HP Network Node Manager i Software Release Notes

Software Version: 9.01 / 27 August 2010

This document provides an overview of the changes made to HP Network Node Manager i Software (NNMi) version 9.01.
It contains important information not included in the manuals or in online help.

For additions to these Release Notes, see sg-pro-ovweb.austin.hp.com/nnm/NNM9.00/releasenotesupdate.htm.

For a list of supported hardware platforms, operating systems, and database, see the *Support Matrix*. For the list of supported network devices, see the NNMi Device Support Matrix at sg-pro-ovweb.austin.hp.com/nnm/NNM9.00/devicematrix.htm.

New In This Version

Overview of the NNMi 9.01 Release

NNMi 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 are not supported (see the NNMi Upgrade Reference). Single system upgrades of NNMi 8.x to NNMi 9.x are supported (see the NNMi Deployment Reference).

For an overview of NNMi 9.00, see *Introducing HP Network Node Manager* in the NNMi Installation Reference (see NNMi Installation Reference and Support Matrix).

NNMi 9.01

- Product Installation
  - NNMi 9.01 is delivered as NNMi 9.0x patch 2. If you have not yet installed NNMi 9.00, you can install the patch as part of the product installation. Ensure that you have the correct product installation image as described in "9.0x patch installation during 9.00 installation/upgrade issues" in the NNMi 9.0x Release Notes Updates.
- Product Changes
  - The `-diagnose` option to `nnmldap.ovpl` tests the LDAP configuration on the NNMi management server for an NNMi user. See the *nnmldap.ovpl* reference page.
  - Support for multi-subnet NNMi application failover for large scale environments. This change removes the previous limitation on the Windows operating system.

- The `nnmmanagementmode.ovpl` command now provides the ability to set management mode on interfaces in addition to nodes. See the *nnmmanagementmode.ovpl* reference page.
- NNMi discovers VMware ESXi devices and the ESX version hosted on an operating system. If you want to analyze any VMware ESXi devices using line graphs or the Custom Poller, see "Required MIBs for graphing and polling VMware ESXi device information" in the NNMi 9.0x Release Notes Updates.
- If you want to be notified whenever an SNMP Trap is received that does not have an associated incident configuration, you can configure NNMi to generate an Undefined SNMP Trap incident. See the *NNMi Incidents* chapter of the NNMi Deployment Reference.
- NNMi can automatically delete nodes that have been unreachable (by either SNMP or ICMP) for a configurable number of days. Enable and configure this feature on the Discovery Configuration form in the NNMi console.
- NNMi can use trap sources as hints to auto-discovery. This change enables faster discovery and can increase the number of devices that are discovered.
- The definitions of the IpSubnetContainsIpWithNewMac and SNMPAddressNotResponding incidents have been updated in the configuration XML file with unique OID values and with default UCMDB enrichment. Load the updated configurations as described in "Configuration updates for the IpSubnetContainsIpWithNewMac and SNMPAddressNotResponding incidents require loading" in the NNMi 9.0x Release Notes Updates.
- The HP NNMi—HP NA integration synchronizes nodes deleted from the NNMi topology with the NA inventory.
- The `nnmcommload.ovpl` command and the Specific Node Configuration form now include a preferred SNMP version option for setting the preferred SNMP version and load communication settings for SNMPv1 nodes.
- Support for the AES-128 privacy protocol for SNMPv3 communication. Use of the AES-128 privacy protocol requires the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files library. For more information, see the *NNMi Communications* chapter of the NNMi Deployment Reference.
- The HP NNMi—HP UCMDB integration supports launches from NNMi to CI Views in the supported versions of UCMDB 8.x, UCMDB 9.x, and UCMDB embedded in HP BAC 8.x. Specify the product version in the HP UCMDB Version field on the HP NNMi-HP UCMDB Integration Configuration form.
- NNMi 9.0x Patch 1 added an option to prefer the IP address in an SNMPv1 trap's UDP header over the contents of the SNMPv1 trap's agent_addr field. To use this option, see "06/25/2010: NNMi 9.0x Patch 1 adds an option for SNMPv1 trap handling preferences" in the NNMi 9.0x Release Notes Updates.

- Documentation Changes
  - The NNMi Deployment Reference has been split into two volumes. The NNMi Upgrade Reference contains the content that was previously in the "Upgrading from NNM 6.x/7.x" section of the NNMi Deployment Reference.

NNMi 9.00

- Upgrade Notes
  - For important notes about upgrading from NNMi 8.1x to NNMi 9.00, see the NNMi Deployment Reference. Please read these notes before performing the upgrade.
- Changes to Supported Environments
  - Support for Windows Server 2008
  - Support for Red Hat 5.2 or newer minor version. (Red Hat 4.x no longer supported, you must upgrade to Red Hat 5.2 or later before upgrading to NNMi 9.00.)
  - Support for VMware ESX Server 4.0
  - Support for Internet Explorer 8.0 and Firefox 3.6 (Firefox 2.0 no longer fully supported.)
  - Support for Oracle 11g

- Support for NNMi Application Failover when using an Oracle database
- Support for Veritas Cluster Server for High Availability on Linux
- Global Network Management (GNM) (see Global Network Management)
- IPv6 (see IPv6 Discovery and Monitoring)

- Global Network Management (NNMi Advanced only)
  - Global Network Management (GNM) is the new distributed architecture for NNMi. GNM provides a single consolidated end-to-end view of managed networks from a centralized Global Manager. GNM distributes discovery, monitoring, and trap reception across multiple Regional Managers that are separated geographically.
    - GNM supports hierarchical management by combining data from multiple geographically distributed Regional Managers to be combined into a single Global Manager. Regional Managers can forward information about their management domain to one or two Global Managers.
    - The GNM model of collecting management information (discovery, monitoring, and traps) remotely reduces the use of network bandwidth on WAN links and simplifies management through firewalls.
    - GNM supports increased scale. A standalone NNMi management server can manage up to 25k nodes; a Global Manager can manage up to 65k nodes. For more information, see the *Support Matrix*.
  - Each Regional Manager is a fully functional installation of NNMi.
    - The Regional Manager is responsible for managing the devices in its domain.
    - The Regional Manager handles all SNMP and ICMP communication to the devices it manages.
    - A Regional Manager forwards the following information to Global Managers:
      - Node inventory changes detected by Discovery
      - State changes for any monitored objects
    - The Regional Manager administrator can filter the set of node topology data forwarded to Global Managers.
    - A Regional Manager can forward SNMP traps and remote NNM 6.x/7.x events to Global Managers. This forwarding can be throttled for event storms.
    - Local network management continues if the link between the Global Manager and a Regional Manager goes down.
  - The Global Manager displays the combined network topology data from all connected Regional Managers.
    - The Global Manager Causal Engine determines the status of objects on the Global Manager and generates incidents based on the more comprehensive topology available on the Global Manager.
    - The Nodes by Management Server view provides easy filtering of nodes by Regional Manager source.
    - Node group filter definitions can be based on the Regional Manager Node source.
    - Global Manager administrators can establish secure connections to Regional Managers using SSL.
  - In the Global Manager NNMi console, for a selected node that is managed by a Regional Manager, a user can do the following:
    - Open and sign in to the NNMi console of the Regional Manager
    - Open the Node form provided by the Regional Manager
    - View the current communication and monitoring settings of the node
    - Initiate a configuration poll or status poll that instructs the Regional Manager to update the node information
    - Perform other actions from the Regional Manager (ping, traceroute)
  - When the GNM feature is enabled, the Global Network Management tab of the `Help → System`

`Information` window shows information about the connected Global or Regional Managers.

- When Single Sign-On (SSO) is configured, users can access the Regional Manager without signing in.
- High Availability and NNMi Application Failover are supported for a Global Manager, for a Regional Manager, or both. If a Global Manager or a Regional Manager fails, NNMi establishes a new GNM connection with the standby node when it becomes active.
- (NNM iSPI for Metrics only) State Poller metrics exported to the NNM iSPI for Metrics are propagated to the Global Manager to for consolidated performance reports.

- IPv6 Discovery and Monitoring (NNMi Advanced only, UNIX operating systems only)
  - Enable, disable, and configure IPv6 management in the `nms-jboss.properties` file (see the NNMi Deployment Reference)
  - IPv6 inventory discovery, monitoring, and trap reception for IPv6-only and IPv4/IPv6 dual-stacked devices:
    - IPv6 Addresses (global unicast and link local), associated nodes and associated interfaces
    - IPv6 subnets, associated addresses
  - Native IPv6 SNMP communication for the following:
    - Node discovery
    - Interface monitoring
    - Trap/inform reception and forwarding
    - Automatic selection of IPv4 or IPv6 SNMP communication (management address) for dual-stacked devices
    - Configurable preference – IPv4, IPv6, or no preference
  - Native ICMPv6 communication for IPv6 Address fault monitoring
  - Seeded device discovery with IPv6 address or hostname
  - IPv6 device discovery through:
    - IPv6 Layer 3 neighbor discovery hints
    - Layer 2 neighbor discovery hints with LLDP IPv6 neighbor information
  - Layer 2 connectivity for IPv6 devices
  - Consolidated presentation of IPv4 and IPv6 information
    - Inventory views for nodes, interfaces, addresses, subnets and associations
    - Layer 2 and Layer 3 neighbor views and topology maps for IPv4 and IPv6 devices
    - Incidents, conclusions, root-cause analysis
  - Actions in the NNMi console: ping and traceroute for IPv6 addresses and nodes
  - NNMi configuration using IPv6 addresses and ranges:
    - Communication Configuration
    - Discovery Configuration
    - Monitoring Configuration
    - Node Groups
    - Interface Groups
    - Incident Configuration
  - SDK web services support IPv6 inventory and incidents

NNM iSPI for Metrics support for IPv6 interfaces

- Management of Virtualized Servers (NNMi Advanced only)
  - VMware ESX Server and Virtual Machine Capability discovery
  - Capabilities added to nodes for virtualization
    - An ESX server node has a "VMware ESX Host" capability.
    - A VM node running on that ESX server node has a "Virtual Machine" capability.
  - Predefined node groups enable viewing of "VMware ESX Hosts" and "Virtual Machines".
  - `Tools → Find Attached Switch Port` can find virtual machines using the virtual machine's hostname, IP address, or MAC address.
- MPLS WAN (NNMi Advanced only, requires HP Route Analytics Management Software (RAMS) 9.00 integration)
  - Provides discovery and visualization of MPLS WAN Clouds and connections of CEs to the WAN cloud.
  - Requires configuration of a RAMS server (in the RAMS Server view in the Configuration workspace).
  - Enabled with the HP RAMS MPLS WAN Configuration form in the Integration Module Configuration workspace.
  - Inventory view of MPLS WAN Clouds (RAMS).
  - MPLS WAN objects list the MPLS WAN connections, including the CE interface, CE IP address, and PE IP address.
  - Map views are available for MPLS WAN objects.
- Cards and Ports
  - Discovery now automatically discovers cards, daughter cards, and card redundancy groups (Redundant Cisco Supervisor Engines), as well as the ports on each card.
  - Inventory views of cards, ports, and card redundancy groups
  - Fault monitoring of cards
    - Support for management mode on cards
    - Root cause analysis of failures on cards and card redundancy groups
  - Processing of card traps
  - Analysis of card insertion and removal (Cisco only)
- Events
  - Incident configuration for suppression, enrichment, dampening, and lifecyle transition actions can be customized to interface groups, node groups, or both. Each incident configuration can also have default configurations in these areas that apply when the incident source does not match any of the specified interface or node groups.
  - Incident Suppression, Enrichment, and Dampening:
    - Suppression of an incident means that the incident is dropped and not persisted to the database.
    - Enrichment of an incident alters an incident before it is persisted to the database. Enrichment can modify one or all of the following:
      - Message format
      - Severity
      - Priority
      - Category
      - Family

        - Incident owner
        - Correlation nature
        - Custom incident attributes
    - Dampening of an incident delays the running of lifecycle transition actions. notification through the SDK, and the running of diagnostic flows until the incident goes to an undampened state. Incident dampening is useful for cases where, for example, an interface is flapping (downs then ups) repeatedly, and actions are run repeatedly for each down episode.
    - Incident payload filtering is also supported for suppression, enrichment, dampening, and lifecycle transition actions.
    - The `Actions → Incident Configuration Reports` menu items are useful for testing these incident configuration features.
  - User interface improvements
    - All tables in the incident configuration forms can be filtered and sorted on any column. These tables can be shown in a new window to show more columns at a time.
    - You do not need to save the top-level Incident Configuration form for changes to take effect.
    - All node, interface, and IP address menu items are available on the incident's `Actions` menu.
    - Administrators can use `Actions → Open Incident Configuration` on an Incident form to open the incident configuration form for that incident type.
  - Incident actions are now run by the nnmaction process. This change improves performance and increases the number of actions that can be run simultaneously. See the *nnmaction* reference page for more information.
  - Incidents can have a "Rate Stream Correlation" or "Dedup Steam Correlation" correlation nature. These two more specific correlation natures are used instead of the 8.x "Stream Correlation" nature. The "Rate Stream Correlation" nature is included in the Key Incident views. The "Dedup Stream Correlation" nature is not included in the Key Incident views.
  - `Tools → Incident Actions Log` displays the contents of the actions log.
  - When the NNMi Causal Engine closes an incident, NNMi adds the following information to the incident correlation notes and as CIAs:
    - Reason closed
    - Length of time the incident was outstanding
    - Time the incident was detected
    - Time the incident was resolved
  - Incident configuration includes an option to display traps received from nodes that are not in the NNMi topology.
  - Incident configurations can be enabled or disabled while being loaded from MIB files. See the *nnmincidentcfg.ovpl* reference page for more information.
- Custom Correlation
  - The Custom Correlation feature enables the creation of new incident correlations of multiple child incidents under an existing incident or a new parent incident.
  - Enabled with the Custom Correlation Configuration form in the Configuration workspace:
    - Incident filtering and correlation logic can be based on incident CIA values as well as the attribute values of the source node or source object of the participating incidents.
  - NNMi provides a sample Custom Correlation for correlating sub-interface down incidents under the main interface down incident (for Cisco devices)
- Northbound Interface Integration

- The NNMi northbound interface integration module forwards NNMi incidents and other event notifications to registered trap receivers as SNMPv2c traps. In this manner, an external integration (for example, an event consolidator) can consume the NNMi event stream.
- Enabled with the HP NNMi-Northbound Interface Destination form in the Integration Module Configuration workspace.
- The northbound interface can send the following information:
  - Incidents:
    - Management events
    - SNMP traps (SNMPv1, v2c, and v3)
  - Lifecycle state change notifications (for example, incident closed)
  - Deletion notifications
  - Correlation notifications
- The northbound interface can send traps to multiple destinations.
- See the NNMi Deployment Reference for more information about the northbound interface.

- MIB Expressions
  - Custom MIB expressions consist of one or more MIB variables and arithmetic operators that define the SNMP information that NNMi polls (Custom Poller) or graphs (Real-Time Line Graphs).
  - The MIB expression editor is a graphical tool for creating MIB expressions from the MIB variables loaded into the NNMi database. See *MIB Expression Example* in the NNMi help for an example of creating a MIB expression using this editor.
  - The MIB Expression view in the Configuration workspace shows both custom MIB expressions and the many MIB expressions provided by NNMi.
  - Use `Actions → Graph MIB Expression` from the MIB Expression form to test the expression.
- MIB Browser and MIBs
  - New SNMP MIB browser:
    - The tree control includes expand all, collapse all, and find operations.
    - SNMP data appears in a table format.
    - Lists of OID aliases facilitate walking common MIBs.
    - Copy selected rows to the clipboard.
    - Show more information about a MIB variable.
    - Print MIB information.
    - Available with `Tools → MIB Browser` or from a selected node or MIB Variable with `Action → Browse MIB`.
  - Show the MIBs that a node supports:
    - `Actions → List Supported MIBs` in the NNMi console
    - `Tools → List Supported MIBs` in the MIB browser
  - Load MIBs from the NNMi console with `Tools → Load MIB`:
    - List the MIBs loaded into the NNMi database as well as MIBs that are available in the `snmp-mibs` or the `user-snmp-mibs` directory but are not yet loaded.
    - If a MIB supports the TRAP-TYPE or NOTIFICATION-TYPE macro, load SNMP trap incident configurations from the MIB file.
    - Upload MIB files to the `user-snmp-mibs` directory on the NNMi management server.

- Use loaded MIB information in MIB expressions and for mnemonic display in the MIB browser.
- More MIB information available:
  - NNMi installation loads more than 140 MIBs.
  - From the Loaded MIBs table view in the Configuration workspace open a MIB to see the MIB variables, syntax, and description.
  - MIB Variables table view in the Inventory workspace shows all loaded MIB variables.
  - `Actions → Display MIB File` shows the MIB text file.

- Real-Time SNMP Line Graphs
  - Line graphs show real-time SNMP data for the selected nodes and interfaces.
    - MIB expressions define the SNMP data to graph.
    - A graph can show multiple instance SNMP MIB variables for a node.
  - Line graph user interface:
    - Select the lines to graph.
    - Select the visible time segment.
    - Adjust the polling interval.
    - Lock the Y-axis to prevent changes while scrolling.
    - Print a graph.
  - Define line graphs with the SNMP Line Graph form as menu item actions.
  - Instance label algorithms include:
    - Query another MIB variable for a label
    - Numeric
    - Alphabetic
    - Interface name
    - Interface name indirect
  - The Default Line Graph Settings tab on the User Interface Configuration form provides for setting default graph behavior.
  - Start line graphs in a variety of ways:
    - The `Actions → Graphs` menu provides many default NNMi graphs. This menu lists the graphs available based on the capabilities of the selected objects.
    - Start graphs from a Custom Poller incident or a Custom Polled instance.
    - Embed URLs that start graphs in custom web pages and applications. For URL syntax, see `Help → NNMi Documentation Library → Integrate NNMi Elsewhere with URLs`.
  - SNMP line graphs fall back to low capacity MIB-II interface counters (interfaces MIB) if the high capacity counter (ifMIB MIB) is not available.

- Custom Poller
  - Custom Poller supports user-defined MIB expressions.
  - Custom Poller collected metrics can be exported to comma separated values (CSV) files that provide access to the raw metrics.
    - To save disk space, you can compress the contents of these CSV files.
    - See the *Maintaining NNMi* chapter of the NNMi Deployment Reference for more information.

- Detailed Custom Poller statistics are available on the Custom Poller tab of the `Help → System Information` window.
- (NNM iSPI for Metrics only) Custom Poller can be configured to export specific groups of collections to the NNM iSPI for Metrics for reporting.

- State Poller
  - State Poller can be configured to ICMP ping the management address only.
  - Users can starts a Status Poll from an interface, IP address, node component, or card object.
  - Management Mode support added for node components. A specific node component (for example, a fan) can be unmanaged so that it does not affect node status.
  - Detailed State Poller statistics are available on the State Poller tab of the `Help → System Information` window.
- SNMP
  - Communication Configuration
    - Changes to Communication Configuration are now dynamic and take effect quickly.
    - Communication Configuration includes the Enable SNMP GetBulk flag for disabling the use of SNMP GetBulk queries in environments where SNMP Agents do not properly respond to SNMP GetBulk requests.
    - The SNMP write community string can be included in the Communication Configuration for use by the `nnmsnmpset.ovpl` command.
  - SNMP Commands
    - Improved performance of `nnmsnmp*.ovpl` command line tools.
    - Removed web services dependency.
    - SNMP packet debug available in the `nnmsnmp*.ovpl` command line tools with the `-d` option.
  - Support for Global Network Management
    When a Regional Manager manages a node, the following behaviors apply:
    - SNMP requests are forwarded to the appropriate Regional Manager station.
    - Command line tools send requests to the appropriate Regional Manager.
    - `Actions → Communication Settings` displays the configuration from the appropriate Regional Manager.
    - Real-time line graphs perform the SNMP queries from the appropriate Regional Manager.
  - SNMP Stack
    - Improved performance and reduced memory footprint for the SNMP stack, including a new NIO-based implementation.
    - The SNMP stack by default reduces to 3 the number of simultaneous SNMP requests to a node (to reduce the risk of SNMP Agents dropping responses).
    - SNMP version rediscovery is performed if the SNMP stack is no longer able to communicate using the previously used version of SNMP.
    - `Actions → Configuration Poll` rediscovers the SNMP versions for a node (to enable moving between versions based on configuration).
    - Table handler checks for looping agents and duplicate requests.
    - Improved SNMPv3 engine parameter discovery and caching.
    - Added SNMP Health Report.
  - SNMP Traps

    - SNMP Trap Forwarding configuration has its own form in the Configuration workspace.
    - Support for the RFC 3584 varbinds specified for proxy forwarding of SNMP traps, including the snmpTrapAddress and snmpTrapCommunity varbinds. If the snmpTrapAddress varbind is set in an incoming trap, this value is used as the source address for the trap. Only IPv4 addresses are supported. If the snmpTrapCommunity varbind is set, this value is used as the community string for the trap.
  - The `Actions → Communication Settings` window now shows the configuration used for each of the active agent settings.
- Discovery
  - Interfaces can be excluded from discovery on the Discovery Configuration form.
  - Command line tool to rediscover nodes. See the *nnmnoderediscover.ovpl* reference page.
  - Command line tool to delete nodes. See the *nnmnodedelete.ovpl* reference page.
  - Node names and hostnames can be forced to lowercase or uppercase to make searching easier. See the *Maintaining NNMi* chapter of the NNMi Deployment Reference for more information.
- Node and Interface Groups
  - Node group configuration includes a Calculate Status check box to improve performance by only calculating status when user specified.
  - Filtering
    - New filter attributes for node group additional filters, interface group additional filters, and menu item enablement filters:
      - devCategoryNode
      - devCategoryInterface
      - devVendorNode
      - devVendorInterface
      - devFamilyNode
      - devFamilyInterface
      - isSnmpNode
      - isSnmpInterface
      - sysOidNode
      - sysOidInterface
      - isNnmSystemLocal
      - nnmSystemName
    - More powerful additional filters for node group additional filters, interface group additional filters, and menu item enablement filters. The NOT and EXISTS operators enable more powerful combinations of multiple custom attributes that might not exist. See the NNMi help for more information.
    - Filter controls have drag and drop editing.
    - Interface group filters enable finding impacted VLANs, physical address, and duplex mode.
  - Commands
    - You can define node groups from a .csv file based on attributes and capabilities, which enables the creation of location-based node groups. See the *nnmloadnodegroups.ovpl* reference page for more information.
    - You can set custom attributes can be set in bulk on interfaces and nodes. See the *nnmloadattributes.ovpl* and *nnmdeleteattributes.ovpl* reference pages for more information.

Note: These commands deprecate the `nnmnetloadnodeattrs.ovpl` and `nnmnetdeletenodeattrs.ovpl` commands.

- User Interface
  - Menus
    - Menu items can be placed on the items can be added to the Tools, Actions, and Help menus and their submenus.
    - All menu items can be selectively disabled by the administrator. Entire submenus (such as a Graph submenu) can be disabled.
    - The minimum required role can be changed for any menu item.
    - Menu items that will be unavailable when a temporary or instant-on demonstration license expires now include the text "(Evaluation)".
    - See the Menus and Menu Items tabs on the User Interface Configuration form in the Configuration workspace.
  - Map Views
    - Find in Map functionality. A Find button is available on all map views.
    - Map views have toolbar buttons and keyboard accelerators to zoom in (+), zoom out (-), fit (=), or show symbols as full size (1).
    - Multiple connections between nodes or node groups are collapsed into one multiconnection on the map.
      - Double-click a multiconnection to expand the connections.
      - The minimum number of redundant connections for collapse can be configured per saved node group map or globally.
    - Map views display family-specific icons for HP ProCurve and Cisco device families.
  - Table View Filtering Improvements
    - Can filter on enumerated types.
    - Can select multiple enumerated types at one time.
    - The Apply button gives quick feedback on the results of the filter.
    - Can filter on IP Addresses or timestamps as ranges.
  - Miscellaneous
    - The Monitoring, Management Mode, and Incident Browsing workspaces are simpler (because views can be easily filtered, multiple permutations of views are not required in these workspaces).
    - Performance improvement for large tables.
      When the table filter is not specific enough and too many rows would be returned, the size of the returned table is limited to a smaller size. The status at the bottom of the table and the count of the table indicate that the table is limited and that a more restrictive column filter should be applied.
    - Updated look and feel, including new sign-in and welcome pages.
    - Merged user account, principal, menu, and menu item configuration onto the User Interface Configuration form.
    - Multiple menus, menu items, correlation rules, or incident configurations can be enabled or disabled at one time.
    - Secure HTTP console access is enabled by default.
      - Secure HTTP access to the console is available with `https://machine:port/nnm`.
      - To disable non-secure HTTP, use a firewall to block the HTTP port.
      - For information about forcing a redirect from HTTP URLs to HTTPS URLs, see the *Maintaining*

NNMi chapter of the NNMi Deployment Reference.

- Improved Router Redundancy form navigation, including a Router Redundancy tab on Node forms.
- Added VLAN ID and VLAN Name to the Find Attached Switch Port and Show Attached End Nodes tools.
- URLs to the NNMi console can include objects identified by custom attribute values.

- NNMi Self-Monitoring
  - New `Help → System Information` window.
  - NNMi performs more self-monitoring checks (including memory, CPU, and disk resources), and generates an incident when the system is low on resources or when NNMi detects some other serious condition.
    - This health information is available on the Health tab of the `Help → System Information` window or through a detailed self-monitoring report available with `Tools → NNMi System Health Report`.
    - The health report can also be generated with the `nnmhealth.ovpl` command.
    - A status message is displayed at the bottom of the NNMi console when an NNMi self-monitoring health exception is detected. For information about disabling these messages, see the *Maintaining NNMi* chapter of the NNMi Deployment Reference.
  - `Tools → Signed In Users` displays the currently signed-in users.
  - `Tools → NNMi Self-Monitoring Graphs` adds menu items for graphing NNMi communication and discovery progress.
- General
  - `Tools → Status Distribution Graphs` adds menu items for graphing the status distribution of objects.
  - Author field for configuration objects:
    - The Author field must be non-empty when modifying a configuration the includes Author field. If the author is Hewlett-Packard, you must change the author before saving.
    - The default author value for creating new configuration objects is configurable.
  - `Actions → Show Attached End Nodes` and `Tools → Find Attached Switch Port` no longer require the NNM iSPI NET license.
  - Licensing information (available from the Product tab of the `Help → System Information` window) provides a breakdown of the NNM iSPI points consumed by each NNM iSPI licensed through points.
- NNM iSPI NET (requires an NNM iSPI NET license, see Licensing)
  - Trap Analytics
    - Reports and graphs that visualize the total, recent, and real-time sources of traps using NNMi Trap Analytics are available with `Tools → Trap Analytics`.
    - Trap Analytics log file is accessible on the client with `Tools → Trap Analytics → Trap Analysis Log`.
  - Visio Export of Map Views
    - Export of current map or all node group maps to a Microsoft Visio file with the following menu items:
      - `Tools → Visio Export → Current Map`
      - `Tools → Visio Export → Saved Node Group Maps`

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, "9.00" 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 Acrobat Reader must be installed on your system. To download Adobe Acrobat 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.

NNMi Deployment Reference

The HP Network Node Manager i Software Deployment Reference is a web-only document providing advanced deployment, configuration, maintenance, integration, and upgrade from NNMi 8.x information. To obtain a copy of the most current version, go to h20230.www2.hp.com/selfsolve/manuals.

NNMi Upgrade Reference

The HP Network Node Manager i Software Upgrade Reference is a web-only document providing information for 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.

Documentation Errata

No documentation errata.

NNMi Installation Guide and Support Matrix

To obtain an electronic copy of the most current version of the HP Network Node Manager i Software Installation Guide, go 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 is available from the NNMi console with `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 60-day/250-node license. This license also temporarily enables the NNMi Advanced features and the NNM iSPI Network Engineering Toolset Software for the 60-day trial period. The additional features available with each license are listed below.

To check the validity of your NNMi licenses, in the NNMi console click `Help → System Information`, and then click View Licensing Information. Compare the node count with the count displayed in the `Help → System Information` window.

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

HP Network Node Manager i Advanced Software Features

An NNMi Advanced license enables the following features:

- Global Network Management (Global Manager requires an NNMi Advanced license; Regional Managers do not); see Global Network Management
- IPv6 Discovery and Monitoring (Not supported on Windows operating systems); see 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 Node 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 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 and MPLS WAN
- VMware ESX and Virtual Machine Capability Discovery; see Management of Virtualized Servers

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 into 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.
  - Requires installation of the NNM iSPI NET embedded diagnostics server or a previously installed HP Operations Orchestration Central server.
  - For more information, see the Incident Configuration form and the Diagnostics tabs on the Node and Incident forms.
- 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.
  - Detects per-node and per-OID SNMP trap storms.
  - For more information, see the *nnmtrapdump.ovpl* reference page.
- 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.
- Show mismatched connections (Requires HP Network Automation Software)
  - Displays a table of all Layer 2 connections with possible speed or duplex configuration differences.
  - See the *HP Network Automation* chapter of the NNMi Deployment Reference for more details.
- 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

- 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. 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` command or `Actions → Configuration Poll`. For more information, see the *nnmloadseeds.ovpl* and *nnmconfigpoll.ovpl* reference pages.
- If there is a need to use the Specific Node Settings of the Communication Configuration form to add special instructions for a node, there are some complicated factors to consider first. See the *NNMi Discovery* chapter of the NNMi Deployment Reference for more details.
- NNMi relies heavily on Layer 2 connectivity for Layer 2 neighbor maps, root cause analysis (correlating faults that

are in the shadow of other faults), and determining which interfaces to monitor.
NNMi requires that the node on the far side of a Layer 2 connection support SNMP for computing 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 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 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. 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:
     - Value name: InheritConsoleHandles
     - Data type: REG_DWORD
     - Radix: Decimal
     - Value data: 1
  5. Quit the Windows 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 form, and then reload the incident with the `nnmincidentcfg.ovpl` command.
- Cross-launch to NNM 7.x using an NNMi "Management Station" object requires the use of a specific version of the Java Plug-in, which depends on the NNM version and operating system. Review the latest release notes for your version of NNM, and then download and install the correct Java Plug-in version to all web browsers from which NNMi console users will launch NNM Dynamic Views.
- HP-UX systems that are not running the required set of patches might hang when the system starts running low on memory in very large environments. See the *Support Matrix* for a list of HP-UX required patches.
- In Auto-Discovery mode, NNMi discovery ignores a node with empty ipAddrTable (RFC1213-MIB) that is NOT seeded explicitly. The workaround is to load missing nodes due to empty ipAddrTable as seeds.
- In forms with 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 on saving the form.
- In neighbor views, when you enter a Node Name in the auto-complete field, if you press return before the list displays, the view might close.
- If devices do not respond with required SNMP MIB values, NNMi discovery might not find nodes, Layer 2 connections, or VLANs. See "Supported Devices" in the *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. To disable the Linux firewall, use `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 NNMi web server port as defined by the `jboss.http.port` value in the `$NnmDataDir/conf/nnm/props/nms-local.properties` file.

- 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 uppercase letters in a user name against case insensitive directory server, incident assignment and the My Incidents view do not work when the case sensitivity differs between what is returned from the directory service and the name with which you signed in. Sign in using the same case as shown when you perform Assign Incidents.
- 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.
- Attempting to delete a collection or policy with a large number of 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 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...
     - 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.
     - 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, edit the associated node group to remove nodes from the group, which will result in custom node collections and their polled instances being 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.
- If you are browsing between multiple NNMi installations, edit the `%NnmDataDir%\shared\nnm\conf\lwssofmconf.xml` (Windows) or `$NnmDataDir/shared/nnm/conf/lwssofmconf.xml` (Unix) file in one of the following ways:
  - Disable Single Sign-On by setting `enableLWSSOFramework="false"`.
  - Configure Single Sign-On by ensuring that the `initString` and `domain` parameters are the same across all systems. Then restart jboss.

  Otherwise, browsing to a second NNMi installation will sign you out of the previous NNMi installation when you return to the first system. See the *lwssofmconf.xml* reference page.
- (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 NNMi database directory (on Windows Server 2003, `C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\databases`; or on Windows Server 2008, `C:\ProgramData\HP\HP BTO Software\databases`).
- Some multi-level objects (such as Node Groups and Custom Poller Configuration) cannot be saved a second time once invalid fields are reported. For these forms, please close the form and all parent forms, then re-enter the

offending value.

- The `Query Password` field of a RAMS configuration will only be valid when imported into the same NNMi installation on the same system. If imported into a different system, the `Query Password` will need to be re-entered.
- On Linux, if you are using IPv6 and forwarding NNM 6.x/7.x events, ovjboss communication with PMD can be lost, due to the way gethostbyname() returns IPv6 tunneled IPv4 addresses when "options inet6" is specified in `/etc/resolv.conf`. The workaround is to remove the `options inet6` option from `/etc/resolv.conf`.
- Incorrect browser proxy settings with non-DNS hostname can prevent sign in. 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 the entry to local system hosts file. For example “192.168.0.100 myhost.mycompany.com”. This hostname is not resolvable by DNS server. If the browser is configured with HTTP proxy, the browser will ignore the hosts file for NNMi hostname resolution, and will use the proxy for NNMi hostname resolution. Since DNS cannot resolve the NNMi hostname, NNMi console sign in will fail. To resolve this problem, the user should either disable proxy setting or add Exceptions to browser proxy settings. To Add Exceptions to browser proxy settings:
  Internet Explorer:
  Internet Options → Connections tab, click "LAN Settings".
  If the "Proxy Server" is configured, click "Advanced", and add non-DNS NNMi hostname into Proxy Settings Exceptions.
  Firefox:
  Options → Network tab
  Check "Connection → Settings". If the Proxy is configured, please add non-DNS NNMI hostname into "No Proxy for" list.
- There may be no status for nodes with down Interfaces. If the active IP Address that responds to SNMP communication is on an 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 will be a node with valid system information and Device Profile, but no SNMP Agent. A configuration poll will resolve the problem.
- The Action server can hang if a configured action script prints a lot of output to stdout or stderr. The workaround is to change your action scripts to redirect output to a file rather than stdout or stderr.
- (Windows only) The `nnmcertmerge.ovpl -directory` command does not work correctly when the specified directory path includes spaces. The workaround is to place the `nnm.keystore` and `nnm.truststore` files in a directory path, such as `C:\Temp`, that does not contain any spaces.

Potential Installation Issues

- See installation prerequisites in the NNMi Installation Reference and *Support Matrix* for complete instructions.
- In addition to the web server port, the NNMi server uses several ports for process communication as documented in the *NNMi 9.00 and Well-Known Port Availability* appendix of the NNMi 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 login technology such as Remote Desktop Connection, verify that you are accessing the Windows console and not a secondary connection.
- Installation using symlinks on Solaris:
  On Solaris, to install onto a file system other than `/opt/OV` and `/var/opt/OV`, you can create these directories as symlinks to some other directory. In this case, the Solaris `pkgadd` command requires that the following environment variable is set:
  ```
  PKG_NONABI_SYMLINKS="true"
  ```
- 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 posgresql off`.
- NNMi supports Single Sign-On (for use with NNM iSPIs).
  - 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 NNMi Deployment Reference.

- Issue with Silent Install on Windows (specifically, non-English locales):
For silent installation on a target system, the NNMi Installation Reference says to run an installation using the user interface on another system. This approach 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. If this file was generated on non-English locale machine (for example: Japanese, 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. Therefore, it is recommended to use Wordpad (or some other editor) instead of Notepad to modify the `ovinstallparams.ini file.`
- (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 8.x 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 *Configuring NNMi in a High Availability Cluster* chapter of the NNMi Deployment Reference.
- If you have NNM iSPIs installed on the NNMi management server, 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 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 user's browsers are configured to trust. For more information, see the *Working with Certificates for NNMi* chapter of the NNMi Deployment Reference.
- (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. If this permission were "2750", all subdirectories below `/var/opt` or `/opt` would also be 2750, which would mean that world read-access has been stripped. Some processes run as non-root user (the database, the action process, and so forth). These processes need read access to files below `/opt/OV` and `/var/opt/OV`. If the inherited directory permission strips world read, these processes will fail.
- (High Availability only) If you run `nnmhaconfigure.ovpl` to configure the secondary node for HA, the FQDN of the virtual hostname is queried using OS-specific HA commands, and the `NnmDataDir/conf/nnm/props/nms-local.properties` is updated to include this new FQDN. One of the fields in this nms-local.properties file is `com.hp.ov.nms.ssl.KEY_ALIAS`. The value of that variable is set to "<FQDN>.selfsigned.". If the FQDN happens to have a newline character in the name, then this one line ends up being split into two lines. The fix is to edit the file and join the two lines into one.

Internet Explorer Browser Known Problems

- The telnet:// URL is not enabled by default with Internet Explorer. See the NNMi Deployment Reference for instructions on how to enable telnet protocol, which requires a registry change on each web client. 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.

- Internet Explorer tracks long running JavaScript operations, and displays a "This page contains a script which is taking an unusually long time to finish" dialog 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 windows 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.

- 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:

  1. 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 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.

- If Integration URLs are rendered inside of a <frame> tag on a page which uses Internet Explorer "Quirks mode", a

JavaScript error will occur.

- In Internet Explorer, URLs should not be launched in Quirks mode. Quirks Document mode is not at all standards compliant and NNMi doesn't support it at this time.
- This may 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 picked to enable standards document mode. For example, this DOCTYPE should NOT be used in a web page which has a frame that references an NNMi Integration URL:
  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
  Instead 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">
- Internet Explorer's Developer Tools are useful for seeing and changing the browser and document mode.

Mozilla Firefox Browser Known Problems

- The telnet:// URL is not enabled by default with Firefox. See the NNMi Deployment Reference for instructions on how to enable telnet protocol, which requires configuring a telnet application on each web client.
- Firefox by default opens windows in a new tab instead of a new window. This can cause NNMi to open windows which do not pop to the foreground. To remedy:
  Under Tools → Options... | Tabs
  set "New pages should be opened in:", check "a new window".
  check "When I open a link in a new tab, switch to it immediately"
  This affects web pages that use "_blank" as a target, such as some help content
- 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 enabled. These 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 NNM 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
- Firefox may incorrectly indicate that a request is still in progress while using the MIB Browser or Real Time Line Grapher, 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 server. Please see Bugzilla defect #383811 at https://bugzilla.mozilla.org/show_bug.cgi?id=383811 for more information.
- Using the "F5" refresh will cause a corrupt display of the form. To refresh a form, please use the "Refresh" toolbar button on the form.
- If you have previously created an Account and later delete and recreate it, Firefox's autocomplete will fill in the

password field for you, without notifying the UI, 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.
- 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 to browse an Asian language NNM 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.
- (NNM 6.x/7.x integration only) Non-applet-based views, such as the NNM 6.x/7.x SNMP Data Presenter, SNMP MIB 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.
- 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". Please read Microsoft document at support.microsoft.com/kb/925261 for details.
- The ovjboss process does not run correctly on HP-UX systems with a Turkish locale (e.g. LC_ALL=tr_TR.iso8859-9). For these systems running the Turkish locale, start NNMi processes with the C locale, e.g. `LC_ALL=C ovstart`

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` and view the topic *Discovering Your Network → Prerequisites for Discovery.*

IPv6 Known Problems

- IPv6 features are not supported on any Windows operating system.
- 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 Sweeper for Auto-discovery
  - IPv6 Address Fault monitoring via SNMP (not available for IPv4 Addresses either)
  - IPv6 Link Local Address fault monitoring, or as discovery seeds / hints

Device Support Known Limitations

- Device Support known limitations can be found in the NNMi Device Support Matrix at sg-pro-ovweb.austin.hp.com/nnm/NNM9.00/devicematrix.htm.

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.

Copyright Notices

Trademark Notices

Acrobat® is a trademark of Adobe Systems Incorporated.

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 Technology — Notice of Restricted Rights

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)

This product includes software developed by The Legion of The Bouncy Castle. (http://www.bouncycastle.org)

This product contains software developed by Trantor Standard Systems Inc. (http://www.trantor.ca)