
HP Network Node Manager i Software Release Notes

Software Version: 10.01 / 08 December 2014

This document provides an overview of the changes made to HP Network Node Manager i Software (NNMi) version 10.01

It contains important information not included in the manuals or in online help.

For the latest additions to these Release Notes, see [NNMi 10.0x Release Notes Updates](#).

For a list of supported hardware platforms, operating systems, and database, see the [HP Network Node Manager i Software System and Device Support Matrix](#). For the list of supported network devices, see the [HP Network Node Manager i Software \(NNMi\) Device Support Matrix](#).

[What's New In This Version](#)

[Documentation Updates](#)

[Deployment Reference](#)

[Upgrade Reference](#)

[Documentation Errata](#)

[Installation Guide and Support Matrix](#)

[Licensing](#)

[HP Network Node Manager i Advanced Software Features](#)

[HP Network Node Manager i Premium Software Features](#)

[HP Network Node Manager i Ultimate Software Features](#)

[HP Network Node Manager iSPI Network Engineering Toolset Software Features](#)

[Known Problems, Limitations, and Workarounds](#)

[Potential Installation Issues](#)

[Internet Explorer Browser Known Problems](#)

[Mozilla Firefox Browser Known Problems](#)

[Non-English Locale Known Problems](#)

[Domain Name System \(DNS\) Configuration Known Problems](#)

[IPv6 Known Problems and Limitations](#)

[Device Support Known Limitations](#)

[MIB Loader Migration Known Problems](#)

[Integration Known Problems](#)

[HP Software Support](#)

[Legal Notices](#)

What's New In This Version

Overview of the NNMi 10.01 Release

NNMi 10.01 is a patch of the NNMi 10.00 release with some enhancements. Single system upgrades of NNMi 9.1x and NNMi 9.2x to NNMi 10.0x are supported (see the [Upgrade Reference](#)). NNMi 8.x or 9.0x installations must be upgraded to NNMi 9.1x or 9.2x before being upgraded to NNMi 10.0x.

NNMi 10.01

- **Changes to Supported Environments**
 - Adds support for Apple Safari 7 on an OS X client.
 - Adds support for Firefox 31.x ESR.
- **Configuring the Locale for Sort Order of User Names when Assigning Incidents**
 - An NNMi administrator can specify the language locale for the NNMi management server that should be used to determine the sort order of user names when assigning incidents (in the **Assign Incidents** dialog (only)). When determining alphabetical order, NNMi uses the user display name rather than the actual login name and does not sort capital letters separately from lowercase.
 - To configure the language locale to use for the sort order of the user names, edit the `server.properties` file. The default sort

locale value is English (en_US). See the **Configuring the Locale for Sort Order of User Names when Assigning Incidents** section of the [Deployment Reference](#) for more information.

- **Replicate NNMi Management Server Configuration**

- NNMi enables you to use the export and import option to replicate the configuration between two NNMi management servers. To replicate the NNMi configuration from one NNMi management server to another, use the `nnmconfigexport.ovpl` command with the `-c all` option and then use `nnmconfigimport.ovpl` command with the `-sync` option.
- When you use the `-sync` option to the `nnmconfigimport.ovpl` command, NNMi does the following:
 - Replaces all object instances with matching key identifiers (see the **Troubleshooting Imports of Configuration Files** in the Online Help for Administrators for information about key identifiers).
 - Adds all object instances with key identifiers that do not exist in the NNMi database.
 - Deletes all existing object instances with key identifiers that do not match any in the exported file.

Note: If you are exporting a customized subset of a configuration workspace using the `-a` option (for example, `-c device -a <authorUniqueKey>`), do not use the `nnmconfigimport.ovpl` command with the `-sync` option.
- See the **Online Help for NNMi Administrators** for more information.

- **SSLv3 Ciphers**

- By default, SSLv3 ciphers are now disabled.
- When SSLv3 ciphers are disabled, note the following:
 - Ensure that at least one of your web browser protocols match that used in NNMi. NNMi supports the following TLS ciphers by default:
TLS v1, TLS v1.1 and TLS v1.2
 - If you have any issues with your web browser, try the following in the order specified:
 - a. Check that your web browser version is supported by NNMi.
 - b. Enable SSLv3 as described in **Configuring NNMi to Enable or Disable SSLv3 Ciphers** in the Deployment Reference.
 - If you are integrating NNMi with other HP or Third Party software products, monitor your log files for connection issues with SSL.
 - If the HP or Third Party software only supports SSLv3, enable SSLv3 as described in **Configuring NNMi to Enable or Disable SSLv3 Ciphers** in the Deployment Reference.
- If you are using NNM iSPI software that is running on the NNMi management server, SSLv3 is also now disabled by default for each iSPI.
- If you enable SSLv3 on NNMi to resolve web browser issues, you must also enable SSLv3 for each iSPI that is running on the NNMi management server. See the Deployment Reference for each corresponding NNM iSPI for information about enabling and disabling SSLv3.
- If you are using NNM iSPI software that is running on a separate server from the NNMi management server, SSLv3 is enabled by default for that iSPI. See the Deployment Reference for each corresponding NNM iSPI for information about enabling and disabling SSLv3.

Known Problems

- *NNMi Installation only.*

Warning: If you are installing NNMi on a non-English system and want to install NNMi in English, you must configure the NNMi management server to use the English locale BEFORE the NNMi installation. You cannot change the locale to English after your NNMi installation.

To configure the NNMi management server to support the English locale on a non-English system, follow these steps:

Linux

Run the installer with the LANG=C option. For example:
export LANG=C; export LC_ALL=C ; ./setup.bin

Windows

Change the locale of the NNMi management server to English before the NNMi installation. To do so follow the steps documented for your version of the Windows operating system.

- *NNMi Upgrade only.*

The information in this section applies only if your current version of NNMi is installed in English and your NNMi management server locale is set to any of the following languages:

- German
- French
- Russian
- Spanish

Warning: If you are upgrading NNMi on a non-English system, configure the NNMi management server to use the English locale BEFORE you begin the NNMi upgrade. Otherwise, the NNMi User Interface will be a mixture of English and non-English strings. This is because strings which are new in NNMi 10.00 are inserted into the database using the language configured on the NNMi management server at the time of upgrade.

To configure the NNMi management server to support the English locale on a non-English system, follow these steps:

Linux

Run the installer with the LANG=C option. For example:
export LANG=C; export LC_ALL=C ; ./setup.bin

Windows

Change the locale of the NNMi management server to English before you begin the NNMi upgrade process. To do so follow the steps documented for your version of the Windows operating system.

- **Uninstalling NNMi.** If you have NNMi patches installed, you must first uninstall those patches before uninstalling NNMi. For information about how to uninstall a patch, see the .txt file that was delivered with the NNMi patch.

Note: You must uninstall the patches in reverse order, beginning with the most recent patch.

- *Mozilla Firefox only.* If you try to access NNMi using an unsupported version of Mozilla Firefox, NNMi displays a message that does not include the correct list of supported Web browser version numbers. See the [HP Network Node Manager i Software System and Device Support Matrix](#) for the list of Web browser versions that NNMi supports.
- *Internet Explorer only.* If you click a help link from an NNMi form, the title of the breadcrumb is displayed as true or false rather than displaying the breadcrumb to the current form. To reset the breadcrumb value, sign out of NNMi and sign in again. To access the help without changing the breadcrumb value, use the Help menu.

NNMi 10.00

• **Upgrade Notes**

- Read the new *NNMi 10.00 Upgrade Path Requirements* document for supported paths for upgrading to NNMi 10.00.
- For important notes about upgrading to NNMi 10.00, see the [Upgrade Reference](#). It is important to read these notes before performing the upgrade.

When upgrading to NNMi 10.00, you will need to add new license keys for all the products you have purchased. This is true whether you are entitled to NNMi, NNMi Advanced, NNMi Premium, or NNMi Ultimate. To obtain additional license keys, go to the HP License Key Delivery Service:
<https://webware.hp.com/welcome.asp>.

- o See the Upgrade Notes section of the *HP Network Node Manager i Software Release Notes* for 9.2x if you are upgrading from NNMi 9.1x to NNMi 10.00, since many of these points are also relevant when upgrading from NNMi 9.1x to NNMi 10.00.
- o It is recommended that you clear the browser cache of cookies and web pages before upgrading to NNMi 10.00.
- o (Linux only) If you plan to upgrade a Linux NNMi management server from NNMi 9.1x or NNMi 9.2x to NNMi 10.00, you must import the HP public key into the Linux RPM database before installing NNMi 10.00. Please see the *NNMi 10.00 Interactive Installation Guide* for more information.
- o The method of configuring LDAP user roles used in NNMi versions prior to 9.10 is no longer supported. Please ensure your LDAP configuration has been updated to use the new method before upgrading to NNMi 10.0 or later version. For more information on LDAP configuration please refer to the NNMi Deployment Reference.
- o If you are using the older NNMi 8.1x/9.0x LDAP configuration, where the LDAP groups used as roles in NNMi are identified by a specific attribute on the LDAP Group itself, you will need to update to use the newer style of configuration before upgrading to NNMi 10.00 as the older configuration is no longer supported. If you are using the 9.10 (and later) approach of mapping NNMi User Groups to LDAP Groups by registering the LDAP Group DN with the corresponding NNMi User Group, no changes are required. See "Changing the Directory Service Access Configuration to Support the NNMi Security Model" section in the [Deployment Reference](#) for instructions on updating the LDAP configuration for NNMi 9.10 or later.
- o The previous "HP UCMDB" Integration Module has been replaced by a new "HP BSM/UCMDB Topology" Integration Module. Because the UCMDB topology synchronization had previously been enabled from the UCMDB product, Administrators will need to re-enable the UCMDB topology integration via the new "HP BSM/UCMDB Topology" Integration Module. In other words, no automatic migration of UCMDB integration configuration occurs when upgrading to NNMi 10.00.
- o NNM 6.x / 7.x integration is no longer supported. Support for NNM 6.x / 7.x has ended. These changes occur when upgrading to NNMi 10.00:
 - The migration scripts from NNM 6.x / 7.x are removed.
 - The `pmd` process is removed.
 - The NNM 6.x / 7.x configuration views are removed (Management Stations (6.x / 7.x), Remote NNM 6.x / 7.x Event Configurations)
 - The NNM 6.x / 7.x Events view is removed.
 - Cross-launch menu items to NNM 6.x / 7.x servers are removed
 - All data (except existing incidents) relating to NNM 6.x / 7.x are deleted from the database.
 - If you have any remote NNM 6.x or 7.x event configurations, or pairwise configurations that involve a remote NNM 6.x or 7.x event, note the following:
 - When upgrading from NNMi 9.1x or 9.2x to 10.00, any remote NNM 6.x or 7.x event configurations, or pairwise configurations that involve an NNM 6.x or 7.x event, are automatically exported to the following directory for reference purposes and then removed from NNMi:
 - **Windows:**
`%NnmDataDir%\backups\config\legacy-remote-event-config.backup`
 - **Linux:**
`$NnmDataDir/backups/config/legacy-remote-event-config.backup`
 - All pairwise configurations that do not involve a remote NNM 6.x or 7.x event remain unchanged.
 - Any existing NNM 6.x or 7.x events are preserved in the NNMi database.

- Configuration import ignores NNM 6.x / 7.x configuration.
- Obsolete files (including /etc/opt/OV) are removed.
- In previous releases, the creation of L2 Connections based on Unnumbered Interfaces was configured through configuration files - `UnnumberedNodeGroup.conf` and `UnnumberedSubnets.conf`. This configuration is now in the NNMi database. On upgrade to NNMi 10.00, the configuration data from these files will be imported into the NNMi database; after that, these files will no longer be used.
- The NNMi SNMP Trap Receiver is now delivered as a process outside of the NNMi Application Server. This allows SNMP traps to be received for a certain period even while the NNMi Application Server is down (e.g., in a failover situation) for improved availability of trap processing. The SNMP Trap Receiver will start before NNMi on OS startup. See the *NNMi TrapReceiver Process* section in the [Deployment Reference](#) for more information on administration of the new SNMP Trap Receiver process.

• Changes to Supported Environments

- Adds support for Firefox 24.x ESR.
- Add support for Internet Explorer 10.
- Adds support for SUSE Linux 11 SP3.
- Adds support for Red Hat Linux 6.4 or later minor version.
- Adds support for Veritas 6.0 for Red Hat Linux 6.4 (or later minor version) and SUSE Linux 11 SP3.
- Adds support for Oracle Real Application Clusters (RAC) 11g Release 2.
- Internet Explorer 8 is no longer supported.
- Firefox 17.x ESR is no longer supported.
- Non-R2 Windows Server 2008 is no longer supported.
- HP-UX is no longer supported.
- Solaris is no longer supported.
- Red Hat Linux 5.x, 6.0, 6.1, 6.2, and 6.3 are no longer supported.
- SUSE Linux 11 SP1 and SP2 are no longer supported.
- VMware ESX Server 3.5 is no longer supported.
- Oracle 10g Release 2 is no longer supported.
- Veritas 5.x is no longer supported.

• Documentation Changes

- Each of the integration sections in the [Deployment Reference](#) has been moved to a separate document.
- The *NNMi 10.00 Interactive Installation Guide* is now delivered as an interactive document. See the `nnmi_interactive_installation_en_README.txt` file on the NNMi installation media for more information.

• Licensing Changes

- When upgrading to NNMi 10.00, you will need to add new license keys for all the products you have purchased. This is true whether you are entitled to NNMi, NNMi Advanced, NNMi Premium, or NNMi Ultimate. To obtain additional license keys, go to the HP License Key Delivery Service: <https://webware.hp.com/welcome.asp>.
 - You can enter the new license keys as part of the NNMi 10.00 installation process.
 - If you are still on the NNMi or NNMi Advanced license, you will also need new license keys for any NNM iSPI licenses you are using (including NNM iSPI Points).
- NNMi Premium and NNMi Ultimate licensing

NNMi Premium and NNMi Ultimate license keys are now supported. In NNMi 9.2x, NNMi Premium and NNMi Ultimate licensing was done through a combination of NNMi Advanced and NNMi Smart Plug-in (NNM iSPI) license keys.

- See the [Licensing](#) section on what is enabled by the NNMi Premium and NNMi Ultimate licenses.
- If an NNMi Premium or NNMi Ultimate license key is used, **no additional license keys**, including for NNM iSPI Points, are required for any of the NNMi Smart Plug-ins (NNM iSPIs) to which you are entitled based on the NNMi Premium or NNMi Ultimate license.
 - NNMi Premium licensing is simply based on the NNMi discovered node count. There is no separate licensing for any of the NNM iSPIs included in NNMi Premium. For example, there is no separate licensing for probes or CBQoS-enabled interfaces or intelligent Response Agents (iRA) for the NNM Performance iSPI for Quality Assurance.
 - NNMi Ultimate licensing is based on the NNMi discovered node count and the number of IP Phones managed by the NNM iSPI for IP Telephony. Except for the NNM iSPI for IP Telephony IP Phone count, there is no other separate licensing for any of the NNM iSPIs included in NNMi Ultimate. For example, there is no separate licensing for NetFlow or sFlow interfaces for the NNM Performance iSPI for Traffic or for LSRs or VRF interfaces for the NNM iSPI for MPLS or for gateways or IP PBX servers for NNM iSPI for IP Telephony.
- If you are using the NNM iSPI for IP Telephony as a feature of NNMi Ultimate, every ten IP Phones managed by the NNM iSPI for IP Telephony counts as one NNMi node for the purposes of licensing. The license node consumption due to these IP Phones is not automatically added to the Consumption value for the NNMi Ultimate license. You can determine the NNMi Ultimate node license count consumed by the NNM iSPI for IP Telephony by running the `nmsiptlicinfo.ovpl` command provided with the NNM iSPI.
- If an NNMi Premium or NNMi Ultimate license key is used, individually licensed NNM iSPIs will no longer be supported. For example, you can't have NNMi Premium and then use NNM iSPI Points to add support for the NNM iSPI Performance for Traffic.
- The NNMi integration with IBM Tivoli Netcool/OMNIbus no longer requires a license.
- (*NNMi Advanced*) In Global Network Management (GNM), nodes remotely managed by the global manager no longer consume a license node count. So, if a node is managed by a regional manager and replicated on the global manager through GNM, it only consumes a single node count (at the regional manager). Nodes that are locally managed by the global manager do consume a license node count.
- (*NNMi Premium*) Non-production licenses are no longer used for High Availability and Application Failover if the product is licensed with NNMi Premium or NNMi Ultimate. See the "Resilience" chapter of the [Deployment Reference](#) for more information.

• Scalability Changes

- Single system scalability limit increases for Very Large tier
 - 30k discovered nodes
 - 60k polled address
 - 120k polled node and physical sensors
- Single system scalability limit increase for Large tier
 - 30k polled address
- Custom Poller limit increases for Very Large tier
 - 200k custom polled objects for "Instance" collection
 - 15 million records daily for "Bulk" collection (where a record can contain values for multiple OIDs from a single SNMP table entry)
- Node Group limit increases

- 12,000 Node Groups
- A hierarchy of 6 Node Groups deep
- Security Configuration limit increases
 - 2000 User Groups
 - 2000 Security Groups

- **Network Virtualization**

- Chassis
 - Chassis are now fully managed objects. A node may have multiple chassis (as in a switch stack case) or a single chassis may have multiple nodes (as in virtual device context case). This separation of the logical (node) and physical (chassis) model allows more complete support for network virtualization.
 - The following chassis views are available:
 - The **Chassis** view in the **Inventory** workspace lists all chassis.
 - The **Chassis** tab on the Node form shows all the chassis associated with a node.
 - The **Chassis** form shows the chassis attributes, such as serial number, and associated Ports, child Cards and Chassis, and Physical Sensors. The **Managed By** attribute indicates the associated Node that manages the Chassis.
 - Node Components have been split into Node Sensors and Physical Sensors.
 - Node Sensors are associated with a Node and have the following types:
 - CPU
 - MEMORY
 - BUFFERS
 - DISK
 - Node Sensors (e.g., CPU) can also be associated with a Physical Component (Card or Chassis).
 - Physical Sensors are associated with a Physical Component (Card or Chassis) and have the following types:
 - FAN
 - POWER
 - TEMPERATURE
 - VOLTAGE
 - BACKPLANE
 - Chassis can participate in redundancy groups. See the **Chassis Redundancy Groups** view in the **Inventory** workspace.
 - Chassis can be nested. For example, this is used for HP C-class blade enclosure support.
 - Chassis polling can be enabled or disabled through Monitoring Configuration. Chassis polling is enabled by default.
 - The following new incidents are generated for the causal analysis associated with chassis:
 - AllCardsDownInChassis
 - CardsDownInChassis
 - ChassisDisabled

- ChassisDown
- Custom Attributes are now supported on Chassis and Cards. These can be viewed and modified on the **Custom Attributes** tab of the Chassis and Card forms. You can also load these custom attributes using with the `nnmloadattributes.ovpl` command (with the `physcomp` type).
- (NNMi Advanced) NIC Teaming and Link Aggregation
 - NNMi discovers and stores server interface aggregations. These types of Link Aggregations on servers are also known as NIC Teaming or NIC Bonding. L2 connections between the server and access switch aggregator interfaces are created with the new L2 Connection Topology Source of IEEE LAG.
 - See the Discovering Link Aggregation section in the [Deployment Reference](#) for tips on configuring servers for more effective discovery of Server-to-Switch Link Aggregations.
 - Link Aggregation Map Visualization
 - Link Aggregations are displayed on maps as a thick line with a superimposed ellipse.
 - Split Link Aggregations (a link aggregation between one device and two or more other devices) are displayed on the map as multiple thick lines that are associated by means of a superimposed ellipse.
- Switch Stacks
 - NNMi now supports improved management of switch stacks (also known as stackables or stacked switches). This includes associating a Node with multiple Chassis and showing the Interswitch Link (ISL) connectivity between the chassis of the switch. The devices participating in the stack switch (e.g., HP Intelligent Resilient Framework (IRF)) are discovered as chassis participating in a Chassis Redundancy Group.
 - Nodes that consists of multiple chassis can be expanded and collapsed on the map. When the node is expanded, the chassis and inter-chassis connections are shown as well as the connections to external nodes or chassis.
 - The following incidents are generated for the causal analysis associated with switch stacks:
 - ChassisDown
 - StackWithNoSlave
 - StackDegraded
- Virtual Device Contexts
 - NNMi supports virtual devices contexts, such as Cisco Virtual Device Contexts (VDC) for Nexus switches, in which multiple logical devices share the same hardware.
 - The administrative contexts, as well as any contexts configured on the device, are discovered as separate nodes.
 - The administrative context hosts the non-administrative contexts. This relationship is navigable on the Node form either via the **Hosted Nodes** tab (for the administrative context) or via the **Hosted On Node** attribute (for non-administrative contexts).
 - The administrative context owns and manages the hardware for the device (chassis, cards, ports, physical sensors)
 - The non-administrative contexts share the hardware with the administrative context.
 - Logical resources (interfaces, nodes, sensors, etc.) are dedicated to the context that reports them.
 - NNMi propagates status of hardware incidents only to the affected contexts/nodes.
- Cisco Nexus

See the [HP Network Node Manager i Software \(NNMi\) Device Support Matrix](#) for details on the enhanced Cisco Nexus support.

- **Scheduled Outage**

- Planned outages for Nodes can be scheduled from the NNMi console. This changes the management mode of the Node to **Out of Service** for the period specified. This feature is available from the **Management Mode → Schedule Node Outage** menu item on Nodes and the **Management Mode → Schedule Group Members Outage** menu item on Nodes Groups.
- The **Scheduled Outages** tab on Node form and the **Scheduled Outages** analysis pane provide access to the list of scheduled outages on a Node.
- The **Scheduled Node Outages** view in the **Management Mode** workspace provides a global list of all scheduled node outages.
- You can record an outage in the past to indicate that the outage was intentional (e.g., a service window that you forgot to schedule an outage for before the fact).
- The new `nnmscheduledoutage.ovpl` command provides the ability to create, list, modify, and delete scheduled outages for nodes. See the `nnmscheduledoutage.ovpl` reference page for more information.
- (*NNM iSPI Performance for Metrics*) The output of the `nnmscheduledoutage.ovpl` command can be provided to the Network Performance Server (NPS) to retroactively adjust reporting data after an outage has occurred (e.g., in the case where the outage was recorded after the fact).

- **Commands**

- Enhanced CLI support makes it easier to automate provisioning and configuration tasks.
- Communication Settings
 - The new `nnmcommunication.ovpl` command provides the ability to create, list, modify, and delete communication settings. See the `nnmcommunication.ovpl` reference page for more information.
 - The administrator can now also change the SNMP configuration information (e.g., management address) for a node directly. This can be done from the `nnmcommunication.ovpl` command (see `listSnmpAgentSettings` and `updateSnmpAgentSettings`).
- Discovery Seeds
 - The `nnmloadseeds.ovpl` command now provides the ability to list seeds and see seed status. See the `nnmloadseeds.ovpl` reference page for more information.
- Node Groups
 - The `nnmnodegroup.ovpl` command now provides the ability to create, list, modify, and delete nodes groups. See the `nnmnodegroup.ovpl` reference page for more information.
- Node Group Map Settings
 - The new `nnmnodegroupmapsettings.ovpl` command provides the ability to create, list, modify, and delete node group map settings. See the `nnmnodegroupmapsettings.ovpl` reference page for more information.
- Scheduled Outage
 - The new `nnmscheduledoutage.ovpl` command provides the ability to create, list, modify, and delete scheduled outages for nodes. See the `nnmscheduledoutage.ovpl` reference page for more information.
- Custom Poller
 - The new `nnmcustompollerconfig.ovpl` command provides the ability to create, list, modify, and delete all aspects of Custom Poller configuration. It also provides the ability to enable and disable Custom Poller. See the `nnmcustompollerconfig.ovpl` reference page for more information.
 - The new `nnmmigrateovpi.ovpl` command provides the ability to generate Custom Poller configuration commands for `nnmcustompollerconfig.ovpl` from OVPI collections. See the `nnmmigrateovpi.ovpl` reference page for more information.

- Unnumbered Interface Connectivity

- The new `nnmunnumberedcfg.ovpl` command can also be used to do Unnumbered Interface Connectivity configuration. See the `nnmunnumberedcfg.ovpl` reference page for more information.

- Connected Neighbor Interfaces

- You can use the new `nnmtopoquery.ovpl` command to list the connected neighbor interfaces for a node. See the `nnmtopoquery.ovpl` reference page for more information.

- **User Interface**

- Dashboard Views

- The new **Dashboard** workspace has Dashboard Views that provide overview information about the health and status of the network. These views include the **Network Overview** view as well as other top-level dashboard views added by installed NNM iSPIs. These views are filtered based on the nodes that the user has access to depending on security configuration.
- Dashboard Views are also available for specific objects (node groups, nodes, interfaces, applications, etc.) via the **Open Dashboard** menu item on the right-click context menu.
 - Object-specific Dashboard Views can be displayed through a URL outside the NNMi console. See **Help → NNMi Documentation Library → Integrate NNMi Elsewhere with URLs** for more information (`cmd=showDashboard`).
- Dashboard Views contain different types of panels, including tables, map views, pie charts, and chart views. For chart views, users can interactively change the style of chart view: line, bar, area, and scatter plot.
- The following NNM Performance iSPIs provide content in Dashboard Views:
 - NNM iSPI Performance for Metrics (Network Overview, Component Performance, Interface Performance, object-specific dashboard views)
 - NNM iSPI Performance for Quality Assurance (Network Overview, QA Performance, object-specific dashboard views)
 - NNM iSPI Performance for Traffic (object-specific dashboard views)
- Dashboard drill-down
 - Some panels in dashboard views provide context-sensitive links to another level of dashboard for various types of objects (Node, Interface, Traffic Application, and QA Probe) if the associated object is available in the NNMi environment. The hyperlinks are shown as underlined text in dashboard table cells and dashboard graph legends. You can click on the link to navigate to a dashboard view specific to that object.
 - As you click through various dashboard drill-down links, the previous view is preserved in the breadcrumb trail area of the NNMi Console.
 - Dashboard table cells and dashboard graph legends that do not show a hyperlink indicate objects that are not available in the NNMi environment. For instance, some Source Nodes and Destination Nodes provided by the NNM iSPI Performance for Traffic may not have been discovered as nodes in NNMi; hence, opening a dashboard for these nodes is not possible.
- A global Time Filter control is available for each dashboard view, so that you can change the time period for which you are viewing the data. Not all panels respond to the time control. See the online help topic *Customize a Dashboard View* for more information.

- Maps

- Maps have an Overview Pane that allows you to pan around the map. You can also pan the map using left-click drag on the map background.
- You can select and move multiple nodes on a map. Use shift left-click drag to select multiple nodes.
- New map icons to display various kinds of connections. See the help topic *About Map Symbols* for

details.

- New icons representing multi-chassis nodes provide the ability to expand and collapse nodes that contain multiple chassis on L2 connection maps. When expanded, these nodes show the connections between the contained chassis as well as external connections. External connections can be either to the enclosing node or to contained chassis. Expanded multi-chassis nodes can be moved and resized. See the help topic *About Map Symbols* for more details.
 - The expanded or collapsed state of these multi-chassis nodes can be saved for node group maps.
 - (*iSPI NET*) This map visualization of multi-chassis nodes can be exported to Visio as part of Visio map export.
- Searching in a map (via the Find icon) will now zoom to the result.

o Node Group Maps

- Users can add Map Annotations to a Node Group Map. A right-click on the map background brings up the **Add a Map Annotation** menu item. You can specify the text and background box for a Map Annotation. Map Annotations can be copied. The size of the background box can be resized to cover a particular area on the map.
 - (*iSPI NET*) Map annotations can be exported to Visio as part of Visio map export.
- Node group maps can be configured to display additional one hop neighbors that are connected to nodes in the Node Group but are not themselves members of the Node Group. See the **Node Group Connectivity** section of the **Node Group Map Settings** form for configuration. Three new tree views appear in the **Topology Maps** workspace:
 - **Node Group Maps** provides a hierarchical view of all saved Node Group Maps (i.e., those Node Groups that have an associated Node Group Map Settings object saved).
 - **Quick Access Maps** provides a list of Node Group Maps ordered by the **Topology Maps Ordering** attribute on the Node Group Map Settings object for the Node Group Map.
 - **All Node Groups** provides a hierarchical view of all Node Group Maps

o Accessibility (See the NNMi online help for details about the enhanced keyboard navigation)

- Menu and sub-menu navigation using Shift-Ctrl and the underlined character (menu mnemonics).
- Improved keyboard navigation of table views.

• Events

- o The NNMi SNMP Trap Receiver is now delivered as a process outside of the NNMi Application Server. This allows SNMP traps to be received for a certain period even while the NNMi Application Server is down (e.g., in a failover situation) for improved availability of trap processing. The SNMP Trap Receiver will start before NNMi on OS startup. See the *NNMi TrapReceiver Process* section in the [Deployment Reference](#) for more information on administration of the new SNMP Trap Receiver process.
- o Incident configuration of SNMP traps now supports wildcards. The "*" character matches all SNMP Object OIDs (e.g. .1.3.6.1.4.* matches both .1.3.6.1.4.1 and .1.3.6.1.4.1.2). With this feature, you only need to create one SNMP Trap Configuration for similar traps.

• SNMP Communication and MIBs

- o The administrator can now change the SNMP configuration information (e.g., management address) for a node directly. This can be done from the NNMi console (via the **SNMP Agent** form) or from the `nnmcommunication.ovpl` command (see `listSnmpAgentSettings` and `updateSnmpAgentSettings`).
- o When using Management Address Selection settings with an interface that has multiple IP addresses, NNMi now selects the management address based on ascending order of IP addresses, beginning with the lowest IP address.
- o MIB Browser

- MIB browser now has a MIB tree to allow MIB navigation.
- MIB browser now supports SNMP set.
- Users can specify the SNMP Version parameter in the MIB Browser.
- There is enhanced `INFO` level logging to help identify various SNMP communication problems.

• Discovery

- Unnumbered Interface Connectivity
 - In previous releases, the creation of L2 Connections based on Unnumbered Interfaces was configured through configuration files - `UnnumberedNodeGroup.conf` and `UnnumberedSubnets.conf`. This configuration is now in the NNMi database. On upgrade to NNMi 10.00, the configuration data from these files will be imported into the NNMi database; after that, these files will no longer be used.
 - Unnumbered Interface configuration can now be done in the UI through **Discovery Configuration** form. See the **Enable Unnumbered Interface Connectivity** attribute and the **Unnumbered Interface Node Groups** tab. Also, now you can specify the Subnet filters per Node Group.
 - The new `nnmunnumberedcfg.ovpl` command can also be used to do Unnumbered Interface Connectivity configuration. See the `nnmunnumberedcfg.ovpl` reference page for more information.
 - (*NNMi Advanced*) L2 Connections derived from Unnumbered Interfaces are now replicated from the regional manager to the global manager in Global Network Management (GNM).
- The administrator can add multiple Discovery Seeds via the UI. See the **Add Multiple Seeds** menu item available in the **Discovery** → **Seeds** view. You can either enter multiple seeds directly or load from a local seeds file.

• State Poller and Monitoring Configuration

- Addresses associated with administratively down interfaces will not be polled. This eliminates status from these addresses contributing to node status.
- Improved logging in `statepoller.trace.log` of details about invalid data returned by polled devices.

• Custom Poller

- A new type of Custom Poller collection called "Bulk" collection has been introduced for use with high-volume collections. The traditional style of Custom Poller collection is now called "Instance" collection. The Bulk type should only be configured for collections that require very high scale. (See the Support Matrix for the supported limits for Custom Polled Objects for Instance collection.) The Bulk type bypasses instance discovery and simply polls all instances of the configured MIB variables for nodes matching the Custom Poller policy that uses a Bulk collection. The features provided by Bulk collections are a subset of those available for Instance collections. You can switch between Bulk and Instance collection if you determine that the other is more appropriate.
- Custom Poller supports polling multiple MIB variables per Custom Poller collection.>
- The new `nnmcustompollerconfig.ovpl` command provides the ability to create, list, modify, and delete all aspects of Custom Poller configuration. It also provides the ability to enable and disable Custom Poller. See the `nnmcustompollerconfig.ovpl` reference page for more information.
 - This command includes MIB Expression configuration and the ability to directly enter an OID for a MIB variable.
- The new `nnmmigrateovpi.ovpl` command provides the ability to generate Custom Poller configuration commands for `nnmcustompollerconfig.ovpl` from OVPI collections. See the `nnmmigrateovpi.ovpl` reference page for more information.
- (*NNM iSPI Performance for Metrics*) String and Integer data types can now be exported to NPS (Network Performance Server) for Custom Poller reports.
- (*NNM iSPI Performance for Metrics*) Custom Poller provides cross-domain extension pack reporting support.

- **Causal Engine**

- The processing of Link Up/Down traps was changed to decrease SNMP traffic during flapping situations. A window was added so that if multiple Link Up/Down traps are received in a 30 second window, only the first trap will trigger SNMP traffic.

- **Security**

- NNMi audits user actions that result in changes to the NNMi database (whether made through the UI or CLI) , as well as certain other user actions (e.g., Configuration Poll of a device). NNMi auditing is enabled by default. See the "NNMi Auditing" section in the [Deployment Reference](#) for more details on the feature and configuration options available.
- A new LDAP `displayNameAttribute` configuration property has been added that can be used to display a more descriptive name in the NNMi Console when using LDAP accounts.
- Some of the encryption algorithms and key lengths used by NNMi for data encryption are now configurable. See the *NNMi Data Encryption* section in the [Deployment Reference](#) for more information.
- NNMi 10.00 uses a stronger hashing algorithm for storing user account passwords in the NNMi database. See the *User Account Passwords* section in the [Deployment Reference](#) for more information.
- NNMi supports 2000 User Groups and 2000 Security Groups

- **Integrations**

- HP Network Automation
 - The NNMi – NA integration has been improved in a distributed environment involving NNMi Global Network Management (GNM) and NA Horizontal Scalability. The integration is now supported in an NNMi GNM / NA Horizontal Scalability environment for all features initiated by NNMi and all features initiated by NA (except for NA to NNMi node synchronization).
 - Different deployment models are possible to associate NNMi regional managers to NA cores. All NNMi regional managers can integrate to the same NA core, or each NNMi regional manager can integrate to a different NA core in the Horizontal Scalability environment to distribute the load.
 - The NNMi global manager can integrate with an NA Horizontal Scalability environment. Cross-launch operations to NA are supported for both locally and remotely managed NNMi nodes on the global manager. No topology synchronization of remotely managed NNMi nodes happens between the NNMi global manager and the NA Horizontal Scalability environment; the needed topology information for these nodes is replicated on the NNMi global manager from the NNMi regional manager(s) that are integrated with the NA Horizontal Scalability environment.
 - In addition to integrating an NNMi GNM environment to an NA Horizontal Scalability environment, you can also integrate a standalone NNMi server to an NA Horizontal Scalability environment or an NNMi GNM environment to a standalone NA core.
 - NNMi does not move nodes out of NA partitions on topology synchronization if **Map NNMi Security Groups to NA Partitions** is disabled in the HP NA Integration Module.
 - NA provides a **Node Policy Compliance** analysis pane in NNMi to show the compliance status of nodes and provide a link to the compliance report.
 - Management address changes in NNMi are propagated to NA through topology synchronization so that NA uses the same address for managing the node.
 - Refined configuration for restricting NNMi user access to NA information in the NNMi analysis pane.
 - See the *HP NHP Network Node Manager i Software – HP Network Automation Integration Guide* for more information.
- HP BSM / HP UCMDB
 - In prior releases, there were separate integration mechanisms for BSM Topology and UCMDB. The previous HP UCMDB integration has been replaced by a new combined **HP BSM/UCMDB Topology**

Integration Module (configured in the **Integration Module Configuration** workspace). This integration supports topology synchronization with both BSM and UCMDDB in a consistent manner. You can use this integration module to integrate with either BSM Topology (RTSM) or UCMDDB (but not both together) at any given time.

- With the same integration mechanism for both BSM Topology and UCMDDB, there are functional improvements to both integrations:
 - VLAN synchronization is now supported by the BSM Topology integration.
 - The Impact Analysis action for Nodes is now supported by the BSM Topology integration.
 - The UCMDDB integration now supports enhanced filtering of the objects that participate in topology synchronization.
 - The UCMDDB integration now has more dynamic topology synchronization with the "push" model supported by the combined integration module
- There are additional options for filtering out synchronized topology objects to reduce the amount of topology data synchronized to the BSM Topology or UCMDDB, including filters on the following objects: subnets, interfaces, unconnected interfaces, addresses, unhosted addresses, cards, ports, connections, VLANs.
- See the *HP Network Node Manager i Software – HP Business Service Management/Universal CMDDB Topology Integration Guide* for more information.
- The following integrations have been added. See [ref="supportmatrix_en.html#integrations">Integrations](#) in the *Support Matrix* for details on supported versions.
 - HP Advanced TeMIP NNM Integration (ATNI)
 - HP Operations Analytics
 - HP Operations Log Intelligence
- The following integrations are no longer supported:
 - HP Network Node Manager version 6.x, 7.x
 - HP ProCurve Manager Plus (PCM Plus)
 - xMatters inc. (formerly AlarmPoint Systems) xMatters lite, xMatters workgroup, xMatters enterprise, and xMatters mobile access
 - Clarus Systems ClarusIPC⁺

• Localization

- If you want to force the locale for all users to be the same regardless of the locale specified by the Web browser (e.g., to display English localized messages for all users), it is possible to do this using a server property. See the *Override the Browser Locale Setting* section in the [Deployment Reference](#) for more information.

• IPv6 (**NNMi Advanced required**)

- IPv6 management is now supported on Windows. See the *Configuring NNMi Advanced for IPv6* section in the [Deployment Reference](#) for more information on IPv6 management.
- IPv6 management is now enabled by default for new installs. In previous releases, IPv6 management was turned off by default and had to be explicitly enabled.

• Global Network Management (**NNMi Advanced required**)

- Custom Attributes are now automatically replicated from the regional manager to the global manager in GNM environments. The list of Custom Attribute names for which replication is done is configured on the **Custom Attribute Replication** tab on the **Global Network Management** form on the global manager. Custom attribute names associated with nodes, interfaces, cards, and chassis are valid. If no Custom Attribute name filter is configured, custom attributes with that name are not replicated.

- The new `nnmgnmattrcfg.ovpl` command provides the ability to create, list, and delete custom attributes to be replicated in a GNM environment. See the `nnmgnmattrcfg.ovpl` reference page for more information.
- Unnumbered Interface Connectivity: L2 Connections derived from Unnumbered Interfaces are now replicated from the regional manager to the global manager in GNM.
- Nodes remotely managed by the global manager no longer consume a license node count. So, if a node is managed by a regional manager and replicated on the global manager through GNM, it only consumes a single node count (at the regional manager). Nodes that are locally managed by the global manager do consume a license node count.
- **Performance Management (NNM iSPI Performance for Metrics required)**
 - You can install a single instance of Network Performance Server (NPS) on multiple servers and assign specific roles to each server. The distributed deployment model enables you to achieve greater performance, which eventually leads to faster processing and report building. For more information, see the *NNM iSPI Performance for Metrics Installation Guide*.
 - Custom Poller supports cross-domain extension pack reporting provided by NPS. You can build cross-domain reports with metrics and topology attributes from NPS extension packs provided by NNM iSPI Performance for Metrics, NNM iSPI Performance for Quality Assurance, NNM iSPI Performance for Traffic, and Custom Poller. For more information, see the *Using the Cross-Domain Extension Pack* topic in NNM iSPI Performance for Metrics Online Help.
 - NNM iSPI Performance for Metrics adds new performance inventory table views to the NNMi console. These new inventory views (**Node Performance Metrics** and **Interface Performance Metrics** in the new **Performance Analysis** workspace) enable you to view the performance metrics collected by NNMi from the nodes and interface on which you have enabled performance monitoring. For more information, see the *Performance Analysis with Additional Views* topic in NNM iSPI Performance for Metrics Online Help.
 - The Performance Graphing console (available from the **HP NNM iSPI Performance** → **Performance Troubleshooting** menu item on Nodes and Interfaces) allows you to save favorites.
 - Descriptions of each of the performance metrics are available in the online help. To view a metric description, right-click a metric in the list of metrics in the Report Options panel on a report, and then click **Show Description**.
 - See the Release Notes for each of the NNM Performance iSPIs for What's New for each NNM iSPI:
 - NNM iSPI Performance for Metrics
 - NNM iSPI Performance for Quality Assurance
 - NNM iSPI Performance for Traffic

NNMi 9.23

- **Security**
 - PKI User Authentication
 - NNMi now supports smart card logons including Common Access Card (CAC) and Personal Identity Verification (PIV) cards. See the *Configuring NNMi to Support Public Key Infrastructure User Authentication* chapter in the [9.23 Deployment Reference](#) for more information.
 - You can configure NNMi to restrict certificates used for logons. See the *Configuring NNMi to Support Public Key Infrastructure User Authentication* chapter in the [9.23 Deployment Reference](#) for more information.
 - You can configure NNMi to use the following certificate validation methods for Public Key Infrastructure (PKI) user authentication:
 - Certificate Revocation Lists (CRLs)
 - Online Certificate Status Protocol (OCSP)

See the *Configuring NNMi to Support Public Key Infrastructure User Authentication* chapter in the [9.23 Deployment Reference](#) for more information.

- NNMi now supports the use of subjectAlternativeName (SAN) for principal mapping in PKI user authentication. See the *Configuring NNMi to Support Public Key Infrastructure User Authentication* chapter in the [9.23 Deployment Reference](#) for more information.
- You can configure NNMi to use Access Control Lists (ACLs) to enable non-root users to run Command Line Interface (CLI) commands. This is useful where CAC is enabled and password credentials are not available for running CLIs. See the *Configuring NNMi to Support Public Key Infrastructure User Authentication* chapter in the [9.23 Deployment Reference](#) for more information.

• Device Extensions

- NNMi now uses NETCONF (RFC 4741 and 4742) communication with some device vendors and models (for example, Juniper Networks QFabric) to supplement the management information collected by SNMP. See the [9.23 Deployment Reference](#) for additional information on NETCONF and instructions to configure the requisite credentials in NNMi. See the *HP Network Node Manager i Software System and Device Support Matrix* "Known Limitations" section for supported device vendors and models that use NETCONF, plus vendor-specific prerequisites to allow that usage.

• SNMP Communication and MIBs

- NNMi now supports the discovery of its EngineID using GetBulk and GetNext operations, in addition to SNMP-GET operations (previously supported). See the *SNMP Communication and MIBs* release note in the **NNMi 9.21** section of this document for more information.

• Events

- NNMi now provides Custom Incident Attributes (CIAs) in the order of the original trap varbinds for traps received after applying the patch. You can observe the new CIA ordering in the NNMi console as well the Northbound Interface and NNMi SDK.

• Integrations

- HP Network Automation (NA)
 - You can configure the integration between NNMi and NA using two new options:
 - NNMi-NA Integration Level
The default setting enables full integration functionality. The other settings limit integration functionality for multi-tenancy environments and for architectures in which two or more NNMi regional managers connect to one NA core.
 - Out Of Service Completion Delay
This delay provides time for a device to recover after NA completes a task that placed that device out of service

See the *HP Network Node Manager i Software—HP Network Automation Integration Guide* and the *NA User Guide* (Administrative Settings—3rd Party Integrations page) for more information.

NNMi 9.22

• Integrations

- HP Network Node Manager i - HP Intelligent Management Center
When HP Networking devices are installed in your network, you can combine either ANM or HP NNMi with HP Intelligent Management Center (HP IMC) using the HP NNMi - HP IMC integration. The result is a better solution for managing your enterprise network. HP IMC adds change, configuration, and compliance features along with add-on modules for other device management needs.

NNMi 9.21

User Interface

- NNMi permits User Accounts assigned to the NNMi Operator Level 2 User Group to run Status Poll and Configuration Poll on nodes to which they have access. See the *Maintaining NNMi* chapter in the [9.21 Deployment Reference](#) for more information.
- NNMi permits User Accounts assigned to the NNMi Operator Level 2 User Group to edit maps and node groups. See the *Maintaining NNMi* chapter in the [9.21 Deployment Reference](#) for more information.

Events

- The trap server now starts sooner and begins capturing traps earlier after restarting NNMi.
- The Incidents View now includes Tenant and NNMi Management Server Columns.
- Remote site unreachable incidents (Management Incident Configuration IslandGroupDown) have been updated to include custom incident attributes (CIA) `cia.incidentDurationMs`, `cia.timeIncidentDetectedMs`, and `cia.timeIncidentResolvedMs`. See the help topic *Custom Incident Attributes Provided by NNMi* for a description of these CIAs.

SNMP Communication and MIBs

- NNMi now supports SNMPv3 engine-ID discovery by devices that will use an engine-ID to send SNMPv3 informs. This feature works as follows:
 - a. A device sends an empty SNMP-GET request to NNMi's configured trap port (typically port 162).
 - b. NNMi generates and sends an SNMPv3 report PDU response to the device. NNMi's response contains NNMi's engine-ID.

Discovery

- NNMi has been enhanced so it no longer shows a "Subnet connection" in a subnet where there are two or more MPLS Provider Edge (PE) interfaces involved.
- You can configure NNMi to not consider some firewall and loadbalancer devices as duplicates. Many firewall and loadbalancer devices have duplicated IP addresses, duplicated layer 2 addresses, or both. This is especially true when the device is a virtual instance hosted on a physical device. NNMi often considers such devices to be duplicates of each other when they are not really duplicates. NNMi has a new configuration file in which you can list the `sysObjectId` values of these nodes. Doing so tells NNMi not to consider such nodes to be duplicates when it finds overlapping IP addresses, layer 2 addresses, or both. See the *macdedupexceptions.txt.4* reference page, or the UNIX manpage, for more information.

State Poller and Monitoring Configuration

- One common way to test network latency is to adjust the ICMP polling frequency and ICMP echo request packet data payload size for a management address being managed by NNMi. NNMi permits you to experiment with different packet sizes to measure the network latency. See the *Maintaining NNMi* chapter in the [9.21 Deployment Reference](#) for more information.

Causal Engine

- A new tab, called "Causal Engine", has been added to System Information window. This tab will display key statistic for the Causal Engine including how far behind it is processing state messages.
- Traps sent by a proxy SNMP gateway might not show the original trap address when using NNMi's default configuration. An administrator can configure NNMi to determine the original trap address. See the *Maintaining NNMi* chapter in the [9.21 Deployment Reference](#) for more information.

Security

- You can configure NNMi (using PKI) to map certificates to NNMi user accounts. See the *Configuring NNMi to Support Public Key Infrastructure Authentication* chapter in the [9.21 Deployment Reference](#) for more information.
- You can configure cipher suites in `$NnmDataDir/shared/nnm/conf/props/nms-jboss.properties` (Windows) or `%NnmDataDir%\shared\nnm\conf\props\nms-jboss.properties` (UNIX). See the *Configuring NNMi to use only TLSv1 Ciphers* section in the [9.21 Deployment Reference](#) for more information.

- **Integrations**

- You can configure HP NNMi to permit NNMi incidents to close automatically after the corresponding alert is acknowledged in HP BSM Operations Management.
- **SiteScope System Metrics**
The SiteScope System Metrics Integration Module now supports the use of the SiteScope 11.20 Dynamic Disk Space monitor. Metrics collected by this SiteScope monitor and sent to NNMi according to SiteScope Data Integration preferences will now be processed correctly in NNMi and made available in NPS just as they had with the older Disk Space Monitor.
- **ArcSight**
 - Out-of-the-box Support for ProCurve syslog messages
 - Out-of-the-box support for H3C syslog messages

- **Commands**

- The `nnmsetiospeed.ovpl` script permits the user to change the input or output speed on an interface either individually or in batch mode. See the `nnmsetiospeed.ovpl` reference page, or the UNIX manpage, for more information.
- The `nnmloadinterfacegroups.ovpl` script provides a command line interface for creating or replacing interface group configurations. See the `nnmloadinterfacegroups.ovpl` reference page, or the UNIX manpage, for more information.

Documentation Updates

The complete documentation set is available on the HP Product Manuals web site at h20230.www2.hp.com/selfsolve/manuals. Use your HP Passport account to access this site, or register a new HP Passport identifier. Choose the "network node manager" product, "10.00" product version, and then choose your operating system. From the search results, open the Documentation List and click the link for the appropriate version of a document.

NOTE: To view files in PDF format (.pdf), Adobe Reader must be installed on your system. To download Adobe Reader, visit the Adobe web site at www.adobe.com.

You can run the NNMi help system independently from the NNMi console. See *Help for Administrators: Use NNMi Help Anywhere, Anytime* in the NNMi help.

Deployment Reference

The HP Network Node Manager i Software Deployment Reference is a web-only document providing advanced deployment, configuration, and maintenance. To obtain a copy of the most current version, go to h20230.www2.hp.com/selfsolve/manuals.

Upgrade Reference

The HP Network Node Manager i Software Upgrade Reference is a web-only document providing information for upgrading from earlier releases of NNMi and upgrading from NNM 6.x or NNM 7.x to NNMi. To obtain a copy of the most current version, go to h20230.www2.hp.com/selfsolve/manuals.

Integration Guides

The integration guides for integrations with other products are available as individual web-only documents. To obtain a copy of the most current version of the integration guide for the particular integration you are interested in, go to h20230.www2.hp.com/selfsolve/manuals. See the [HP Network Node Manager i Software System and Device Support Matrix](#) for the list of available integrations.

Reference Pages

Reference Pages are available in the NNMi console through the Help → NNMi Documentation Library

→ **Reference Pages** menu item. They are also available on UNIX systems through the *man(1)* command. To view NNMi manpages, set MANPATH to /opt/OV/man before running the *man* command.

Documentation Errata

No documentation errata.

Installation Guide and Support Matrix

To obtain an electronic copy of the most current version of the *NNMi 10.00 Interactive Installation Guide*, go to <http://h20230.www2.hp.com/selfsolve/manuals>.

Installation requirements, as well as instructions for installing NNMi, are documented in an interactive version of the *NNMi 10.00 Interactive Installation Guide*. The *NNMi 10.00 Interactive Installation Guide* is included on the NNMi installation media as `nnmi_interactive_installation_en.zip` or `nnmi_interactive_installation_en.jar` files. For instructions explaining how to extract and view the *NNMi 10.00 Interactive Installation Guide*, see the `nnmi_interactive_installation_en_README.txt` file located at the root of the NNMi installation media.

For a list of supported hardware platforms, operating systems, and databases, see the [HP Network Node Manager i Software System and Device Support Matrix](#).

For a list of prerequisite packages or patches, see the **Installation Prerequisites** in the Operating System section of the [HP NHP Network Node Manager i Software System and Device Support Matrix](#).

Licensing

NNMi installs with an instant-on 60-day/250-node license. This license also temporarily enables the [NNMi Ultimate](#) features for the 60-day trial period.

To check the validity of your NNMi licenses, in the NNMi console click **Help** → **System Information**, and then click **View Licensing Information**. Compare the **Capacity** count with the **Consumption** count to see how much unused capacity is remaining.

- **NOTE:** If you are using the NNM iSPI for IP Telephony as a feature of NNMi Ultimate, every ten IP Phones managed by the NNM iSPI for IP Telephony counts as one NNMi node for the purposes of licensing. The license node consumption due to these IP Phones is not automatically added to the Consumption value for the NNMi Ultimate license. You can determine the NNMi Ultimate node license count consumed by the NNM iSPI for IP Telephony by running the `nmsiptlicinfo.ovpl` command provided with the NNM iSPI.

NOTE: In these Release Notes and the online help, any feature marked "NNMi Advanced" also applies to NNMi Premium and NNMi Ultimate. Likewise, anything marked as "NNMi Premium" also applies to NNMi Ultimate. Each of these is a superset of the preceding one in the following order: NNMi, NNMi Advanced, NNMi Premium, and NNMi Ultimate. Any feature marked "NNM iSPI Performance for Metrics" also applies to NNMi Premium. Some items marked "iSPI NET" apply to NNMi Premium (Trap Analytics and Visio Map Export); all items marked "iSPI NET" apply to NNMi Ultimate.

For information about installing and managing licenses, see the *NNMi 10.00 Interactive Installation Guide*.

HP Network Node Manager i Advanced Software Features

An NNMi Advanced license enables the following features:

- All features licensed by the NNMi license.
- Global Network Management. (The global manager requires an NNMi Advanced license; regional managers do not.)
- IPv6 Discovery and Monitoring
- Monitoring of router redundancy groups (HSRP, VRRP).
- Support for port aggregation protocols (for example, PaGP) with results displayed in the **Link Aggregation** tab of the Interface form.

- HP Route Analytics Management Software (RAMS) integration for RAMS traps and path information from RAMS, enhancing the path displayed in Path View.
- Extension of path visualization (for example, Equal Cost Multi-Path). When multiple paths are possible, the user interface provides for selection of specific paths for opening an NNM iSPI Performance for Metrics path health report.
- MPLS WAN Clouds (RAMS) view from the Inventory workspace, including map views of the MPLS WAN cloud; see *Using Route Analytics Management Software (RAMS) with NNMi Advanced* in the NNMi help.
- VMware ESX and Virtual Machine Capability Discovery.

HP Network Node Manager i Premium Software Features

An NNMi Premium license enables the following features:

- All [NNMi Advanced](#) features.
- The SNMP Trap Analytics feature of [iSPI NET](#).
- The Visio Export feature of [iSPI NET](#).
- The NNMi Developer Toolkit. See the SDK documentation and examples located in the %NnmInstallDir%\doc folder (Windows) or \$NnmInstallDir/doc directory (Linux).
- HP Network Node Manager iSPI Performance for Metrics. This software requires a separate installation. See the NNM iSPI Performance for Metrics documentation for details.
- HP Network Node Manager iSPI Performance for Quality Assurance. This software requires a separate installation. See the NNM iSPI Performance for Quality Assurance documentation for details.
- See the help topic *Purchase HP Network Node Manager i Smart Plug-ins and More* for more information.

HP Network Node Manager i Ultimate Software Features

An NNMi Ultimate license enables the following features:

- All [NNMi Premium](#) features.
- The Diagnostics feature of [iSPI NET](#). This feature requires a separate installation of an iSPI NET Diagnostics Server or an HP Operations Orchestration server. See the HP *NNM iSPI Network Engineering Toolset Planning and Installation Guide* and the *HP Network Node Manager iSPI Network Engineering Toolset Diagnostics Server Release Notes* for more information.
- HP Network Node Manager iSPI Performance for Traffic. This software requires a separate installation. See the NNM iSPI Performance for Traffic documentation for details.
- HP Network Node Manager iSPI for IP Multicast. This software requires a separate installation. See the NNM iSPI for IP Multicast documentation for details.
- HP Network Node Manager iSPI for IP Telephony. This software requires a separate installation. See the NNM iSPI for IP Telephony documentation for details.
- HP Network Node Manager iSPI for MPLS. This software requires a separate installation. See the NNM iSPI for IP Multicast documentation for details.
- See the help topic *Purchase HP Network Node Manager i Smart Plug-ins and More* for more information.

HP Network Node Manager iSPI Network Engineering Toolset Software Features

An HP Network Node Manager iSPI Network Engineering Toolset Software (NNM iSPI NET) license enables the following features:

- NNM iSPI NET Diagnostics - device diagnostics collection and display.
 - When an incident changes lifecycle state (such as Registered or Closed), NNMi can run diagnostics (flows). The diagnostics results are visible on the **Diagnostics** tab of an Incident form. A diagnostic flow is an SSH

or Telnet session that logs on to a network device and performs commands to extract configuration or troubleshooting information. This automation reduces the time a network engineer spends gathering troubleshooting and diagnostic data.

- Flows can be run manually by selecting a supported node and clicking **Actions** → **Run Diagnostics** to store baseline data about that node on the **Diagnostics** tab of the Node form.
- For more information, see the Incident Configuration form and the Diagnostics tabs on the Node and Incident forms.
- Command line tool to add and manage HP Operations Orchestration flow definitions. See the `nnmooflow.ovpl` Reference Page, or the UNIX manpage, for more information.
- Requires installation of the NNM iSPI NET embedded diagnostics server or a previously installed HP Operations Orchestration Central server.
- NNM iSPI NET SNMP Trap Analytics - trap data is logged in a user consumable form.
 - Measures the rate of incoming traps per device or SNMP Object Identifier (OID).
 - **Actions** → **Trap Analytics** opens the report for analysis of the incoming traps since NNMi was started, or in the last time period. From these reports, you can start graphs of the incoming rates of traps by SNMP OID or source node.
- Map view export to Microsoft Visio
 - **Tools** → **Visio Export** → **Current Map** exports the map in focus to a Visio file.
 - **Tools** → **Visio Export** → **Saved Node Group Maps** exports the Node Group maps marked for export to a Visio file.
- For more information about NNM iSPI NET, see the NNMi help and the *HP NNM iSPI Network Engineering Toolset Planning and Installation Guide*, available at <http://h20230.www2.hp.com/selfsolve/manuals>.

Known Problems, Limitations, and Workarounds

- If NNMi services running inside ovjboss start up slowly, the nnmaction process might stop shortly after it starts up. This is because nnmaction depends on certain event services in the NNMi ovjboss server, which continue to start up after ovjboss has completed its startup. The event services must be fully initialized for nnmaction to function normally. After nnmaction starts up, it monitors the event services, and if the event services are not fully initialized after a certain period of time, the nnmaction process exits. To resolve this issue, run the following from the command line to restart the nnmaction process: `ovstart -c nnmaction`
- The standby node in an NNMi cluster can remain stuck in the standby state while it is trying to receive transaction logs from the active node. This can occur when the active node has recently generated a new database backup that took a long time to create, send to standby, or both. The standby has already acknowledged receipt of database transactions (through the continuous database updates sent through a separate socket), and the corresponding transaction log files, which are pending, have already been deleted from disk. The workaround is to run the `nnmcluster -dbsync` operation.
- The NNMi console might time out and report an error if you try to delete a node having a large number of interfaces. Before deleting the node, you must first unmanage the node regardless of method for deletion. After you successfully unmanage the node, delete the node using the NNMi console. Alternately, use the `nnmnodedelete.ovpl` script to delete nodes having a large number of interfaces. For more information, see the `nnmnodedelete.ovpl` reference page or UNIX manpage.
- When creating filters for NNMi, pay special attention to the values returned by the SNMP Agent before applying your changes. For example, some SNMP agents might return illegal characters for filterable attributes (such as returning null bytes for the `ifDescr` value). Generally, these illegal characters cause the filter to fail. Filtering on null characters or non-Unicode characters might not work, as NNMi interprets each of these characters as the Unicode Replacement Character (such as ? at Unicode codepoint U+FFFD). One way to correct this is to configure NNMi for the proper source character encoding to expect for SNMP Agents in the environment. The SNMP OCTET STRING data is interpreted based on any character encodings defined by the `com.hp.nnm.sourceEncoding` property in the `nms-jboss.properties` file. In the above example, a property value of `"com.hp.nnm.sourceEncoding=UTF-8, Windows-1252"` may work to properly interpret the string data. Different

environments may require different values for the source encoding, depending on the character encoding used by the SNMP Agents. For more information, see "Configuring Character Set Encoding Settings for NNMi" in the [Deployment Reference](#).

- Large table views sorted on certain attributes may contain duplicate rows after paging.
- If an SNMP agent for a node is unreliable, the node component data discovered might differ between NNMi discoveries. For example, in rare cases, the SNMP agent might respond using data from the vendor-specific MIB during initial discovery and then use the standard MIB for a subsequent query. When a Node Component is re-discovered due to unreliable SNMP data, note the following:
 - Previous performance data for that Node Component might be lost.
 - If SNMP Agent information that is used to identify the Node Component changes, it can appear as if a Node Component was removed or added.
- Default, Node Specific, or both SNMP community strings must be set up in SNMP Configuration (**Configuration** → **Communication Configuration**) *before* running the `nnmloadseeds.ovpl` script or adding seeds to the discovery configuration table to initiate discovery. If community strings are not set up in NNMi, initial discovery might classify a node as "Non SNMP". In this case, correct the SNMP Configuration, and then rerun discovery for the node with the `nnmconfigpoll.ovpl` script or **Actions** → **Polling** → **Configuration Poll**. For more information, see the `nnmloadseeds.ovpl` and `nnmconfigpoll.ovpl` Reference Pages, or the UNIX manpages.
- In NNMi map views, the web browser's zoom controls (CTRL++ (plus) and CTRL-- (minus)) do not work properly. These keystrokes zoom the HTML text and not the icons themselves. Instead, use the map's keyboard accelerators (plus (+), minus (-), and equals (=) keys) or toolbar buttons to zoom.

- Redirection of .ovpl scripts on Windows using the implicit file association might not generate an output file. For example:

```
nnmstatuspoll.ovpl -node mynode > out.log
```

If you are not able to view the output file, run the command explicitly from Perl in a command window:

```
"%NnmInstallDir%\nonOV\perl\bin\perl.exe" "%NnmInstallDir%\bin\nnmstatuspoll.ovpl" -node mynode > out.log
```

A second option is to fix your Windows Registry:

1. Back up the Windows Registry.
 2. Start the Windows Registry Editor (regedit.exe).
 3. Locate and then click the following key in the registry:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
 4. On the Edit menu, click Add Value, and then add the following registry value:
 - a. Value name: InheritConsoleHandles
 - b. Data type: REG_DWORD
 - c. Radix: Decimal
 - d. Value data: 1
 5. Quit the Windows Registry Editor
- If devices do not respond with required SNMP MIB values, NNMi discovery might not find nodes, Layer 2 connections, or VLANs. See [Supported Network Devices](#) in the *HP Network Node Manager i Software System and Device Support Matrix*.
 - If the NNMi management server has a firewall blocking incoming HTTP requests, you cannot start the NNMi console remotely.

The Linux firewall is enabled by default. You can either disable the firewall completely, or more specifically add other ports:

```
161:udp, 162:udp, <HTTPPORT>:tcp
```

where <HTTPPORT> is the NNMi web server port as defined by the `jboss.http.port` value in the `/var/opt/OV/conf/nm/props/nms-local.properties` file.

- If using LDAP to access your environment's directory services, you must log on to the NNMi console using the

same case sensitivity of users as reported by the directory service. When the case sensitivity differs between what is returned from the directory service and the name with which you logged on, you cannot assign incidents to your user name and the My Incidents view does not work. Use **Actions > Assign Incidents** to view the list of valid user names, including the required case for each.

- NNMi application failover on Windows systems:
 - Application failover on the Windows platform can have some intermittent issues with Symantec Endpoint Protection (SEP) software that affect NNMi cluster operations. When the Standby node is attempting to receive the database backup, this operation sometimes fails because SEP is not releasing a file lock in a timely manner. The database file is automatically retransmitted on any failure, and this problem eventually clears itself.
 - When application failover is configured for Windows, system reboots or other issues might cause the psql command to fail, generating dialog boxes to the Windows desktop and the event viewer. These dialog boxes do not affect operation and can be ignored.
- When you perform an online backup of NNM, the database password is included in the backup. If you change the database password using the `nnmchangeembddbpassword.ovpl` script after a backup is completed; then restore NNMi from the backup that includes the outdated password, the NNMi database fails to start.

To restore your NNMi database, use a database backup that includes the new password.

- Attempting to delete a Custom Node Collection or Custom Poller Policy with a large number of Custom Polled Instances can fail. When the delete is attempted, the NNMi console shows the "busy circle" icon for a few minutes, and then an error dialog indicates a batch update failure. This case is more likely to happen when collecting data from a MIB table where there are multiple instances being polled for a given node. It is highly recommended that you filter only the instances that you want to poll to help minimize this issue and the load on NNMi.

A workaround is possible using the following sequence:

- a. If you are not able to delete the Custom Node Collection, try to delete each Custom Poller Policy on the Custom Node Collection individually.
For each Custom Poller Policy that fails to delete:
 - a. If the policy has a MIB Filter value, change its value to a pattern that does not match any MIB filter variable value. Check the Custom Node Collection table to ensure that all nodes for that Custom Poller Policy have completed discovery. All Custom Polled Instances for this Custom Poller Policy should be removed.
 - b. If the Custom Poller Policy does not have a MIB filter value, change the Custom Poller Policy's Active State to **Inactive**. This action should cause all Custom Polled Instances associated with the Custom Poller Policy to be deleted. If it does not, edit the associated Node Group to remove nodes from the group. This causes NNMi to delete the associated Custom Node Collections and their Custom Polled Instances.
 - b. It should now be possible to delete the policy successfully.
 - c. When all Custom Poller Policies for a Custom Node Collection are deleted, delete the Custom Node Collection.
- If you are browsing between multiple NNMi installations, browsing to a second NNMi installation logs you off from the previous NNMi installation when you return to the first system. To fix this problem, do the following:
 1. Open the following file:
 - a. **Windows:** `%NnmDataDir%\shared\nnm\conf\props\nms-ui.properties`
 - b. **UNIX:** `/var/opt/OV/shared/nnm/conf/props/nms-ui.properties`

Edit the file in one of the following ways:

- a. Disable Single Sign-On by setting `com.hp.nms.ui.sso.isEnabled="false"`.
- b. Configure Single Sign-On by ensuring that the `com.hp.nms.ui.sso.initString` and `domain` parameters are the same across all systems. Both systems must also have clocks that are in sync, and the

domains of each system's FQDN must match and be configured in `com.hp.nms.ui.sso.protectedDomains` of `nms-ui.properties`.

2. Run `nnmsso.ovpl -reload`.

- (Windows only) Anti-virus and backup software can interfere with NNMi operation if this software locks files while NNMi is running. Any application that locks files should be configured to exclude the following NNMi database directory on Windows Server 2008: `C:\ProgramData\HP\HP BTO Software\databases`.
- The `Query Password` field of a RAMS configuration is only valid when imported into the same NNMi installation on the same system. If imported into a different system, the `Query Password` must be re-entered.
- Incorrect browser proxy settings with a non-DNS hostname can prevent a user from logging on to the NNMi console. For example, if the NNMi server's FQDN is not resolvable in DNS, and the user wants to use an FQDN on the box, a user could add an entry such as `192.168.0.100 myhost.example.com` to local system hosts file. This hostname is not resolvable by the DNS server. If the browser is configured with HTTP proxy, the browser ignores the hosts file for NNMi hostname resolution, and uses the proxy for NNMi hostname resolution. Because DNS cannot resolve the NNMi hostname, the NNMi console logon fails.

To resolve this problem, the user should either disable the proxy setting or add exceptions to the browser proxy settings. To add exceptions to the browser proxy settings, do the following:

- Internet Explorer:
 1. On the **Internet Options** → **Connections** tab, click **LAN Settings**.
 2. If the **Proxy Server** is configured, click **Advanced**, and then add the non-DNS NNMi hostname into the **Proxy Settings Exceptions** list.
- Firefox:
 1. Click **Tools** → **Options**.
 2. In the **Options** dialog box, select the **Advanced** pane.
 3. On the **Network** tab, under Connection, click **Settings**. If a proxy is configured, add the non-DNS NNMi hostname into the **No Proxy for** list.
- Nodes with down Interfaces might have a Status of **No Status** under the following conditions:
 - If the active IP Address that responds to SNMP communication is on a down Interface, it is excluded from the list of candidate Management IP Addresses.
 - If the hint or seed address that was used did respond to SNMP, the result is a node with valid system information and Device Profile, but no SNMP Agent.

To resolve the problem use the **Configuration Poll** option from the **Actions** menu.

- When using the **Actions** → **Custom Attributes** menu items from a Node or Interface form, saving the form can overwrite Custom Attributes that have been added. The workaround is to close the form instead of using Save and Close or use the **Actions** → **Custom Attributes** menu items only from a table view.
- (NNM Performance iSPIs) It is important for you to synchronize the NNMi management server clock and the NPS server clock. This ensures that the analysis panes that retrieve data from the NPS server yield accurate results. If you experience blank analysis panes, check that your clocks are synchronized between the two servers. NPS (Network Performance Server) is the database server installed with any of the NNM Performance iSPI products.
- NNMi permits passing UTF-8 data as arguments to Jython action scripts. NNMi now requires Jython action script source code to be UTF-8 aware. For older Jython scripts to work successfully with NNMi 9.23 or newer, they must meet the following criteria:
 - The PEP-0263 standard is now required to use UTF-8 in Jython action scripts.
 - Jython 2.5 requires users to follow the PEP-0263 standard when writing scripts ([See http://www.python.org/dev/peps/pep-0263](http://www.python.org/dev/peps/pep-0263)).
 - The only supported encodings from PEP-0263 are : ASCII and UTF-8. ASCII is taken as the default if the

encoding is not specified.

- Script writers must have all their Jython scripts follow the same PEP-0263 encoding (UTF-8 or ASCII). Using a combination of UTF-8 and ASCII is not supported.

Customers upgrading from NNMi 9.0 and older that use an earlier version of Jython (that do not meet the above criteria) must update their Jython scripts to be compliant to the above and other relevant standards followed by Jython 2.5.2.

Potential Installation Issues

- See installation prerequisites in the [NNMi 10.00 Interactive Installation Guide](#) and [HP Network Node Manager i Software System and Device Support Matrix](#) for complete instructions.
- If you are installing a localized version of the product, see the [Non-English Locale Known Problems](#) section for additional information.
- In addition to the web server port, the NNMi management server uses several ports for process communication as documented in the *NNMi 10.00 and Well-Known Ports* appendix of the [Deployment Reference](#). Before installing NNMi, verify that these ports are not in use.
- Installation on Windows using Terminal Services:
NNMi installation only works if you are on the machine console. If you use remote logon technology, such as Remote Desktop Connection, verify that you are accessing the Windows console and not a secondary connection.
- Some Linux installations might have a version of Postgres installed and running by default. In this case, disable the default Postgres instance before installing NNMi. NNMi does not support multiple instances of Postgres on the same server. The easiest way to determine whether an existing Postgres instance running is by using the `ps -ef | grep postgres` command. Postgres can be disabled with `chkconfig postgresql off`.
- NNMi supports single sign-on (for use with NNM iSPIs and some integrated products).
 - This technology requires that the NNMi management server be accessed with the official fully-qualified domain name (FQDN). The official FQDN is the hostname used to enable single sign-on between NNMi and NNM iSPIs. The FQDN must be a resolvable DNS name.
 - If the domain name of the installation system is a short domain such as "mycompany" without any dot, you must change a configuration file to prevent automatic sign out from the NNMi console.

For more information, see the *Using Single Sign-On with NNMi* chapter of the [Deployment Reference](#).

- (Windows only) Silent install on non-English locale Windows systems:
For silent installation on a target system, the *NNMi 10.00 Interactive Installation Guide* instructs the user to run an installation using the user interface on another system. This approach creates a `%TEMP%\HPOvInstaller\NNM\ovinstallparams_YYYYMMDD.ini` file. This file can be copied to another system as `%TEMP%\ovinstallparams.ini` and then installed using the silent installer.
Use Wordpad (or some other editor) instead of Notepad to modify the `ovinstallparams.ini` file.
If this `.ini` file is generated on a non-English locale machine (for example: Japanese or Chinese), and if you edit this file in the Notepad editor, Notepad adds 3 bytes at the start of the file to specify the encoding as UTF-8. These 3 bytes cause the subsequent silent installation process to fail.
- (Windows only) Do not use non-English characters in the path name of the installation directory.
- If you plan to upgrade an earlier version of NNMi 9.1x or NNMi 9.2x that is running in an NNMi application failover cluster, see the [Upgrade Reference](#) for detailed instructions on this procedure.
- If you plan to upgrade an earlier version of NNMi 9.1x or NNMi 9.2x that is running in a High Availability environment, see the [Upgrade Reference](#) for detailed instructions on this procedure.
- If you have NNM iSPIs installed on the NNMi management server, and plan to remove NNMi and NNM iSPIs, uninstall the NNM iSPIs before uninstalling NNMi. Otherwise, when you reinstall NNMi, the NNM iSPIs no longer work until you reinstall each one.
Note: NNM iSPI Performance for Metrics is an exception to the above uninstall requirement.
- NNMi creates a self-signed certificate during installation. This certificate enables HTTPS access to the NNMi console without additional configuration. Because it is a self-signed certificate, your browser does not

automatically trust it, resulting in security prompts when using the NNMi console.

- With Firefox, you can choose to permanently trust the certificate, and you will not be prompted again.
- With Internet Explorer, you will be prompted multiple times. There are two ways to prevent these prompts:
 - Import the self-signed certificate into each user's browser.
 - Replace the self-signed certificate with a CA-signed certificate that all users' browsers are configured to trust. For more information, see the *Working with Certificates for NNMi* chapter of the [Deployment Reference](#).
- The "Reinstall from media" (Linux) or "Repair" (Windows) option available through the uninstaller or Control Panel does not work and is not supported.
- (Linux only) Setting the `/opt` or `/var/opt` directory with inherited permissions might cause problems if the inherited permissions are too restrictive.

The inherited permissions are created by enabling the set-groupid bit on the directory itself, for example the "2" in the `chmod 2755` command.

An example of an inherited permission that is too restrictive is "2750". This permission strips world read-access. Some NNMi processes run as non-root user (for example the database and the action process). These processes need read access to files below `/opt/OV` and `/var/opt/OV`. If the inherited directory permission strips world read, these processes fail.
- (Linux only) If the NNMi public key import or a product install fails with the following error:

```
rpmdb: Lock table is out of available locker entries
rpmdb: Unknown locker ID: 56cd
error: db4 error(22) from db->close: Invalid argument
error: cannot open Packages index using db3 - Cannot allocate memory (12)
error: cannot open Packages database in /var/lib/rpm
error: pk.pub: import failed.
```

Complete the following steps:

- Run the following command to save a copy of the rpm database: **`tar cvzf /var/tmp/rpmdbtar.gz /var/lib/rpm`**
- `rm /var/lib/rpm/__.db.00*`**
- `rpm --rebuilddb`**

To validate that you corrected the issue, run the following commands:

- `rpm -q -a`**
- `rpm --import pk.pub`**

If the results of running the **`rpm -q -a`** command lists all packages without error, you can remove the `/var/tmp/rpmdbtar.gz` file. If not, restore the rpm database from the `rpmdbtar.gz` file.

Internet Explorer Browser Known Problems

- The telnet:// and ssh:// URLs are not enabled by default with Internet Explorer. See the *Configuring the Telnet and SSH Protocols for Use by NNMi* chapter in the [Deployment Reference](#) for instructions on how to enable the telnet and ssh protocols, which requires a registry change on each web browser client. Without this registry edit, selecting the **Actions → Node Access → Telnet... (from client)** or **Secure Shell... (from client)** menu item results in a "The webpage cannot be displayed" message.
- When using Internet Explorer, browser settings determine whether the name of an NNMi view or form displays in the title bar. To configure Internet Explorer to display view and form titles:
 1. In Internet Explorer browser, click **Tools**, and then click **Internet Options**.
 2. Navigate to the **Security** tab, **Trusted Sites**, **Custom Level**, **Miscellaneous** section.
 3. Disable the **Allow websites to open windows without address or status bars** attribute.
- Internet Explorer tracks long running JavaScript operations, and displays a "This page contains a script which is

taking an unusually long time to finish" message if a maximum number of JavaScript statements is exceeded. Complex map operations can exceed this maximum default of 5,000,000. To adjust the maximum time, the HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Styles\MaxScriptStatements registry value must be modified. You can set it to 0xFFFFFFFF for infinity, however this is not recommended. For more information, see Microsoft Knowledge Base article <http://support.microsoft.com/kb/175500>.

- When launching one application from another that is in a different domain, Internet Explorer blocks the single sign-on session cookie. To fix this problem, add the application servers to the Trusted Sites zone for the web browser:
 1. In Internet Explorer browser, click **Tools**, and then click **Internet Options**.
 2. Navigate to the **Security** tab.
 3. Select the **Trusted sites** icon, and then click **Sites**.
 4. In the **Trusted sites** dialog box, add each application server the websites list.
- A known problem with memory growth exists in Internet Explorer when using the NNMi console. It might be necessary to periodically restart the Web browser if it is using too much memory.
- If Integration URLs are rendered inside a <frame> tag on a page that uses the Internet Explorer "[Quirks mode](#)", a JavaScript error occurs.
 - In Internet Explorer, URLs should not be launched in Quirks mode. Quirks Document mode is not standards compliant and NNMi does not support it at this time.
 - This situation might become an issue if an NNMi form or view is placed in an HTML document with other content, such as within a <frame> tag. The <DOCTYPE> tag at the top of the HTML document should be chosen to enable standards document mode. For example, the following DOCTYPE should **not** be used in a web page containing a frame that references an NNMi Integration URL:
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
A **better** choice would be to use a strict DOCTYPE such as:
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
 - The Internet Explorer Developer Tools are useful for seeing and changing the browser and document mode.
- Internet Explorer sets a limit to the number of rows that can be shown in table views. A user cannot scroll to see all possible rows. The workaround is to filter the table to show fewer rows. In practice this limit is about 30,000 rows, although it varies with font size.
- If you are installing NNMi in an Oracle RAC environment, you are asked for 4 parameters during installation: Oracle DB server hostname, Oracle DB instance name (RAC Service Name), and a DB user name and password. If you provide any of these 4 parameters incorrectly you will see error messages stating that the installer is unable to connect to the Oracle database and that you should confirm your selections and try again. However, in a RAC environment, a defect in the installer causes the database URL to be the standalone Oracle URL instead of the RAC-specific URL resulting in fatal error later in the installation process. Therefore, if you enter any incorrect parameters and get the database connection error dialogs, please exit the installer and start over again. When the installer asks "A previous installation configuration has been detected", choose "No" to that dialog, and start the installation from the beginning. Note that this does not apply if you correctly enter all 4 values and do not see the DB connection error dialogs.

Mozilla Firefox Browser Known Problems

- The telnet:// and ssh:// URLs are not enabled by default with Firefox. See the *Configuring the Telnet and SSH Protocols for Use by NNMi* chapter in the [Deployment Reference](#) for instructions on how to enable the telnet and ssh protocols, which requires configuring a telnet application, an ssh application, or both on each web client.
- By default, Firefox opens windows in a new tab instead of a new window. This behavior can cause NNMi to open windows that do not pop to the foreground. To change the default setting, under **Tabs** in the **Options** dialog box, do the following:
 - Set **New pages should be opened in:** to a new window.

- Select **When I open a link in a new tab, switch to it immediately**.
This settings affects web pages that use "_blank" as a target, such as some help content.
- By default, Firefox limits the number of pop-up windows to 20. To adjust this limit, do the following:
 1. Type `about:config` in the Firefox address bar.
 2. Scroll down to **dom.popup_maximum**, and then double-click to modify the value.
 3. Restart Firefox for this change to take effect.
- After opening and closing more than 50 forms in a single session, Firefox might start blocking pop-up windows, even when popups are enabled, which results in JavaScript errors. The workaround is to increase **dom.popup_maximum** or restart the browser. A suggested value in this case is a number greater than 500.
- Firefox tracks long running JavaScript operations and displays a "Warning: Unresponsive script" message if that timeout is exceeded. Complex map operations can exceed this maximum default of 5. To adjust the maximum time, do the following:
 1. Type `about:config` in the Firefox address bar.
 2. Scroll down to **dom.max_script_run_time**, and then double-click to modify the value. The value is in seconds. You can set it to 0 for infinity, however this is not recommended.
 3. Restart Firefox for this change to take effect.
- Firefox enables the use of JavaScript by default. Disabling JavaScript requires a privacy extension. When signing in to the NNMi Console, you will see an error in the browser if JavaScript has been disabled. If you see this error, go to Firefox **Add-ons** page and click on **Extensions** to see if there is an extension that is disabling JavaScript. If so, this extension needs to be disabled in order to allow JavaScript in the browser.
- Firefox can incorrectly indicate that a request is still in progress while using the MIB Browser or Line Graphs, even though the request is complete. You will see "Transferring data from <NNMi Server>" in the Firefox status bar, where <NNMi Server> is your NNMi management server. For more information, see Bugzilla defect #383811 at https://bugzilla.mozilla.org/show_bug.cgi?id=383811.
- Using the "F5" refresh key causes a corrupt display of the form. To refresh a form, use the **Refresh** toolbar button on the form.
- If you have previously created a User Account and later delete and recreate it, the Firefox auto-complete feature fills in the password field for you, without notifying the user interface, causing the create to fail. The workaround is to change the password twice, or turn off form completion in Firefox.

Non-English Locale Known Problems

- NNMi localizes "Drop-down Choice" Code Values (such as Incident Category and Incident Family) at database creation time using the locale of the server. Unlike most other content, if accessed from a client under a different supported locale, the values remain in the locale of the server set at the time of database creation, which is typically installation time. The same is true for any user created "Drop-down Choice" Code Values. Other drop-down choices that are Enumeration Values (such as Incident Severity) are locale-sensitive and appear in the locale of the web browser for supported locales.
- (Windows only) On the Windows platform, the NNMi processes run under the Windows Service Manager (WSM) process. If the system has not been configured so that the WSM is in the same locale, these strings are loaded into the database as English strings. When setting the locale to a supported locale, you must also navigate to the **Control Panel → Region and Language → Administrative** tab → **Change system locale**, and then select the **Current system locale** option. This option requires a system reboot, after which all services (including WSM) are restarted in the new locale. After the WSM is in the desired locale, you can install NNMi.
- For English Internet Explorer to browse an Asian language NNMi management server, the client needs to install the "East Asian Language" on the system. Without this change, tooltips for Priority and other table values appear as squares. You can install the "East Asian Language" from the **Control Panel → Regional and Language Options → Language** tab. Select **Install files for East Asian language**. This problem only happens with Internet Explorer. Users see similar problems when browsing to any Asian language web site.
- When displaying the value for MIB variables of type OCTET STRING, NNMi uses the textual conventions defined

in the MIB. In the absence of textual conventions, the data is interpreted based on any character encodings defined by the `com.hp.nnm.sourceEncoding` property defined in the `nms-jboss.properties` file. If this property is not defined, the multi-byte characters will be interpreted with the UTF-8 character encoding. For more information, see "Configuring Character Set Encoding Settings for NNMi" in the [Deployment Reference](#).

- When launching NNMi URLs with Asian strings such as a Node Group Map with a Japanese language Node Group name parameter, the browser settings might need to be changed. For Firefox, input "about:config" in the address bar; find "network.standard-url.encode-utf8"; change the value to be "true". For Internet Explorer: "Turn on sending URLs as UTF-8"; see Microsoft document at support.microsoft.com/kb/925261 for details.
- The Autopass Licensing GUI (`nnmlicensing.ovpl <ProductName> -gui`) is only localized for Japanese. In all other locales, including Chinese and Korean, only English text is displayed.
- (Windows only) Note that when changing passwords from the Windows command shell, under certain code pages such as 850 and 866, localized (non-ASCII) characters may not be read correctly from the console resulting in a saved password that is invalid. The work-around is to avoid non-ASCII characters when changing passwords from the Windows command shell or use an alternate code page such as 1251 or 1252. Passwords entered in the NNMi UI Console are unaffected by this problem
- (Windows only) The default code page for the `cmd` command on Windows (e.g., code page 850 or 866) may not display all characters properly for localized European languages. This may affect the localized message output when using NNMi commands. The Windows `chcp` command can be used to check the current code page and select a better code page for the locale (e.g., code page 1252 for French, German, and Spanish; 1251 for Russian). The default code page for Chinese, Japanese, and Korean works fine.

Domain Name System (DNS) Configuration Known Problems

- Spiral Discovery depends on a well-configured Domain Name System (DNS) to convert discovered IP Addresses to hostnames. An improperly configured name server results in significant performance degradation. See [Help → Help for Administrators](#) and view the topic *Discovering Your Network → Prerequisites for Discovery*.
- For Linux NNMi servers that do not have a DNS server configured and include only "IP-to-Hostname" mappings in the server's `/etc/hosts` file, additional configuration is needed. If the `/etc/hosts` file has entries such as the following:

```
1.1.1.1 testnode
2.2.2.2 testnode
3.3.3.3 testnode
4.4.4.4 testnode
```

for the node "testnode" to be discovered as a single non-SNMP node with four IP addresses, edit the `/etc/host.conf` file to include the following line:

```
multi on
```

This will ensure that all IP addresses will be returned for the single node.

IPv6 Known Problems and Limitations

- Unsupported IPv6 features; the following are not available in NNMi:
 - IPv6-only management server
 - IPv6 Network Path View (Smart Path)
 - IPv6 Subnet Connection Rules
 - IPv6 Ping Sweep for auto-discovery
 - IPv6 Address Fault monitoring through SNMP (not available for IPv4 Addresses either)
 - IPv6 Link Local Address are not supported for fault monitoring, as discovery seeds, or as Auto-Discovery hints

Device Support Known Limitations

- Device support known limitations can be found in the [HP Network Node Manager i Software \(NNMi\) Device](#)

MIB Loader Migration Known Problems

- NNMi 9.10 updated the MIB loader technology to honor the MIB import statements. If a previous version of NNMi loaded MIBs that either are not standards compliant or depend on textual conventions in a different MIB file, NNMi 10.00 most likely cannot migrate those particular MIBs. MIB migration is loaded as a “best effort.” NNMi migration might fail to persist loaded MIB data. In this case, the MIB loader logs the reason for the failure. Failures are logged in `$NnmInstallDir/tmp/nnm9xMibMigrate`. A directory named “failed” contains a copy of each MIB that failed to migrate and a *.log file named for the MIB indicating why migration failed. If a MIB file is not migrated, the previous TRAP-TYPE macro Incident Configuration does not change, but you might not be able to browse a MIB that you loaded prior to NNMi 9.10. This problem can be fixed by using **Tools** → **Load MIB** to load the missing prerequisite MIB and the MIB that failed to load.

Integration Known Problems

- (BSM / UCDBM Topology Integration) Node reconciliation in UCDBM and BSM Topology often depends on string matching of values provided by different data providers. In some cases, for example, the Interface Description values NNMi sends to BSM/UCDBM have contained null bytes at the end. This can prevent an exact match with data provided by other data providers and causes problems for object reconciliation. In this case, the string contains these characters because NNMi by default interprets OCTET STRING values from SNMP Agents with the UTF-8 character encoding, but the SNMP Agent is returning the data in a different character encoding. The way to correct this is to configure NNMi for the proper source character encoding to expect for SNMP Agents in the environment. The SNMP OCTET STRING data is interpreted based on any character encodings defined by the `com.hp.nnm.sourceEncoding` property in the `nms-jboss.properties` file. In the above example, a property value of “com.hp.nnm.sourceEncoding=UTF-8, Windows-1252” would be used to properly interpret the string data. A different environment may require different values for the source encoding. For more information, see “Configuring Character Set Encoding Settings for NNMi” in the [Deployment Reference](#).
- (BSM Integration) If you are an NNMi or BSM administrator and are using NNMi Visualizations within HP Business Service Management (BSM), do not include the Path View component in the MyBSM portal component gallery. This component is not enabled.
- (Northbound Integration) Northbound integration is disabled under the NNMi Community edition license. After a full license is installed, northbound integration can be re-enabled by reconfiguring a northbound destination.
- (Netcool Integration) The NNMi-provided Netcool rules found in `nnmi.include.rules` use column attributes that may be overwritten or cleared by other rules deployed at runtime. If some attributes of Netcool traps received from NNMi have missing or incorrect data, this may be an area to consider for troubleshooting. It may be helpful to include details by specifying “details(\$*)” in `nnmi.include.rules` in order to verify the final value of certain attributes and variables once received. The NNMi Netcool probe rules are designed to operate within the framework of the Netcool Knowledge Library rule set. The NNMi rules store key NNMi incident information in unused alarm columns to enable “right click” tools to be launched from Webtop or the Web GUI. “Compatibility” rules that are distributed with the Netcool Knowledge Library might overwrite these values and should be checked if the “right click” tools fail to launch because of missing data. See rules defined in `$NC_RULES_HOME/include-compat`. The columns to check include `@LocalNodeAlias`, `@LocalSecObj`, `@LocalPriObj`, and `@LocalRootObj`, `@RemoteNodeAlias`, `@RemotePriObj`, `@RemoteSecObj`, and `@RemoteRootObj`.
- (ArcSight Logger / Operations Log Intelligence Integration) Cross-launches to the ArcSight Logger (or OLI) may eventually stop working with a message that the credentials have failed. The easiest workaround for this is to just launch the ArcSight Logger (or OLI) in a browser window and then immediately log out. The cross-launches will then resume working.

HP Software Support

This web site provides contact information and details about the products, services, and support that HP Software offers. For more information, visit the HP Support web site at: [HP Software Support Online](#).

HP 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 being able to:

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

To access the Self-solve knowledge base, visit the [Self-solve knowledge search](#) home page.

Note: Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract. To find more information about support access levels, go to: [Access levels](#).

To register for an HP Passport ID, go to: [HP Passport Registration](#).

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 Notices

© Copyright 1990–2014 Hewlett-Packard Development Company, L.P.

Trademark Notices

Acrobat® is a trademark of Adobe Systems Incorporated.

Apple and Safari are trademarks of Apple Inc., registered in the U.S. and other countries.

Google™ is a trademark of Google Inc.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

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

UNIX® is a registered trademark of The Open Group.

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

Intel® is a trademark of Intel Corporation in the U.S. and other countries.

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.

Acknowledgements

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

This product includes software developed by the Indiana University Extreme! Lab. (<http://www.extreme.indiana.edu>)