HP Network Node Manager i-series Software Release Notes

Software Version: 8.12 / June 30 2009

This document provides an overview of the changes made to HP Network Node Manager i-series Software version 8.12.
It contains important information not included in the manuals or the online help.

For the latest additions to these Release Notes, see sg-pro-ovweb.austin.hp.com/nnm/NNM8.10/releasenotesupdate.htm

For a list of supported hardware platforms, operating systems, and databases, see the *Support Matrix*.

New In This Version

Overview of the NNMi 8.12 Release

NNMi 8.x is a major modernization of the NNM 7.x software. This release contains many new features. Direct single system upgrades of existing NNM 6.x or 7.x installations to NNMi 8.x are not supported (see the Deployment Guide).

For an overview of NNMi 8.12, see *Introducing HP Network Node Manager* in the Installation Guide (see Installation Guide and Support Matrix).

NNMi 8.12

- Defect fixes
- Support for Linux Red Hat 5.2. For special configuration requirements, see Installation Guide and Support Matrix
- Support for AlaxalA devices
- Support for HP ProCurve Component Health
- Support for running the NNMi console in Mozilla Firefox version 3
- Support for application failover across subnets. For more information, see the Deployment Guide
- Support for LDAP access to multiple directory servers. For more information, see the Deployment Guide
- HPOM agent implementation of the HP NNMi–HPOM integration. For more information, see the Deployment Guide
- URL actions do not open a superfluous browser window
- The Status History table for a node contains up to 30 of the most recent changes
- Incident message formats can include short $ arguments. For more information, see the online help

- Updated online help for the new features introduced in NNMi 8.12
- New command-line tools:
  - nnmnodedelete.ovpl - Deletes nodes. See the nnmnodedelete.ovpl reference page
  - nnmseeddelete.ovpl - Deletes discovery seeds. See the nnmseeddelete.ovpl reference page
  - nnmloadnodegroups.ovpl - Loads node groups using custom attributes, capabilities, or both. See the nnmloadnodegroups.ovpl reference page
  - (NNM iSPI NET) nnmnetloadattrs.ovpl - Loads custom attributes on nodes
- Traps can be loaded in a disabled state. See the nnmincidentcfg.ovpl and nnmtrapdload.ovpl reference pages
- Unresolved traps can be discarded

  You can configure NNMi to discard SNMP traps received from devices that are not included in the NNMi topoplogy. For example, if you configure NNMi discovery to find only seeded devices, you can specify whether NNMi should process or discard traps from any other devices. Because the source of those traps cannot be matched with any hostname or interface object in the NNMi database, those traps are considered unresolved SNMP traps.

  Note: NNMi discards SNMP trap information from nodes or interfaces whose Management Mode is Not Managed or Out of Service.

  By default, NNMi does not discard unresolved SNMP traps. Unresolved traps appear in incident views, but have missing information. For example, the incident might appear as follows:

  - Source Node is an IP address.
  - Source Object is None.

  To discard unresolved SNMP traps:

  a. In a text editor, open the ovjboss.jvm.properties file:
     - Windows:
       `%NnmDataDir%\shared\nnm\conf\ovjboss\ovjboss.jvm.properties`
     - UNIX:
       `/var/opt/OV/shared/nnm/conf/ovjboss/ovjboss.jvm.properties`

  b. Include the following entry: `com.hp.nnm.events.discardUnresolvedSnmpTraps = TRUE`

NNMi 8.11

- Defect fixes
- Application failover. Additional NNMi installations can become a primary system in case of system failure. For more information, see the Deployment Guide
- Custom Poller
  - Polling of arbitrary MIB variables to augment out of the box polling
  - Flexible configuration based upon powerful dynamic grouping capabilities
  - Thresholding of poll results to:
    - Affect node status
    - Create incidents to alert on abnormal polled values
- Improved cross-product integrations. For more information, see the Deployment Guide
  - HP Performance Insight
  - HP Network Automation
  - Portlets for the MyBSM portal of HP Business Availability Center

Bulk Incident assignment through new *Actions:Incident Assignment...* menu

- Support for users, passwords, and roles from an enterprise directory service through LDAP. When users are retrieved from the directory service, the Assigned To field for an Incident is now read-only. Use the *Actions:Incident Assignment...* menu when user names are stored in the directory service instead of the NNMi database. For more information, see the Deployment Guide
- New "User Principals" view in the Configuration workspace that makes it easier to delete users
- Improved support for Alcatel devices
- Incident Menus can be made unavailable based on Incident attributes
- Improved control of dynamic management address discovery used by SNMP
- Configuration forms can be directly accessed through URL launch
- nnmtopodump.ovpl - textual output of topology. See the nnmtopodump.ovpl reference page
- Tools for upgrading from NNM 6.x/7.x to NNMi 8.x:
  - nnmmigration.ovpl - Runs on the NNM 6.x/7.x system and calls several other upgrade tools
  - nnmtrapdload.ovpl - Imports NNM 6.x/7.x trapd.conf definitions as Incident configurations
  - nnmmibmigration.ovpl - Imports MIB definitions from the NNM 7.x snmpmib file
  - snmpCapture.ovpl - Lists the NNM 6.x/7.x community strings
  - nnmmapmigration.ovpl - Runs on the NNM 6.x/7.x system to gather node group and background information about the NNM 6.x/7.x location submaps for one OVW map
  - For more information see the "Upgrading from NNM 6.x/7.x" chapter in the Deployment Guide

NNMi 8.10

- New License Levels
  - For details of the new features available with *NNMi Advanced* or the *iSPI Network Engineering Toolset*, see Licensing.
- User Interface New Features
  - Map Based Management through Node Groups
    - Geographical background graphics accessible at http://<MACHINE>:<PORT>/nnmbg/
    - User definable background graphics
    - Layer 2, Layer 3, Subnet Connections, and User Connections can be used to interconnect between Nodes and Node Groups
    - Node Group Map navigation (back button, double click to drill down into child Node Group)
    - External URL launch of Node Group form and Node Group Map
    - Launch Node Group maps from a Node, Incident, Interface or IP Address
    - Connect Node Groups to Nodes or other Node Groups
    - Launch a Node Group Map Settings form or Node Group form directly from a Node Group map
    - Indicate open Key Incidents on Node Group maps by displaying larger icons for Source Nodes
    - If enabled, non-Administrators can update Node Group Map Settings, such as changing the background graphics
  - Path View Improvements
    - Shows Layer 2 connectivity between Layer 3 nodes
    - Path View Editor – Displays missing sections of a path

    - Path View and RAMS Integration – If RAMS is in the environment, Path View uses RAMS data for the Layer 3 portion of the Path View (requires NNMi Advanced)
    - Shows multiple paths from Equal Cost Multi-Path (requires the RAMs product and NNMi Advanced)
  - Quick View Improvements - You can now visualize sets of objects from Quick View without opening the form. These object lists include the following
    - IP Addresses and Interfaces for a Node
    - Conclusions for Node, Interface, IP Address, Layer 2 Connection, Router Redundancy Group, and Node Component Health
    - IP Addresses for an Interface
    - Child Node Groups for a Node Group
    - Custom Attribute name/value pairs for a Node or an Interface
    - Capabilities for a Node or an Interface
    - VLANs for an Interface
    - Ports for a VLAN
    - Members and virtual IPs for a Router Redundancy Group
    - Display Available Bandwidth, Maximum Bandwidth, and Available Bandwidth Percentage for aggregated links (requires NNMi Advanced)
  - New "Topology Maps" workspace which contains:
    - Node Group Overview - a Map View of all toplevel Node Groups
    - Network Overview - a Map View of most highly connected Layer 3 devices
    - Configurable list of Node Group maps
  - User Interface Configuration form to control console timeout, maximum number of nodes on a map, hide unlicensed features, or configure initial starting table/map view displayed when first sign in (defaults to Network Overview)
  - Launch a Node Group, Node, or Source Object form directly from an Incident, including new "Remote Site (Island) Unreachable" Incident
  - Ability to launch multiple Map View windows
  - Added `Help → NNMi Documentation Library → URL Launch Reference` menu item to describe the types of URL launch that is possible
  - "`Help → About HP Network Node Manager i-series`" now shows the number of monitored (polled) interfaces, addresses, agents, Router Redundancy (requires NNMi Advanced), and device component health
  - URL Actions can be made unavailable in the URL Action menu when selected item(s) do not match the configurable set of capabilities, custom attributes, object type, or number of selected objects
  - Link Aggregation Interfaces Interface Group (useful for filtering All Interfaces to see the degraded Aggregated Interfaces, requires NNMi Advanced)
  - Tabular views of Component Health for nodes
  - More information displayed in the VLAN tab in the Node form
- Spiral Discovery New Features
  - The discovery technology leveraged from NNM 7.x has been replaced. As a result, the legacy ovet_* processes (seen when running the ovstatus command) have been removed
  - Spiral Discovery now supports the following protocols and vendors:
    - Q-BRIDGE-MIB

    - Nortel Baystack and Passport private interfaces
    - Nortel and Foundry VRRP
    - Aggregated Ports through Cisco PaGP (requires NNMi Advanced)
    - OSPF neighbors and BGP peers are used for finding new nodes
  - Optional use of Ping Sweep during Continuous Spiral Discovery
  - Layer 2 connectivity is now provided for Non-SNMP Nodes
  - Connection Editor now supports creating user connections to a non-SNMP node
  - Aggregated Ports and connections are discovered. These connections are displayed as thicker lines in Layer 2 connected maps, and Interfaces/Layer 2 Connections have child Interfaces/Layer 2 Connections (requires NNM i Advanced)
  - User-specified IP Addresses can be excluded from discovery using the Discovery Configuration form
  - VLAN table includes Node name and Interface to differentiate between VLANs with identical names
  - Non-SNMP addresses are merged into a single node if the nameserver resolves multiple addresses to the same name
  - Auto discovery uses smarter algorithms for WAN and end-node connectivity, including routing tables
- Incident and Root Cause New Features
  - Threshold Incidents can be generated on CPU, memory, and buffer (Cisco Only)
  - Traps can be forwarded with additional varbinds indicating the original source
  - Original SNMP Trap forwarding is supported on UNIX
  - Enumerated values from loaded MIBs can display text instead of numeric value in Incidents using the `$text($n)` format. See the nnmloadmib.ovpl reference page for details
  - Configurable Trap forwarding
  - Root Cause Analysis has been enhanced to utilize smarter algorithms for isolated islands of nodes
  - Ability to display and modify trap properties such as port number, buffer size, etc. See the nnmtrapconfig.ovpl reference page
  - Additional options to nnmtrimincidents.ovpl to further refine what incidents are trimmed
  - Ability to detect and react to trap storms from the whole environment and specific devices
  - The C-based nnmtrapd has been replaced with a java based nnmtrapserver, which can be configured with ${NNM_DATA}/shared/nnm/conf/nnmtrapserver.properties
  - An Incident is generated when an Island Node Group becomes unreachable
  - Island Node Groups generate an Incident when they are no longer reachable. From this Incident you can launch a Node Group map or open the Node Group definition
  - The Incident workspace has been replaced with the Incident Management and Incident Browsing workspaces to focus on operational versus historical use models
  - "Key Incidents" views have been added to show the most important Incidents
- More Powerful Node and Interface Groups
  - Node Groups can be configured to be hierarchical
  - Hierarchical graphical views of your network environment can be scoped by Node Group definitions
  - Inventory, Incidents, and topology maps can be scoped by Node Groups
  - Node Groups can be configured based on additional attributes, such as sysName, sysLocation, sysContact, management address, custom attributes/values, or capabilities using a new custom filter editor in the Node

Group form

- The nnmloadnodegroups.ovpl tool can be used to bulk load Node Groups from a comma separated values file (csv), such as Microsoft Excel. See the nnmloadnodegroups.ovpl reference page for more information
- Interface Groups can be defined by ifDescr, ifName, and other interface properties, using the same custom filter editor as Node Group configuration
- Node Groups and Interface Groups can be defined by IP Address range
- Configurable Node Group status computation by percentage

- Security Management New Features
  - SNMPv3 natively supported
    - Configurable User Security Model
    - Node discovery is SNMPv3-based
    - NNMi receives SNMPv3 Traps
    - NNMi responds to SNMPv3 notify from agents
  - NNMi uses proxy capabilities to connect with products such as Tavve Zone ranger.
  - Security on the management station has been enhanced to include encrypting of passwords and the obscuring passwords on entry
  - No clear text passwords used by command line tools or for system password
    - New nnmsetcmduserpw.ovpl script to create a ${HOME}/.nnm/nnm.properties file
    - If you are migrating from NNMi 8.0x and you created a ${HOME}/.nnm/nnm.properties, you need to encrypt your password using the nnmsetcmduserpw.ovpl. See the nnmsetcmduserpw.ovpl and nnm.properties reference pages for more information.
    - Commands to reset the system password are provided. See the nnmchangesyspw.ovpl reference page for more information.
- Integration Modules Workspace
  - NNMi to HP Operations Management integration configuration
  - NNMi to HP Universal Configuration Management Database
  - Note: See the *Support Matrix* for supported integration versions
- Device Component Monitoring
  - Fault based monitoring of devices (e.g. fan, temp, etc.) can be completed. This affects status of devices. With iSPI for Performance, additional device component metrics are collected and thresholded on (CPU, Memory, Buffers, etc.).
- The NNMi software interface is localized in Simplified Chinese and Korean (documentation is not translated)
- A command line tool has been added to change the management mode for nodes. See the nnmmanagementmode.ovpl reference page for more information.
- SNMP Command line tools which support SNMPv3, replacing previous executable commands. See the nnmsnmpbulk.ovpl, nnmsnmpget.ovpl, nnmsnmpnext.ovpl, nnmsnmpnotify.ovpl, nnmsnmpset.ovpl, and nnmsnmpwalk.ovpl reference pages for more information.
- Node hostnames from DNS are now in lower-case. If you previously used upper-case for a Node Group filter in 8.0x Node Group settings, you need to change the Node Group definition to use lower-case.

NNMi 8.03

- HP NNMi and HP Operations Manager are integrated. For details on HPOM requirements and configuration instructions, see the *Support Matrix*.

NNMi 8.02

- Support for NNMi on High Availability Systems - MC ServiceGuard for HP-UX/Linux, Veritas for Solaris, and MS Cluster Server for Windows. For more information, see the Deployment Guide). For a list of supported High Availability systems, see the *Support Matrix*.

NNMi 8.01

- Integration for the optional NNM iSPI for Performance product, including user-configurable thresholds
- Japanese language support
- Solaris and Linux support
- Node Group status and new Details action
- Subnet connectivity (configurable Layer 2 Connections created for small subnets)
- More information provided in the `Actions → Monitoring Settings` dialog
- EDP/NDP/FDP used for hints in auto discovery
- HTTPS available as documented in the Deployment Guide
- Author-specific configuration export via `nnmconfigexport.ovpl`
- New `Important Nodes` Node Group which can be manually populated with nodes to have special Causal Engine behaviors

NNMi 8.00

- Low total cost of ownership, easy to use
- Powerful Incident Views
- Powerful configuration paradigm
- Dynamic spiral discovery
- Causal Engine based root-cause analysis
- User Roles
- High per-system scalability
- Web 2.0 AJAX-based user interface
- Web Services-based SDK for Integration

Documentation Updates

The complete documentation set is available on the HP Product Manuals web site at h20230.www2.hp.com/selfsolve/manuals.

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

Deployment Guide

A web-only document providing advanced deployment, configuration, and upgrading information for HP NNM i-series Software is available at h20230.www2.hp.com/selfsolve/manuals. Look for the *HP Network Node Manager i-series Software Deployment Guide*.

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

Documentation Errata

Note the following corrections to the NNMi online help:

- When you configure incidents, NNMi enforces the following length limits:

  Custom Incident Attribute (CIA) name limit is 80 characters
  CIA value limit is 2000 characters

  If you exceed one of these limits, NNMi truncates the value from the left.

- NNMi loads the following MIBs during installation:
  - rfc1213-MIB-II
  - rfc1493-BRIDGE
  - rfc2863-IF-MIB
  - rfc1269-BGP
  - rfc1850-OSPF-MIB
  - rfc2127-ISDN-MIB
  - CISCO-SMI.my
  - CISCO-VTP-MIB.my
  - CISCO-HSRP-MIB.my
  - CISCO-ENVMON-MIB.my

- The information about the new Custom Poller feature in the Japanese online help has not been translated and is, therefore, available only in English at this time.

Installation Guide and Support Matrix

To obtain an electronic copy of the most up-to-date version of the HP Network Node Manager i-series Software Installation Guide, point your browsers to http://h20230.www2.hp.com/selfsolve/manuals.

Installation requirements, as well as instructions for installing NNMi, are documented in the installation guide provided in Adobe Acrobat (.pdf) format. The document file is included on the product's installation media as: `install-guide_en.pdf`. After installation the document can be found from the NNMi console by picking `Help → Documentation Library → Installation Guide`.

For a list of supported hardware platforms, operating systems, and databases, see the *Support Matrix*.

Licensing

Network Node Manager installs with an instant-on 30-day/250-node license. This license also temporarily enables the NNMi Advanced features and the NNM iSPI Network Engineering Toolset for the 30-day trial period. The additional features available with each license are listed below.

To check the validity of your NNMi licenses, from the console pick "`Help → About HP Network Node Manager i-series`", click "View Licensing Information", and then compare any node counts with the count displayed in "`Help → About HP Network Node Manager i-series`".

For information about installing and managing licenses, see the Installation Guide.

HP Network Node Manager i Advanced Software

In addition to the above NNMi features, an NNMi Advanced license (nnmlicense.ovpl NNM -g) enables the following additional features:

- Monitoring of router redundancy groups (HSRP, VRRP)
- Support for port aggregation (for example, PaGP)
- Route Analytics Management System integration for RAMS traps and Path information from RAMS, enhancing the path displayed in Path View
- Extension of Path visualization for the above capabilities (for example, Equal Cost Multi-Path visualization). When there are multiple paths possible, the User Interface allows for selection of specific paths for launching of NNM iSPI for Performance path health report.

HP Network Node Manager iSPI Network Engineering Toolset Software

An HP Network Node Manager iSPI Network Engineering Toolset Software license (nnmlicense.ovpl iSPI-NET -g) enables the following features:

- Device Diagnostics collection and display. For more information, see Incident configuration and the Diagnostics tabs on Nodes and Incidents. Requires installation of the iSPI Network Engineering Toolset server.
- Ability to find the switch port for a discovered or an undiscovered node via MAC Address, IP Address, or hostname. See "`Tools → Find Attached Switch Port...`"
- Ability to show a table of MAC addresses, IP Address, and hostnames for a switch. See "`Actions → Show Attached End Nodes`"
- Trap Analytics data is logged in a user-consumable form. For more information, see the nnmtrapdump.ovpl reference page

Known Problems, Limitations, and Workarounds

- NNMi 8.1x no longer supports the following Solaris T series processors: UltraSparc T1, T2, and T2 Plus.
  NNMi 8.1x does support the following Solaris processors: UltraSPARC IIIi, IV, and IV Plus.
- NNMi 8.1x iSPIs have not been certified on RH 5.2 and are currently not supported.
- Default, Node Specific, or both SNMP community strings must be set up in SNMP Configuration (`Configuration → Communication Configuration`) before running `nnmloadseeds.ovpl` or adding seeds to the discovery configuration table to initiate discovery. Otherwise, initial discovery may classify the node as "Non SNMP". If this classification occurs, correct the SNMP Configuration and rerun discovery for the node using `nnmconfigpoll.ovpl` or `Actions → Configuration Poll`. For more information, see the nnmloadseeds.ovpl and nnmconfigpoll.ovpl reference pages available from the `Help → Documentation Library → Reference Pages` menu in the NNMi console.
- NNMi relies heavily on Layer 2 connectivity for Layer 2 Neighbor Maps, Root Cause Analysis (correlating faults which are in the shadow of other faults), and determining which interfaces to monitor.
  NNMi requires the node on the far side of a Layer 2 connection to support SNMP to compute connectivity. In addition, the node on the far side of the connection must be a supported device. (See the *Support Matrix* for supported devices). If the remote node is not supported, but speaks SNMP, and you have no Layer 2 Connectivity, you can use the Connection Editor (`nnmconnedit.ovpl`) tool to add this connectivity. See the `nnmconnedit.ovpl` reference page for more information. If instead, you only require monitoring of these unconnected interfaces, use a Node Group and Monitoring Configuration to enable polling of unconnected interfaces.
- In NNMi map views, the internet browser's zoom (ctrl+plus and ctrl+minus) does not display properly. These keystrokes only zoom the HTML text and not the icons themselves. Instead, use the Map's keyboard accelerators to zoom (plus (+), minus (-), and equals (=) keys).
- Redirection of `*.ovpl` scripts on Windows using file association might not generate an output file. For example:
  `nnmstatuspoll.ovpl -node mynode > out.log`
  The workaround is to run the command directly from Perl and not use file association:
  `"%NnmInstallDir%\nonOV\perl\a\bin\perl.exe" "%NnmInstallDir%\bin\nnmstatuspoll.ovpl" -node mynode > out.log`
  A second option is to fix your Windows Registry:
  1. Start the Windows Registry Editor (regedit.exe)
  2. Locate and then click the following key in the registry:
     HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
  3. On the Edit menu, click Add Value, and then add the following registry value:
     Value name: InheritConsoleHandles
     Data type: REG_DWORD
     Radix: Decimal
     Value data: 1
  4. Quit Registry Editor
- The `nnmincidentcfg.ovpl -loadTraps <mib_file>` command does not reload an SNMP trap or notification if it has already been loaded into the NNMi incident configuration. Changes to the trap annotations in the MIB file, such as SUMMARY (message) or SEVERITY, are not updated. The workaround is to delete the configured incident from the Incident Configuration, and then reload the incident with the `nnmincidentcfg.ovpl` command.
- Cross-launch to NNM 7.x using an NNMi 8.x "Management Station" object requires the Java Plug-in 1.4.2 to run

the NNM 7.x Home Base (NNMi 8.x does not otherwise require any plugins). If you are cross launching to NNM 7.x you must first install the 1.4.2 plugin on the client browser from java.sun.com/j2se/1.4.2/download.html

- HP-UX systems might hang when the system starts running low on memory in very large environments if it is not running the required set of patches. See the *Support Matrix* for a list of HP-UX required patches.
- In Auto Discovery mode, a node with empty ipAddrTable (RFC1213-MIB) which is NOT seeded explicitly, is ignored by Spiral Discovery. The workaround is to load missing nodes due to empty ipAddrTable as seeds.
- In forms that have the auto-complete feature (such as Child Node Groups in the Node Group form), if you type in a name, you must tab out of the field before saving your changes; otherwise you get an error upon save.
- In Neighbor Views, when you enter a Node Name in the auto-complete field, if you press return before the drop-down list displays, the view might close.
- Do not use the `nnmsnmp*.ovpl` commands in event actions, as they are slower than NNM 7.x native SNMP commands and will significantly degrade event pipeline performance.
- If devices do not respond with required SNMP MIB values, Spiral Discovery may not find Nodes, Layer 2 Connections, or VLANs. See "Supported Devices" in the *Support Matrix*.
- Be sure the management system does not have a firewall blocking incoming HTTP requests; otherwise you will not be able to start the NNMi console remotely. The Linux firewall is enabled by default. To disable the Linux firewall, pick `Applications → System Settings → Security Level`. You can either Disable the firewall completely, or more specifically add to Other ports:
  161:udp, 162:udp, <*HTTPPORT*>:tcp
  where <*HTTPPORT*> is the port you chose for the NNMi web server as defined by the `jboss.http.port` value in `/var/opt/OV/shared/nnm/conf/nnm.port.properties`.
- If using LDAP to access your environment's directory services, you must sign in using the same case sensitivity of users as reported by the directory service. If you use upper case letters in a user name against a case insensitive directory server, Incident Assignment and My Incidents will not work if the case sensitivity differs between what is returned from the directory service and the name with which you signed in. Be sure to sign in using the same case as shown when you perform `Assign Incidents`.
- Due to a timing issue, it is possible that `File → Sign Out` might not redirect your browser to the sign-in screen. If this happens, you'll need to pick `File → Sign Out` a second time.
- Application failover on the Windows platform can have some intermittent issues with Symantec Endpoint Protection (SEP) software which affects 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 dialogs to the Windows desktop and the event viewer. These messages do not affect operation and can be ignored.
- Attempting to delete a Collection or Policy with a large number of Polled Instances can fail. When the delete is attempted, the UI shows the "busy circle" for a few minutes and then shows an error message that 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 really want to poll to help minimize this issue and the load on NNMi.
  A workaround is possible using the following sequence:
  1) Try deleting the Collection. If that fails...
  2) Try deleting each Policy on the Collection individually.
  For each Policy that fails to delete...
  a) If the Policy has a MIB Filter value, change its value to pattern which will not match any MIB Filter Variable value. Check the Custom Node Collection table to ensure that all nodes for that Policy have completed discovery. All Polled Instances for this Policy should be removed.
  b) If the Policy does not have a MIB Filter value, change the Policy to Inactive. This action should cause all Polled Instances associated with the Policy to be deleted. If it does not then try editing the associated node group to remove nodes from the group which will result in Custom Node Collections and their polled instances to be deleted.
  3) It should now be possible to delete the Policy successfully.

4) When all Policies for a Collection have been deleted, it should be possible to delete the Collection as well.

Potential Installation Issues

- In addition to the web server port, the NNMi server uses the following ports for its processes: 1099, 443, 1098, 3873, 4444, 4445, 4446, 4457, 8083, 8087, and 8096. Ensure that these ports are not in use prior to NNMi installation.
- Installation on Windows using Terminal Services:
  NNMi installation only works if you are on the machine console. If you use remote login technology (for example, Remote Desktop Connection), you must ensure that you are accessing the Windows console and not a secondary connection.
- Installation using symlinks on Solaris:
  On Solaris, if you wish to install onto a filesystem besides /opt/OV and /var/opt/OV, you can create these directories as symlinks to some other directory. However, the Solaris "pkgadd" command requires the following environment variable to be set:

  PKG_NONABI_SYMLINKS="true"
- To install NNMi on a 64-bit Linux server, you must have the following library files installed. These are the library versions that NNMi requires:
  - /usr/lib64/libstdc++.so.5
  - /usr/lib64/libstdc++.so.5.0.7

  See the English version of the *Installation Guide* for complete instructions.
- For Solaris systems, NNMi 8.1x requires that the semaphore count be increased to 256 to avoid problems.

  To make this change, run the following commands as root:

  ```
  prctl -n project.max-sem-ids -v 256 -r -i project user.root
  projmod -a -K "project.max-sem-ids=(priv,256,deny)" user.root
  ```
- Some Linux installations might have a version of Postgres installed and running by default. If this is the case, you need to disable the default Postgres instance that is running prior to installing NNMi because NNMi does not support multiple instances of Postgres on the same server. The easiest way to determine if you have an existing Postgres instance running is by running ‘ps –ef | grep postgres’. Postgres can be disabled with 'chkconfig posgresql off'.
- For Linux Red Hat 5.2, the NNMi management server requires additional configuration steps before NNMi 8.10 product installation, after installation, and before patch installation. Firewall configuration might be required. For special configuration requirements, see the patch installation instructions
- NNMi supports Single Sign-On (for use with iSPI integration). This technology requires the NNMi management server to be accessed using the official Fully Qualified Domain Name (FQDN). The official FQDN is the hostname used to enable Single Sign-On between NNMi and iSPIs and must be a resolvable DNS name.
  - During installation, NNMi selects the official FQDN for the NNMi management server and enables you to override the value displayed.
    - You can find out the official FQDN configured for your system in one of two ways:
      - "`Help → About HP Network Node Manager i-series`" dialog
      - $NnmInstallDir/bin/nnmofficialfqdn.ovpl
    - You can change the official FQDN configured for your system after install using the following command
      - $NnmInstallDir/bin/nnmsetofficialfqdn.ovpl
  - If you are using NNM iSPIs with Single Sign-On, you can use the "Enable URL Redirect" option on the User Interface Configuration form (in the Configuration workspace) to have NNMi automatically redirect NNMi URL requests to the official FQDN for the NNMi management server.
    - Note: Before enabling URL Redirect, verify that the official FQDN is set correctly and that it is a DNS name that is resolvable from the remote systems that need to access the NNMi management server. If the official FQDN does not meet these requirements, users will see a "page not found" error when trying

to access the NNMi console

- When URL Redirect is enabled, note the following:
  - You can sign in to the NNMi console using any hostname that is valid for the NNMi management server. For example, if users request http://localhost/nnm, NNMi redirects them to a URL such as: http://host.domain/nnm.
  - If you cannot access the NNMi console, you can get direct access to the NNMi console using the following URL: http://<server>:<port>/nnm/launch?cmd=showMain

- Do not use the "system" user account for normal NNMi operations. NNMi provides the "system" user account for accessing NNMi the first time during installation and for command line access. Single Sign-On and incident assignment do not work with the "system" user account.

- After a silent install, or if you forget your NNMi system password, the NNMi system password can be reset with the $NnmInstallDir/bin/nnmchangeswspw.ovpl script. If you install NNMi using a silent installation, complete the following steps after the NNMi processes are running:

  1) Stop the NNMi processes using the ovstop -c command.
  2) As root or administrator, run the $NnmInstallDir/bin/nnmchangesyspw.ovpl script and follow the displayed instructions to set a new system password. You will need this new system password to complete step 4.
  3) Start the NNMi processes using the ovstart -c command.
  4) Run the Quick Start Configuration Wizard as explained in the *Installation Guide*.
  If you forget your NNMi system user password, you will need to run steps 1 through 3 to reset the system password.

- Issue with Silent Install on Windows (specifically, non-English locales):
  For silent installation on a target system, the *Installation Guide* says to run an install using the UI on another system. This creates a "%TEMP%\HPOvInstaller\NNM\ovinstallparams_*DATETIME*.ini" file. This file can be copied to another system as %TEMP%\ovinstallparams.ini and then installed using the silent installer. However, if you edit this file using the Notepad editor, and if this file was generated on non-English locale machine (e.g. Japanese, Korean, Chinese), then Notepad will introduce 3 bytes at the start of the file to specify the encoding as UTF-8. However these 3 bytes cause the subsequent silent installation process to fail. Therefore the recommendation is to use Wordpad (or some other editor) instead of Notepad to modify the ovinstallparams.ini file.

- If you plan to upgrade an earlier version of NNMi 8.0x that is running in a High Availability environment, the supported upgrade path is to temporarily unconfigure HA, upgrade NNMi, and then reconfigure HA. For detailed information, see the chapter on configuring High Availability in the Deployment Guide.

- If you have iSPIs installed on the NNMi management server, uninstall the iSPIs before uninstalling NNMi. Otherwise, when you reinstall NNMi, the iSPIs no longer work until you reinstall each iSPI.
  Note: NNM iSPI for Performance is an exception to the above uninstall requirement.

Internet Explorer Browser Known Problems

- The telnet:// URL is not enabled by default with Internet Explorer. See the NNMi online help for instructions on how to enable telnet protocol, which requires a registry change. Without this registry edit, selecting `Actions → Telnet... (from client)` displays 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 Microsoft Internet Explorer to display view and form titles:

  a. Open the Internet Explorer browser and select the Tools menu.

  b. Click Internet Options.

  c. Navigate to the Security tab, Trusted Sites, Custom Level, Miscellaneous section.

  d. Disable the Allow websites to open windows without address or status bars attribute.

- Map Views may not be properly drawn in an Internet Explorer client. This results in either a blank window or a window where only labels are displayed. No errors are reported. This is often because VML is disabled in your Internet Explorer Browser. VML (Vector Markup Language) is Microsoft's technology for drawing and embedding vector graphics in web pages in Internet Explorer. A number of Microsoft security fixes disable this functionality.

  You can verify that VML is properly configured by browsing to a site that requires VML.

Workarounds that do not require administrator access:

a. Make sure the NNMi server to which you are connecting is in the appropriate IE security zone
Ideally, the NNMi server should be assigned to the "Local intranet" zone
Note: It is preferable to add the NNMi server to your "Trusted sites" zone than to enable privileges in a more restricted zone.

b. Verify that the "Binary and script behaviors" permission is Enabled for the security zone determined in the previous step.
Windows "Internet Properties" dialog can be accessed from Internet Explorer by selecting the "Internet Options..." item from the Tools menu, or by opening the "Internet Options" icon in the Control Panel.

i. In the Internet Properties dialog, navigate to the "Security" tab

ii. Select the icon corresponding to the zone
Internet Zone - Globe icon
Local Intranet - Monitor in front of a globe icon
Trusted sites - Green checkmark icon
Restricted sites - Red circle with a line through it icon

iii. Press the "Custom level..." button to access the Security Settings dialog for the selected zone

iv. In the "Security Settings - _____ Zone" dialog, scroll down to the radio buttons for "Binary and script behaviors" (under the "ActiveX controls and plug-ins" header), and make sure the Enable radio button is selected
Note: It is preferable to add the NNMi server to your "Trusted sites" zone than to enable privileges in a more restricted zone.

c. Use a remote-client technology (for example, Remote Desktop Connection or VNC) to access a different machine that does not exhibit this problem

The solutions described below require Administrator privileges to the machine on which the Internet Explorer client exhibiting the problem is installed.

a. Verify the latest updates for Internet Explorer 7 are installed on the client machine, using Windows Update or similar. An outdated patch level could be the reason VML is disabled.

b. Make sure Vgx.dll is registered
The following command registers VML's vgx.dll if it was not already registered:
regsvr32 “%ProgramFiles%\Common Files\Microsoft Shared\VGX\vgx.dll”

c. Check the Access Control List settings on Vgx.dll
cacls “%ProgramFiles%\Common Files\Microsoft Shared\VGX\vgx.dll”

- A known problem with memory growth exists in Internet Explorer when using the NNMi console. It may be necessary to periodically restart the Web browser if it is using too much memory.

Mozilla Firefox Browser Known Problems

- Firefox limits the number of popup windows allowed. It is 20 by default. To adjust this limit, type *about:config* in Firefox's Address bar. Scroll down to *dom.popup_maximum*, then double click and modify the value. You need to restart Firefox for this change to take effect.
- After opening and closing more than 50 forms in a single session, Firefox might suddenly start blocking popup windows, even when popups are disabled, 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" dialog if that timeout is exceeded. Complex map operations can exceed this maximum default of 5. To adjust the maximum time, type *about:config* in Firefox's Address bar. Scroll down to *dom.max_script_run_time*, then double click and modify the value. The value is in seconds. You can set it to 0 for infinity, however this is not recommended. You need to restart Firefox for this change to take effect.
- Firefox will not let javascript raise a window to the top of the browser windows. This can cause a previously opened window to not be viewable. (for example, a form might be re-opened at the back of your window stack.) To enable Firefox to raise previously opened windows to:

a. From a new Firefox window, click `Tools → Options...`. This "Tools" menu item is the one in the browser itself, not from within the NNMi console.

b. In the options dialog, select the Content pane.

c. Next to the "Enable JavaScript" checkbox (which should be checked), click on the "Advanced..." button.

d. Check (enable) the "Raise or lower windows" option.

e. Click OK twice.

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.
- Related to the above, 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, then these strings are loaded into the database as English strings. When setting the locale to a supported locale, you must also remember to navigate to `Control Panel → Regional and Language Options → Advanced` tab, and check the "Apply all settings to the current user account and to the default profile." option. This option requires a system reboot, after which all services (including WSM) are restarted in the new locale. Once the WSM is in the desired locale, you can install NNMi.
- For English Internet Explorer 7 to browse an Asian language NNMi server, the client needs to install the "East Asian Language" on the system. Without this change, tooltips for Priority and other table values display as squares. You can install the "East Asian Language" from `Control Panel → Regional and Language Options → Language Tab`. Select "Install files for East Asian language". This only happens with Internet Explorer. Users will see similar problems when browsing to any Asian web site.
- SNMP Traps sent to the NNMi management server must conform to IETF specifications and only contain ASCII characters. Multi-byte characters in SNMP traps do not display properly.
- Non-applet-based views, such as the NNM 6.x/7.x Launcher, SNMP Data Presenter, SNMP MIB Browser, Alarm Browser, and Report Presenter, do not display properly when browsed to from a Linux UTF-8 enabled browser. However, Dynamic Views and the Network Presenter display properly.
- Online help does not display Kanji characters in the correct order in the master online help index.
- When launching NNMi URLs with Asian strings such as a Node Group Map with Japanese language Node Group name parameter, the browser settings may need to be changed. For Firefox, input “about:config” in address bar; find “network.standard-url.encode-utf8”; change the value to be “true”. For IE7: "Turn on sending URLs as UTF-8". Read the Microsoft document at http://support.microsoft.com/kb/925261 for details.

Domain Name System (DNS) Configuration Known Problems

Spiral Discovery depends heavily 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 → Discovering Your Network → Prerequisites for Discovery`.

HP Software Support

Please go to the HP Support web site:
www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued customer, you benefit by being able to do the following:

- 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

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 and HP Passport, go to the following URL:
support.openview.hp.com/new_access_levels.jsp

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.

For information about third-party license agreements, see the license-agreements directory on the product installation media.

Copyright Notices

Trademark Notices

DOM4J® is a registered trademark of MetaStuff, Ltd.

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.

Java™ is a US trademark of Sun Microsystems, Inc.

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

Oracle® is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

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

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