e Click the **Security** tab and click **Add**.
 - f In the Enter the object name to select box, type the name of the Internet Guest Account and click **OK**.
 - g Select Internet Guest Account and add the Write permission to the list of allowed permissions.
 - h Click **OK**.
- 3 **For NNMi 8.1x, NNMi 9.0x, or 9.10 only:** To synchronize the NNM nodes, create a new web service client user account, if a web service client does not exist on the NNM server. For more information about creating a user account, see the *HP Network Node Manager Help*.

If you encounter problems during installation, see [Troubleshooting](#) on page 39.

Installing the Integration Module on NNM

The NNM and PI Integration module to integrate NNM 7.5x and PI is shipped with NNM 7.x version and the module to integrate NNMi 8.1x, 9.0x, or 9.10 and PI is shipped with PI 5.41 version.

Installing the Integration Module on NNM 7.5x

The NNM and PI Integration module is by default in passive mode. After you install NNM and PI, run the `install.ovpl` script to complete the integration. The `install.ovpl` script configures the NNM and PI Integration module. This script is present at the following locations:

- HP-UX and Solaris

```
$OV_MAIN_PATH/newconfig/OVNNM-RUN/OVPI_INTEGRATION/  
install.ovpl
```

- Windows

```
%OV_MAIN_PATH%\conf\OVPI_INTEGRATION\install.ovpl
```

When you run the `install.ovpl` script it will prompt you to enter the fully-qualified name of the PI server and the port number of PI web server.

For more information about the `install.ovpl` script refer to [The install.ovpl Script](#) on page 45.

Installing the Integration Module on NNMi 8.1x, 9.0x, or 9.10

Install PI 5.41 and run the `piurlconf.ovpl` script.

The `piurlconf.ovpl` script configures PI URL actions on the NNM server and SNMP traps on NNMi 8.1x, 9.0x, and 9.10. The PI URL actions lets you launch PI reports on the NNM server. To run the `piurlconf.ovpl` script, follow these steps:

- 1 Navigate to the following location on PI:
 - HP-UX and Solaris: `<DPIPE_HOME>/data/nnmpi_confnew`
 - Windows: `<DPIPE_HOME>\data\nnmpi_confnew`

In this instance, `<DPIPE_HOME>` is the directory into which you installed PI.

- 2 Copy the `piurlconf.ovpl`, `PIURLActions.xml`, and `PIIncidents.xml` files.
- 3 Create a new folder with the name `nnmpi_conf` at the following location on the NNM server:
 - HP-UX and Solaris: `<install_dir>/newconfig/`
 - Windows: `<install_dir>\newconfig\`

In this instance, `<install_dir>` is the directory into which you installed NNM.

- 4 Paste the `piurlconf.ovpl`, `PIURLActions.xml` and `PIIncidents.xml` files in the `nnmpi_conf` directory.
- 5 Run the `piurlconf.ovpl` script. The `piurlconf.ovpl` script will prompt you to enter the fully-qualified name of the PI server, port number of the web server, communication protocol (`http` or `https`), NNM user name, and password.

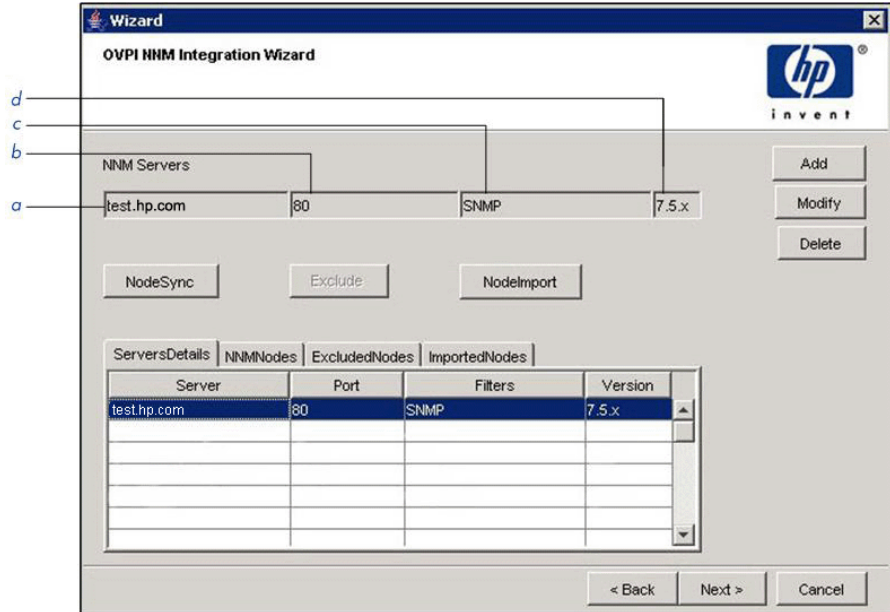
Installing Integration Components on PI

The core components of NNM and PI Integration module is now shipped along with PI 5.41.

To install integration components on PI, follow these steps:

- 1 Locate the `NNMPI_Wizard` file, which is present at the following location:
`<DPIPE_HOME>/bin`
In this instance, `<DPIPE_HOME>` is the directory in which you installed PI.
- 2 Start the NNM and PI integration wizard:
 - UNIX: `$NNMPI_Wizard`
 - Windows: Double-click `NNMPI_Wizard.exe` file.

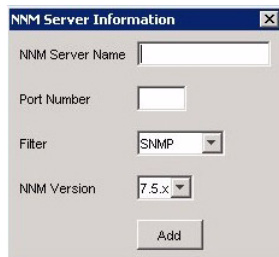
The OVPI NNM Integration Wizard opens. You can add, modify or delete NNM servers details.



Legend

- a NNM server hostname or IP address
- b Port number
- c Filter list
- d NNM server version

3 Click **Add**. The NNM Server Information dialog opens.



4 In the NNM Server Name box, type the hostname or IP address of the NNM server.

- 5 In the Port box, type the port number. The port number *must* be the HTTP port specified during the installation of the Integration Module.
- 6 From the Filter list, select one of the following filters:
 - **SNMP**: Imports all SNMP nodes.
 - **NON SNMP**: Imports all non-SNMP nodes.
 - **ALL**: Imports both SNMP and non-SNMP nodes.
- 7 From the NNM Version list, select one of the following items:
 - **NNM 7.5x**: Proceed to [step 10](#).
 - **NNMi 8.1x, 9.0x, or 9.10**: The User Name, Password, and Re-Type Password boxes are enabled.
- 8 In the User Name box, type the username of the web service client.
- 9 In the Password and Re-Type Password box, type the password of the web service client.
- 10 Click **Add**.

The server details appear in the ServersDetails tab. The details are stored in the `nm_node_src.txt` file. See [Table 1](#) on page 20 for details. Use the **Modify** and **Delete** buttons to modify or delete the server details.

- 11 Click **NodeSync**. The following occurs:
 - A list of NNM nodes is obtained from the NNM server. The list is stored in the `nm_node_list.txt` file. [Table 1](#) on page 20 for details.
 - The specified filters are applied. The nodes that are present after applying the filter are stored in the `nm_node_list_filtered.txt` file. See [Table 1](#) on page 20 for details.
 - The NNM nodes that are not already present in PI appear in the NNMNodes tab.
- 12 If you want to exclude the import of any NNM node to PI, select the node from the **NNMNodes** tab and click **Exclude**. The nodes that you exclude appear in the **ExcludedNodes** tab. The excluded nodes are stored in the `nm_nodes_exclude.txt` file. See [Table 1](#) on page 20 for details.
- 13 Click **NodeImport**. The following occurs:
 - The NNM and PI Integration wizard imports the NNM nodes that are not excluded.


- The imported NNM nodes appear in the ImportedNodes tab. The imported nodes are stored in the `nnm_nodes_import.txt` file. See [Table 1](#) on page 20 for details.
-  If you delete a node in the NNM, the node does not get deleted automatically in the OVPI server.

Table 1 Files Created by OVPI NNM Integration Wizard

File Name	Description	Location
<code>nnm_node_src.txt</code>	Contains the details of NNM server, port, filter, and version. This file is required for automatic scheduling of NNM and PI Integration module.	<code>OVPI_HOME/lib</code>
<code>nnm_node_list.txt</code>	Contains a list of NNM nodes obtained from the NNM server.	<code>OVPI_HOME/lib</code>
<code>nm_node_list_filtered.txt</code>	Contains a list of nodes present after applying the filter.	<code>OVPI_HOME/lib</code>
<code>nnm_nodes_exclude.txt</code>	Contains a list of excluded nodes.	<code>OVPI_HOME/lib</code>
<code>nnm_nodes_import.txt</code>	Contains a list of NNM nodes imported into PI.	<code>OVPI_HOME/lib</code>
<code>NNMPI_Wizard.log</code>	Contains messages pertaining to the operation of OVPI NNM Integration Wizard.	<code>OVPI_HOME/log</code>
<code>NNMPI_Cmd.log</code>	Contains messages pertaining to the operation of <code>nnmpi_cmd</code> command.	<code>OVPI_HOME/log</code>

Integrating Multiple NNM Servers with PI

The steps to add multiple NNM servers are similar to adding a single NNM server.

- 1 Follow steps 1 through 10 listed under [Installing Integration Components on PI](#) on page 17 for every NNM server you want to integrate with PI.

The added servers are stored in the `nnm_node_src.txt` file.

- 2 From the command prompt, run the command:

```
nnmpi_cmd
```

This syncs up all the nodes under the added NNM servers.

Automatic Scheduling of the NNM and PI Integration

You can schedule the process of importing NNM nodes to PI, to run at regular intervals by appending the following line at the end of the `trendtimer.sched` file.

```
24:00+1:00 - - {DPIPE_HOME}/bin/nnmpi_cmd
```

The `nnmpi_cmd` requires the `nnm_node_src.txt` and `nnm_nodes_exclude.txt` files. These files are created when you run the OVPI NNM Integration Wizard. The operations of `nnmpi_cmd` command are present in the `NNMPI_Cmd.log` file.

Post-Installation Steps

After the installation of the NNM and PI Integration Module, you must perform the following configuration steps before PI threshold alarms can populate the NNM alarm browser and PI reports can be generated from NNM nodes:

- Specify the NNM management station to be used as the trap destination for PI threshold traps.

For information on how to enter data in the SNMP Trap Destinations List configuration window, see [Configuring an NNM Trap Destination for PI Threshold Traps](#) on page 22.

- Install other Report Packs of interest to you. For example, to monitor MPLS threshold violation traps, install the suite of MPLS report packs and datapipes, including the MPLS VPN Report Pack and the MPLS Thresholds Report Pack. For more information about the PI Report Packs, see the individual Report Pack user guides.

Configuring an NNM Trap Destination for PI Threshold Traps

During the installation of the OVPI Threshold package, a trap destination for PI-generated threshold traps is defined. By default, the OVPI Threshold package sends traps to the localhost.

Configure an NNM Trap Destination on UNIX

To modify the default trap destination on a PI server running a UNIX operating system, follow these steps:

- 1 As a trendadm user, start the PI administrator utility:
`$DPIPE_HOME/bin/piadmin`
- 2 Click **Objects** in the left-hand pane.
- 3 Click **File** → **New** → **Update SMTP Trap Actions Definition**.
- 4 Click **Create**. The Thresholds window opens.
- 5 Fill all the fields in the Thresholds form
- 6 Click **Apply** and then click **OK**.

Configure an NNM Trap Destination on Windows

To modify the default NNM trap destination on a PI server running a Windows operating system, follow these steps:

- 1 As a user with administrative privileges, start the PI administrator utility by selecting **Start** → **Programs** → **HP Software** → **Performance Insight** → **Management Console**.
- 2 Login as `trendadm` user.
- 3 Click **Objects** in the left-hand pane.
- 4 Click **File** → **New** → **Update SMTP Trap Actions Definition**.
- 5 Click **Create**. The Thresholds window opens.
- 6 Fill all the fields in the Thresholds form
- 7 Click **Apply** and then click **OK**.

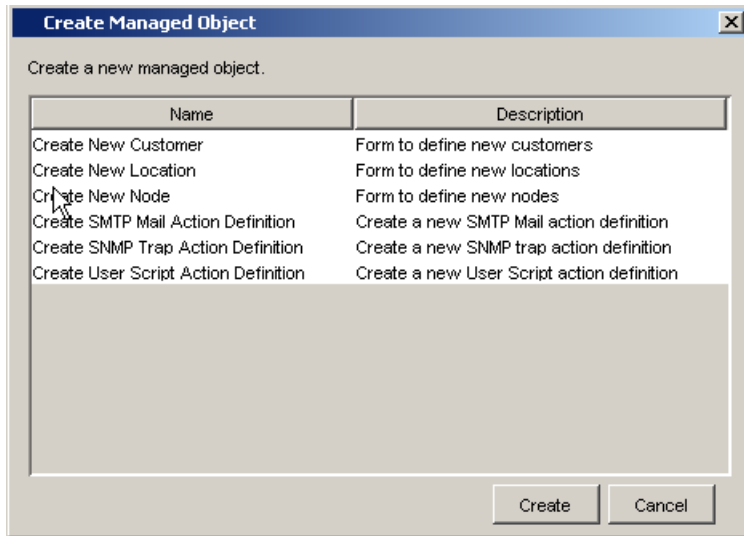
Configure Multiple NNM Trap Destinations

Typically, you need only one NNM management station to accept PI-generated threshold traps, however, multiple NNM management stations can be configured.

To configure multiple trap destinations for PI-generated threshold traps, follow these steps:

- 1 Start the PI administrator utility by executing the following command:
UNIX (as user `trendadm`): **`$DPIPE_HOME/bin/piadmin`**
Windows: **Start** → **Programs** → **HP Software** → **Performance Insight** → **Management Console**
- 2 Click the **Objects** icon in the left-hand pane.
- 3 Click **File** → **New** to open the Create a New Managed Object window as shown in [Figure 1](#).

Figure 1 Create a New Managed Object Window




- 4 From the list, select Create SNMP Trap Action Definition.
- 5 Click **Create** to display the Thresholds:Create SNMP Trap Action Definition form. See [Figure 2](#) on page 25.
- 6 Enter the host name and SNMP port number of the NNM management station to which PI traps have to be forwarded.

Figure 2 Trap Action Destination Form

Thresholds

Create SNMP Trap Action Definition



invent

This form allows SNMP trap action definitions to be created for use with the thresholds package.

The thresholds package monitors OVPi data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then an SNMP trap containing data about the threshold breaches will be sent using the parameters defined below. For information on the trap payload see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.

Example

Category = FRAME_RELAY Severity = MEDIUM Server = nnm.mydomain.com Port = 162 Community = public	If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then an SNMP trap containing details of the threshold breach will be sent to the port 162 on nnm.mydomain.com with community set to public.
--	--

All fields are mandatory.

Click the Apply button to save any changes.
 Click the Cancel button to cancel any changes.
 Click the OK button to save changes and close the form.

Category	<input style="width: 80%;" type="text"/>
Severity	<input style="width: 80%;" type="text"/>
Server	<input style="width: 80%;" type="text"/>
Port	<input style="width: 80%;" type="text"/>
Community	<input style="width: 80%;" type="text"/>

Last action definition created

Category	Severity	Server	Port	Community
*	*	test100.cnd.hp.com	80.00	public

Uninstalling the NNM and PI Integration Module

To uninstall the NNM and PI Integration Module, you must uninstall PI. For more information about uninstalling PI, see *Installation and Upgrade Guide for Oracle Databases* or *Installation and Upgrade Guide for Sybase Databases*.

3 Verifying the Installation

This section describes the process for checking if your system is configured properly.

Verifying NNM Node Synchronization

To verify devices have been imported into PI from NNM through the NNM node synchronization, follow these steps:

- 1 Start the PI administrator utility:

UNIX: `$DPIPE_HOME/bin/piadmin`

Windows: click **Start** → **Programs** → **HP Software** → **Performance Insight** → **Management Console**; or run

`%DPIPE_HOME%\bin\piadmin`

- 2 Select **Polling Policies**.
- 3 Click **Edit** → **Nodes** to open the Nodes window.

The Nodes window displays all nodes known to PI for data collection, and should contain nodes imported from NNM.

Verifying Report Launching

To verify that PI reports can be launched from NNM, try one of the following report launching utilities:

- 1 Verify that you can launch a report from the NNM alarm browser by selecting a PI threshold alarm and launching a report with the **Actions:Additional Actions** menu.
- 2 Verify that you can launch a report from a view in Dynamic Views by selecting a node in the view and using the **Performance:OVPI Launch Pad** menu to launch a PI performance report.
- 3 Verify that you can launch a report from an NNM map by selecting a node and using the **Performance** menu to launch a PI report.

4 Launching Device-Specific Reports

The NNM and PI Integration Module supports the launching of PI performance reports from NNM 7.x, 8.1x, 9.0x, or 9.10 servers.

Launching Reports from NNM 7.x Server

You can launch PI performance reports from several NNM 7.x user interfaces, including:

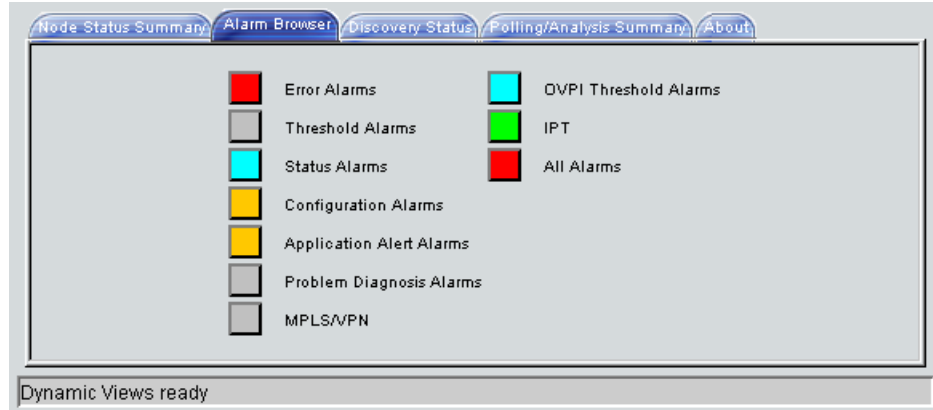
- Native NNM alarm browser
- NNM Extended Topology dynamic view
- NNM submap (ovw)

A launched report contains information specific to the node that was selected (if launching from a map or view) or the node that caused the alarm (if launching from the alarm browser).

Launching Reports from the Native NNM Alarm Browser

A key feature of the NNM and PI Integration Module is the creation of an alarm category, OVPI Threshold Alarms, in the Alarm Categories window of the NNM alarm browser. See [Figure 3](#) on page 30.

Figure 3 OVPI Threshold Alarm Category of the NNM Alarm Browser.



You can view alarms received by the NNM management station by double-clicking the **OVPI Threshold Alarms** category to open the OVPI Threshold Alarms Browser.

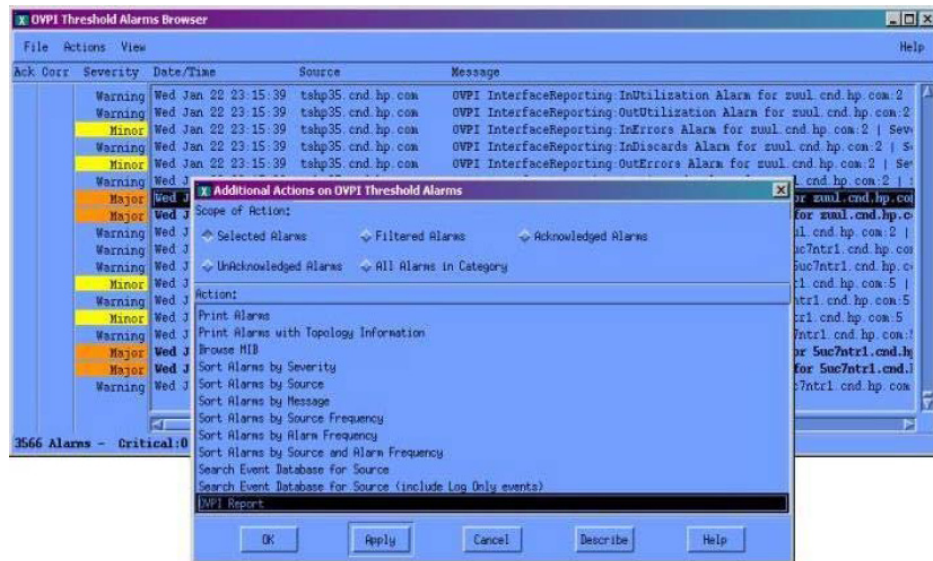


Launching PI performance reports from a PI threshold alarm is available only from the native NNM alarm browser. In Dynamic Views, you can view threshold traps in the OVPI Threshold Alarms Browser, however, menus for launching PI reports are not available.

To launch a PI performance report from an alarm in the Threshold Alarms Browser, following these steps:

- 1 Select an alarm in the alarm browser.
- 2 Click **Actions:Additional Actions**, and then select **OVPI Report**. [Figure 4](#) on page 31 depicts the OVPI Threshold Alarm Browser containing PI threshold alarms and also shows the OVPI Report action selected.

Figure 4 PI Report from Threshold Alarm Browser.



The PI report launch action is defined for all PI threshold alarms. The MIB definition for the PI threshold event can be found at:

UNIX: `$OV_NEWCONFIG/OVPI_INTEGRATION/hp-ovpi.mib`

Windows: `<install_dir>\conf\OVPI_INTEGRATION\hp-ovpi.mib`

- The result of launching the OVPI Report action depends on how the node that caused the alarm is configured.

- Launching a PI report for a node that has an assigned PI OID causes the report specific to that OID to launch.

The `OvpiRptLaunch.conf` configuration file contains the assignments of PI reports to PI OIDs, and is located at:

UNIX: `$OV_NEWCONFIG/OvpiRptLauncher.conf`

Windows: `<install_dir>\conf\OvpiRptLauncher.conf`

- Launching a PI report for a node that does not have a PI OID causes the Report Launchpad window to launch, as shown in [Figure 5](#) on page 32.

Figure 5 The Report Launchpad Window



► The report launch menu lists items for nodes that are known to NNM as Routers, Bridges, Hubs, or Connectors.

- 4 From the Report Launchpad window, select the desired report to launch. A launched report contains information specific to the node that caused the alarm.

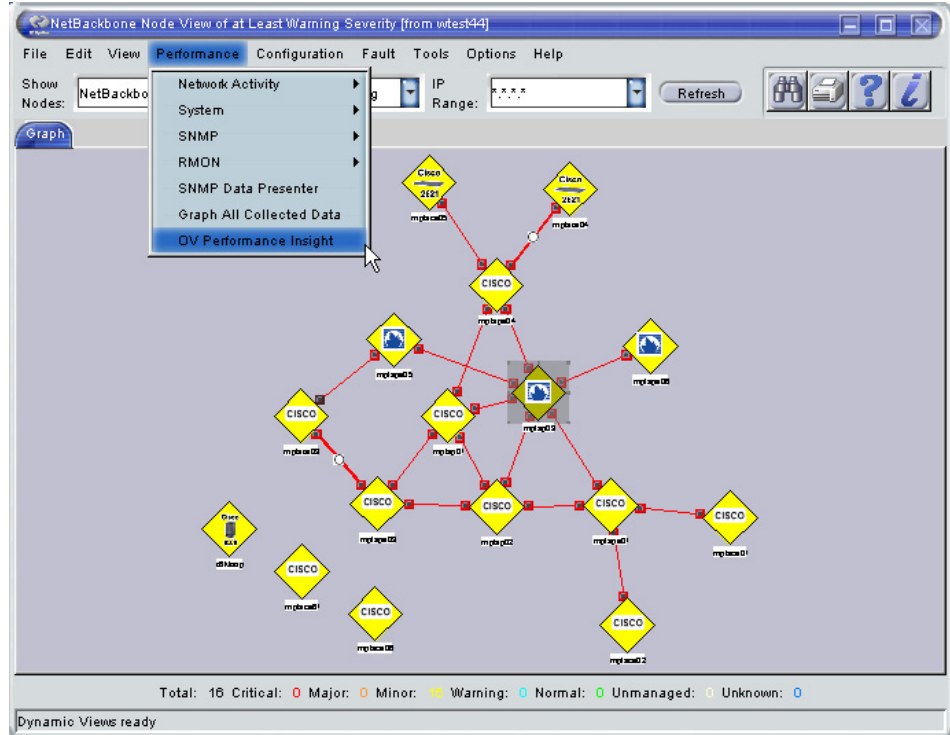
Launching Reports from NNM Dynamic Views

To launch a performance report from an NNM Extended Topology dynamic view, do the following:

- 1 Select a node.
- 2 Use either the Performance menu or the OVPI Launch Pad shortcut menu (right-click the node):
 - Click **Performance: OV Performance Insight**, as illustrated in [Figure 6](#) on page 34.
The Report Launchpad window opens, as shown in [Figure 5](#) on page 32.
 - Right-click, and select **OVPI Launch Pad**.
- 3 Select the desired report to launch.

The launched report contains information specific to the node that was selected.

Figure 6 Launching PI Reports from Dynamic Views

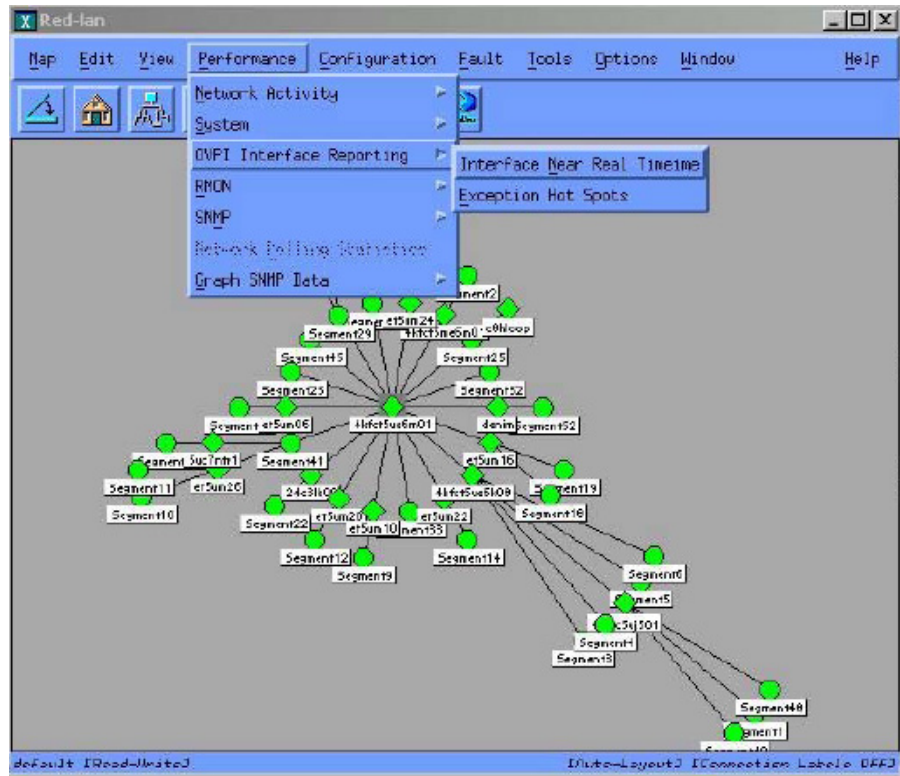


Launching Reports from an NNM Map

To launch a PI performance report from an NNM map, do the following:

- 1 Select a node in the NNM map.
- 2 Use either the Performance menu or the report launcher shortcut menu (right-click the node):
 - Click **Performance: OVPI Report Launcher** as shown in [Figure 7](#) on page 35.
 - Right-click, and then select **OVPI Report Launcher**.

Figure 7 Launching PI Reports from NNM Maps



When you launch a report, NNM notifies PI of the device name. PI, in return, launches a Report Launchpad window that displays a list of appropriate reports for that device.

- 3 From the Report Launchpad window, select the desired report to launch. See [Figure 5](#) on page 32.

The launched report contains information specific to the node that was selected.

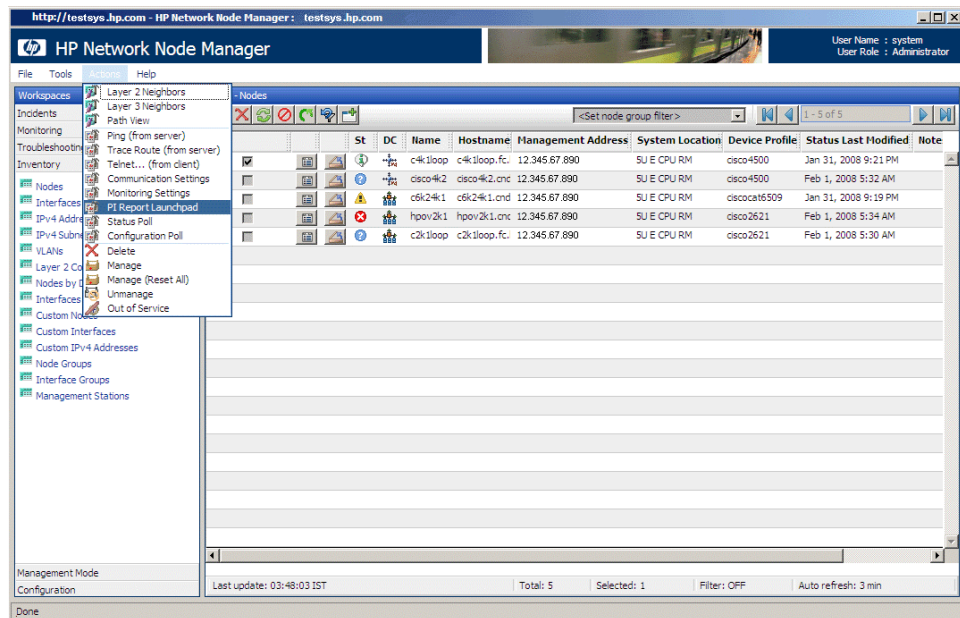
Launching Reports from NNMi 8.1x, 9.0x, or 9.10 Server

You can launch PI performance reports from NNMi 8.1x, 9.0x, or 9.10 Inventory and Incidents.

Launching Reports from Inventory Workspace

To launch PI reports from Inventory workspace, follow these steps:

- 1 Log on to the console of NNMi 8.1x, 9.0x, or 9.10 using administrative privileges.
- 2 From the workspace navigation panel, select the **Inventory** workspace.
- 3 Click **Nodes**.
- 4 Click to select a Performance Insight node of interest.
- 5 From the **Actions** menu in the menu toolbar of the NNM console, select **PI Report Launchpad**. See the figure below.



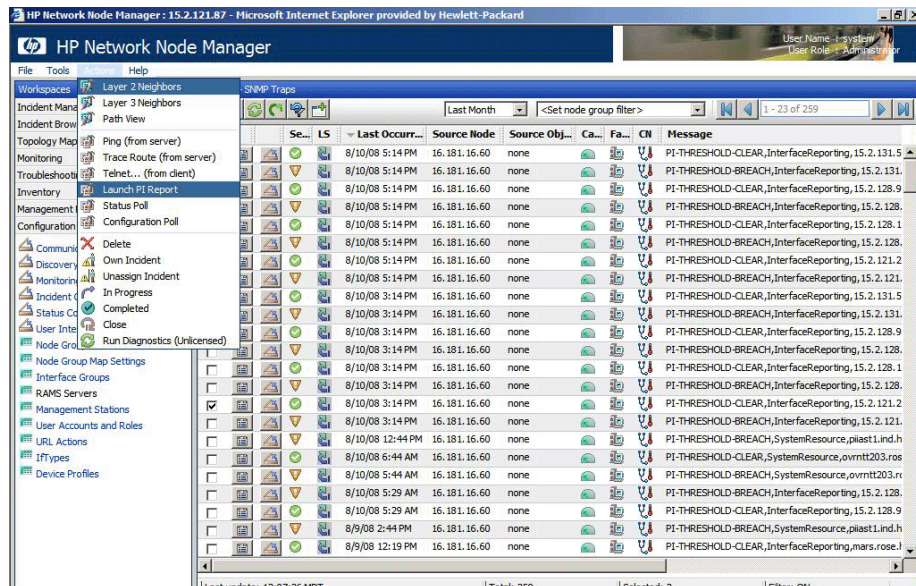
The Report Launchpad window for the selected node opens.

- From the Report Launchpad window, select the desired report to launch. A launched report contains information specific to the selected node.

Launching Reports from Incidents Workspace

To launch PI reports from Incidents workspace, follow these steps:

- Log on to the console of NNMi 8.1x, 9.0x, or 9.10 using administrative privileges.
- From the workspace navigation panel, select the **Incidents** workspace.
- Click **SNMP Traps**.
- Click to select a SNMP trap with respect to Performance Insight where the value of the Message is `PI_THRESHOLD_BREACH` or `PI_THRESHOLD_CLEAR`.
- From the Actions menu in the menu toolbar of the NNM console, select **Launch PI Report** for the report that you want to view. For example, if you have selected `PI_THRESHOLD_CLEAR` trap, you must select a corresponding clear trap report. See the figure below.



A launched report depends on the node and the threshold category that caused the incident.

5 Troubleshooting

This section contains troubleshooting information about NNM 7.5x. For troubleshooting information about NNMi 8.1x, 9.0x, or 9.10, see the log files at the following location:

- UNIX: `/var/opt/OV/log/nnm/`
- Windows: `<install_dir>\data\log\nnm\`

In this instance, `<install_dir>` is the directory into which you installed NNMi 8.1x, 9.0x, or 9.10.

Node Synchronization is not Working

NNM devices are not being imported into PI from NNM through NNM Device Synchronization

If no NNM devices are being imported into PI from NNM through NNM Device Synchronization, follow these steps:

- 1 Verify that the NNM management station from which device information is to be imported is running and accepting requests on the port specified during the installation of the Integration Module package.

To verify NNM management station is accepting requests by using its assigned port, enter the following URL in a web browser:

`http://<hostname>:<port>/OvCgi/nodeList.ovpl`

where *hostname* is the name of the NNM management station, and *port* is the HTTP port number assigned to the NNM management station during installation of the Integration Module package. For NNM management stations running UNIX, the port number should be 3443. For NNM management stations running Windows, the port number should be 80.

Note that the output appearing in the web browser is encrypted.

- 2 Verify that the Trend timer process is running. If it is not, restart it.
- 3 Verify that there is an entry for `SyncNodeList` in the `trendtimer.sched` file located at:

UNIX: `$DPIPE_HOME/lib/`

Windows: `%DPIPE_HOME%\lib`

If no entry exists, device synchronization is not taking place. The cause for the missing entry is most likely a failure during installation.

- 4 Check `$TREND_LOG/trend.log` for errors.
- 5 Check web server log for error:

UNIX: `/var/opt/OV/log/httpd_error_log`

Windows: System Events

NNMi devices are not being imported into PI from NNMi through NNMi Device Synchronization

If no NNMi devices are being imported into PI from NNMi through NNMi device synchronization, follow these steps:

- 1 Verify the NNMi management server's availability.

To verify whether the NNMi management server accepts requests by using its assigned port or not, test the following two URLs by using a web browser:

a **`http://<hostname>:<port>/`**

where `<hostname>` is the name of the NNMi management server and `<port>` is the HTTP port number assigned to the NNMi management server during installation of the Integration Module package. The default HTTP port for NNMi used for Web UI and Web Services is 80.

The application index page opens if the integrated NNMi management server is up and running.

b **`http://<hostname>:port/NodeBeanService/NodeBean?wsdl`**

where `<hostname>` is the name of the NNMi management server and `<port>` is the HTTP port number assigned to the NNMi management server during installation of the Integration Module package. The default HTTP port for NNMi used for Web UI and Web Services is 80.

The rest of the URL identifies the web-service which handles the *nodeList* transaction.

When you type this URL in to the browser, WSDL (web service Description Language) an XML content is displayed indicating the web-service handling the *nodeList* transaction is up and running.

- 2 Check the status of the web-service call (whether it is a success or a failure) and the number of nodes fetched from NNMI (when the call succeeds) that are logged in `NNMPI_Wizard.log` located at `OvInsallDir/log` directory.
- 3 Verify that the Trend timer process is running. If it is not running, restart it.
- 4 Verify that there is an entry for `SyncNodeList` in the `trendtimer.sched` file located at:

UNIX: `$DPIPE_HOME/lib/`

Windows: `%DPIPE_HOME%\lib`

If no entry exists, device synchronization is not taking place. The cause for the missing entry is most likely a failure during installation.

- 5 Check `$TREND_LOG/trend.log` for errors.
- 6 Check web server log for error:

UNIX: `/var/opt/OV/log/httpd_error_log`

Windows: System Events

Launched Reports Contain no Data

If this condition occurs, verify that the NNM device synchronization components are functioning by using the procedures described in [Node Synchronization is not Working](#) on page 39.

NNM Device Sync Installation Fails

Common installation failures include the following:

- All NNM node sources specified by the user are not reachable

- The NNM and PI Integration Module was not installed on those NNM management stations.
- The wrong HTTP port number was specified for the NNM management station during the installation of the Integration Module package.

Details of the failure can be found in the `$DPIPE_HOME/log/trend.log` file.

NNM Device Sync Fails for Some of the NNM Node Sources

This may occur if the NNM node is not reachable, or if the NNM and PI Integration Module is not installed on that NNM management station for which the NNM Device Sync failed. The details of the failure can be found in the `$DPIPE_HOME/log/trend.log` file.

Unable to Open NNM Event reports on Windows



This problem occurs only when NNM is running on a Windows operating system.

When using the NNM and PI Integration Module in conjunction with the HP Performance Insight NNM Event Report Pack, NNM may not be able to access its version of Perl. As a result, NNM Event reports may not be generated properly.

On the NNM management station, modify the Windows PATH environment variable so that the path to NNM's copy of Perl is listed first. When NNM is installed in its default location, the following must be added to the beginning of the Windows PATH environment variable:

```
C:\Program Files\HP OpenView\bin\Perl\bin
```

Additional Troubleshooting Resources

For additional troubleshooting information, see the log files created by the OVPI NNM Integration wizard. [Table 1](#) on page 20 lists the files created by the OVPI NNM Integration wizard.

You can also refer to the latest *NNM and PI Integration Module Release Notes* available on the web at <http://h20230.www2.hp.com/selfsolve/manuals> under the NNM and PI Integration Module product category.

6 Reference

The install.ovpl Script

The Perl install script, `install.ovpl`, first installs the HPOvIco3.01.00.1 (HP Interconnect) package on the NNM management station. The script then modifies Application Registration Files (ARF) with the node name and port information of the PI server.

It then places these files in the correct location on the NNM management station. This configuration enables node-specific launching of PI reports from the NNM management station.

The script prompts you for the hostname of the PI server and the port number on which that server receives HTTP requests. See [Table 2](#) on page 46 for a complete list of command line options for `install.ovpl`. For the standard installation, run the script without any options.



Run this script with the version of Perl shipped with NNM.

Table 2 Command Line Options for install.ovpl

install.ovpl option	Description
No options <i><default></i>	If no options are specified, install.ovpl updates every ARF file and browser action file in the OVPI_INTEGRATION directory and places those files in their appropriate locations.
-force all	By default, install.ovpl does not replace ARF files on repeated invocations to guard against accidentally overwriting already configured versions. The use of the force option with the all argument causes install.ovpl to reconfigure and re-place the ARF files located in the OVPI_INTEGRATION directory. This option is useful when modifying every ARF to point to a different PI server, or if the HTTP port number on the PI server has changed.
-force <file.arf>	Using the <i><file.arf></i> argument with the force option causes install.ovpl to configure and place the specified ARF file only. This option is useful when launching different reports on different PI servers.

Index

A

alarm category
 OVPI Threshold Alarms, 10, 29

C

commands
 install.ovpl, 45
 nodeList.ovpl, 39
configuring trap destination, 22
Create a New Managed Object window, 23
Create SNMP Trap Action Definition option,
 24, 25

D

device list synchronization
 troubleshooting, 39, 40
 uninstalling, 26
 verifying list of nodes, 27
documentation
 related, 11

F

features
 Integration Module, 9
filters
 all nodes, 19
 non-SNMP, 19
 SNMP, 19

H

HP Performance Insight Installation and
 Upgrade Guide for Oracle Databases, 11
HTTP port number
 specifying, 39

I

install.ovpl script, 45
Installation
 PI components, 17
installation
 PI Report Packs, 22
Integration Module
 installing PI components, 17
 launching PI reports
 from alarm browser, 29
 from Dynamic Views, 33
 from NNM maps, 34
 MIB files, 31
 uninstalling, 26

L

launching PI reports
 from alarm browser, 30
log files
 trend.log, 42

M

manuals

- Creating and Using Registration Files, 11
- HP Performance Insight Administration Guide, 11
- HP Performance Insight Guide to Building and Viewing Reports, 11
- HP Performance Insight Installation and Upgrade Guide for Oracle Databases, 11
- listing related, 11
- Managing Your Network, 11
- NNM and OVPI Integration Module Release Notes, 43
- Threshold and Event Generation Module, 11

MIB files, 31

N

NNM alarm browser

- launching PI reports from, 29
- OVPI Threshold Alarms, 29

NNM Device Sync package

- troubleshooting installation, 41

NNM Event reports

- troubleshooting, 42

NNM management station

- configuring multiple trap destinations, 23
- verifying port number, 39

nodeList.ovpl script, 39

node sources

- troubleshooting, 39, 40

node synchronization

- SyncNodeList entry, 40
- troubleshooting, 39, 40

O

OvpiRptLauncher.conf file, 31

OVPI Threshold Alarms Browser window, 30

OVPI Threshold Alarms category, 29

P

PI

administrator GUI, 27

PI reports

- launching, 11
- launching from an alarm, 30
- launching from Dynamic Views, 33
- launching from NNM maps, 34
- verifying launching to, 28

PI Threshold Alarms browser

launching PI reports, 29

port numbers

- NNM management station on UNIX, 39

prerequisites

service packs and patches, 13

R

Report Launchpad window, 31, 32, 33, 35

reports

- launching PI, 11
 - from Dynamic Views, 33
 - from NNM alarm browser, 29
 - from NNM maps, 34
- NNM Event, 42
- verifying launching to PI, 28

resources

related documentation, 11

S

SNMP port number, 24

SNMP Trap Destinations List window, 22

T

Thresholds window, 23

threshold traps

 configuring to receive, 22, 23

trap destination

 configuring another, 22

 configuring multiple, 23

trend.log file, 42

trendadm user, 23

trendtimer.sched file, 40

Trend timer process

 verifying running, 40

U

users

 trendadm, 23

W

windows

 OVPI Threshold Alarms Browser, 30

 PI Management Console, 27

 Report Launchpad, 31, 32, 33, 35

 SNMP Trap Destination, 22

 Thresholds

 Create a New Managed Object, 23