HP Network Node Manager i Software Release Notes

Software Version: 9.10 / 09 March 2011

This document provides an overview of the changes made to HP Network Node Manager i Software (NNMi) version 9.10.
It contains important information not included in the manuals or in online help.

For the latest additions to these Release Notes, see sg-pro-ovweb.austin.hp.com/nnm/NNM9.10/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/NNM9.10/devicematrix.htm.

What's New In This Version

Overview of the NNMi 9.10 Release

NNMi is a major modernization of the NNM 7.xx software. This release contains many new features. Direct single system upgrades of existing NNM 6.xx or 7.xx installations to NNMi are not supported (see the Upgrade Reference). Single system upgrades of NNMi 9.0x to NNMi 9.10 are supported (see the Deployment Reference). NNMi 8.xx installations must be upgraded to NNMi 9.0x before being upgraded to NNMi 9.10.

For an overview of NNMi 9.10, see *Introducing HP Network Node Manager* in the Installation Guide (see Installation Guide and Support Matrix).

NNMi 9.10

- Upgrade Notes
  - For important notes about upgrading from NNMi 9.0x to NNMi 9.10, see the Deployment Reference. Also read these notes before performing the upgrade.
  - Web browser bookmarks for accessing the NNMi console in the format `http://<fully_qualified_domain_name>:<port>/nnm/welcome.jsp` no longer work. All NNMi console users should update their bookmarks to the supported URL format of `http://<fully_qualified_domain_name>:<port>/nnm/`.
  - During the upgrade, NNMi users are assigned to one of five special predefined NNMi user groups, depending

on their previous role. These user groups define access to NNMi itself. Upon completion of the upgrade, all NNMi users are linked to the Default Security Group, which provides access to all nodes in the NNMi topology.

- The minimal refresh rate for the Network Overview map has been increased from 3 seconds to 4 minutes, so that it does not refresh as often after restarting ovjboss.
- In NNMi 9.0x, the NNMi Application Failover feature supported a UDP solution where cluster hosts were automatically discovered on the network. Beginning with NNMi 9.10, HP eliminated the UDP solution and only supports the TCP solution. For more information on configuring Application Failover and especially if you are upgrading a system that currently uses UDP for Application Failover, see *Configuring NNMi for Application Failover* in the Deployment Reference.
- Upgrading high availability (HA) clusters from NNMi 9.0x to NNMi 9.10 while keeping the clusters under HA configuration is supported. For more information, see *Configuring NNMi in a High Availability Cluster* in the Deployment Reference.
- Beginning with NNMi 9.10, the *NNMi Integration Enablement* license is obsolete and is not needed for run-time use of the NNMi Web Services. The *NNMi Developer* license is still required for Web Services SDK development.

- Changes to Supported Environments
  - Adds support of SUSE Linux.
  - Adds support of Oracle Solaris Zones.
  - Adds support of ESX 4.0 and ESXi 4.1.
  - Adds support of Microsoft Hyper-V R2.
  - Adds support of Red Hat Cluster Suite.
  - HP Serviceguard on Linux is no longer supported.
  - Microsoft Windows 2003 is no longer supported.
  - Internet Explorer 7 is no longer supported.
- Documentation Changes
  - The Deployment Reference has been split into two volumes. The Upgrade Reference contains the content that was previously in the *Upgrading from NNM 6.x/7.x*section of the Deployment Reference.
  - An introductory overview of NNMi is available from **Help → Getting Started with NNMi** in the NNMi console.
  - Access to this release notes document is available from **Help → What's New?** in the NNMi console.
- Security and Multi-Tenancy
  - Object level security provides for fine-grained control of operator access to topology objects and incidents.
  - User Group objects group users and define access to the product. The special NNMi user groups "admin", "level2", "level1", "guest", and "client" define access to the entire product (when no object has been selected).
    - Updated LDAP directory service support to use a Distinguished Name to directly map a directory service group to an NNMi User Group.
  - Security Groups control access rights to objects based on the corresponding node's Security Group assignment and the Security Group to User Group mapping. This same control is used for SNMP queries using the MIB Browser and MIB Grapher.
  - Security Groups affect the visibility of incidents. The Unresolved Incidents security group controls access to incidents without a resolved source node.
    - An incident CIA indicates the tenant associated with an incident.
  - The Security Wizard simplifies the process of configuring User Groups, User Group mappings, Security Groups, and Security Group mappings.

- Tenants divide the topology into separate spaces for managed service providers. Tenants indicate which organization a node belongs to.
  - A tenant can be specified when seeding a node for discovery (with the `nnmloadseeds.ovpl` command or in the NNMi console).
  - Configuration can be done per tenant using node groups.
- Node groups can be defined based on the node's Tenant or Security Group.
- The `nnmsecurity.ovpl` command is multi-functional:
  - Manages User Accounts, User Groups, Security Groups, and Tenants.
  - Reports on the security configuration (also available from **Tools → Security Reports**).
  - The `nnmprincipalconfig.ovpl` command has been deprecated; use `nnmsecurity.ovpl` instead.
- Operators can change their password by using **File → Change Password**.
- Single Sign-On is now configured in the `nms-ui.properties` file. Changes can be made to take effect without restarting ovjboss. See the *nnmssso.ovpl* reference page, or the UNIX® manpage, for more information.
- (*NNM iSPI Performance for Metrics*) Performance reports are filtered based on NNMi security configuration (User Groups and Security Groups). Topology filtering of reports based on tenants is also available.
  - The NNMi administrator can restrict access at the interface level for reporting purposes.
- (*NNMi Advanced*) In a Global Network Management (GNM) deployment, tenants and tenant node assignments are replicated from the regional manager to the global manager.

- State Poller
  - Enhanced ICMP (ping) monitoring of management addresses in networks supports networks using Name Address Translation (NAT) in which the management address may not be an IP address hosted on the node. Note the following about this feature:
    - A new Agent ICMP State that indicates whether a node's management address responds to ICMP is displayed for each node and SNMP Agent.
    - The configuration setting controlling this monitoring is still enabled using the Enable ICMP Management Address Polling check box.
    - The ICMP state of the IP address hosted on the node is only monitored if Enable ICMP Fault Polling is selected.
  - Time-based thresholds provide for thresholds that occur for a specified duration within a sliding period. Thresholds can be configured to be generated when a threshold has been exceeded for X minutes of Y hours.
  - Thresholds on Management Address ICMP Response Time can be configured.
  - For detecting renumbering of interfaces on a device, the Interface Reindexing Type attribute on Device Profile objects has an additional value: ifName or ifDescr or ifAlias.
  - You now can now be alerted if a threshold is above 0 by setting the high threshold value to 0. This functionality is useful when thresholding against errors and discards and it is expected that there should not be any on a properly running network. This capability is also available with Custom Poller.
- Performance Management (***NNM iSPI Performance for Metrics required***)
  - Configurable baseline thresholds, including configuration of number of deviations from normal.
  - Collect and report on many new performance metrics:
    - Interface Metrics
      - Additional interface metrics from the IF MIB
      - Etherlike MIB
      - OLD-CISCO-INTERFACES MIB

        - Wireless LAN MIBs (IEEE802dot11 MIB, CISCO-DOT11-ASSOCIATION MIB)
        - WAN Metrics (DS1/DS3, SONET)
            - Monitoring configuration control over monitoring of DSx and SONET WAN metrics
    - Node Component Metrics
        - Disk space utilization (HOST-RESOURCES MIB)
        - Backplane utilization
            - CISCO-STACK-MIB (Cisco)
            - RAPID-CITY MIB (Nortel)
            - XYLAN-HEALTH-MIB Alcatel)
    - Node availability (SNMP) and node reachability (ICMP)
    - Bad polls. Bad polls fall into the following categories:
        - Unresponsive target
        - Target error (such as SNMP "no such object" error)
        - Invalid data (such as number of packets > number of octets)
- Many new performance thresholds available:
    - Count-based, Time-based, and Baseline Thresholds:
        - Disk Space Utilization
        - Backplane Utilization
        - Management Address ICMP Response Time
        - Buffer Utilization
        - CPU Utilization
        - Memory Utilization
        - Interface Input Utilization
        - Interface Output Utilization
    - Count-based and Time-based Thresholds:
        - FCS Error Rates (LAN, WLAN)
        - Queue Drop Rates
        - Buffer Failure Rate
        - Buffer Miss Rate
        - Buffer Utilization

- User Interface
    - By default, forms open in the NNMi console with breadcrumbs to navigate between previous views and forms.
    - An actions context menu is available when you right-click on one or more table entries or map objects.
    - The Analysis Pane provides additional information on the selected object:
        - Clickable links provide for direct navigation to referenced items.
        - Expandable lists are clickable and show the total number, such as indicating the number of IP Addresses and Interfaces on a Node.
        - The Summary Panel shows an overview of the object.

        - Nodes show in the Summary Panel the total number of Incidents received, along with the first and last time and the frequency with which they were received.
    - The Details tab provides more detailed information about the object.
    - Various Analysis Pane tabs are available depending on the type of object:
        - Topology objects
            - Objects have tabs showing related topology objects (such as the Node and Interface for an IP Address).
            - The Status History tab shows the percentage of time the entity had each status.
            - The Gauges tab shows real-time SNMP gauges to display State Poller and Custom Poller SNMP data.
                - These gauges are displayed for Nodes, Interfaces, Custom Node Collections, Custom Node Instances, and for Node Components of type CPU, MEMORY, BUFFERS, or BACKPLANE.
                - An icon appears at the bottom of each gauge that can be clicked to launch a real-time SNMP line graph for the metric.
                - Double clicking on a gauge opens a window for selecting and copying the tooltip information.
            - The State Poller and Custom Poller tabs show the results of the last collected values.
            - Nodes have a MIB Values tab that displays sysUpTime and ifNumber. Cisco nodes also displays the chassis serial number.
            - Nodes have a Security tab that shows the Security Group and User Groups with access to the Node.
            - Nodes have a Layer 2 Map tab shows the 1-hop neighbors of the selected Node.
            - Layer 2 Connection, Interface, Port, and IP Address have a Connection tab that shows mismatches of speed, duplex, and other settings between two ports.
        - Incidents have tabs that shows Custom Attributes, Parent Incidents, Child Incidents, and Similar Incidents. The Custom Attributes tab shows Textual Conventions values for SNMP varbinds. Tabs show details for the Source Node and Source Object.
        - Node Groups display a pie chart of the status for contained Nodes.
        - User Accounts, User Groups, Security Groups, User Account Mappings, and Security Group Mappings display tabs indicating unused User Accounts, User Groups, or Security Groups.
- A new Initial Discovery Progress map view is the default view immediately after product installation. After more than 100 connectors have been discovered, the Open Key Incidents table view becomes the initial starting view. To change this behavior, change the Initial View parameter on the User Interface Configuration form from Installation Default to the initial view of your choice.
- Incident tables can have color-coded rows. This feature can be enabled using the User Interface Configuration form in the Configuration workspace.
- URLs (http://, https://, ssh://, telnet://, and mailto:) in Notes, Incident fields, Analysis Pane, and descriptions are clickable.
- Operators no longer see the Node Group configuration tab in a Node Form. They only see the Status tab. Only Administrators can see the "Device Filters", "Additional Filters", "Additional Nodes", and "Child Node Groups" tabs.
- Views and Forms in the Configuration workspace are grouped with a tree control.
- CSV Export:
    - Export an entire table (or selected rows) to a comma-separated values file with right-click Export to

CSV.

    - Export to a .csv file from Real-time Line Graphs.
  - Node access menu items:
    - Menu item to launch a web browser to the selected Node, IP Address, or Incident Source Node.
    - New Secure Shell... (from client) menu item requires the configuration of client browsers to respond to the ssh:// protocol. For information on configuring your browser, see *Configuring the Telnet and SSH Protocols for Use by NNMi* in the Deployment Reference.
- SNMP Communication and MIBs
  - Configuration of the SNMP Management Address Selection algorithm in the Communication Configuration form: "Seed IP", "Lowest Loopback IP", "Highest Loopback IP", and Interface matching. By default, the management address is set to the seeded address.
  - Now handles changing the SNMPv3 engine ID on the device.
  - The `nnmsnmpset.ovpl` command now accepts multiple varbinds as arguments.
  - The `nnmcommload.ovpl` command now includes options for setting SNMP enabled, SNMP address discovery enabled, and get bulk enabled.
  - SNMP MIB loading:
    - Improved MIB loading performance.
    - Stricter enforcement of MIB conventions. Invalid MIBs do not load.
    - Support for Textual Conventions: table of Textual Conventions; visible in MIB Browser, command line tools, and Analysis Pane.
    - When loading incidents as traps from a MIB, `nnmincidentcfg.ovpl` no longer has a -loadMib option. First, use `nnmloadmib.ovpl` to load the necessary MIBs before calling `nnmincidentcfg.ovpl -loadTraps`.
- Discovery
  - Discovery takes MAC Addresses into account for the following benefits:
    - Improves support for DHCP or other nodes that change IP addresses.
    - Improves node identity for nodes configured with duplicate IP addresses.
    - Improves support for devices that do not report hosted IP addresses.
  - The `disco.SkipXdpProcessing` configuration file can contain the management addresses of the devices for which NNMi should ignore the Discovery Protocol SNMP tables. This configuration file is especially important for customers who have Enterasys devices in their management domain.
  - The `disco.NoVLANIndexing` configuration file is now fully supported.
- Events and Causal Engine
  - Better dampening defaults for many Management Events.
  - Faster root cause incident generation for Node Down, Interface Down, and Connection Down.
  - Jython version 2.5.1 now supported for event actions.
  - The `trapFilter.conf` file can be used to block traps based on IP address ranges or trap OIDs. The blocking happens before the trap is written to the trap binary store and before it is analyzed for rate, which means that traps blocked by this filter do not affect trap rate calculations and do not appear when using the `nnmtrapdump.ovpl` command.
- Integrations
  - HP SiteScope
    - HP SiteScope trap integration for SiteScope monitor alerts

        - Includes canceling of traps when the alert condition is cleared in SiteScope
    - HP SiteScope System Metrics integration (*NNM iSPI Performance for Metrics* required)
        - Configured through the HP SiteScope System Metrics link in the Integration Module Configuration workspace
        - Reports on HP SiteScope system resource metrics:
            - Memory Utilization
            - CPU Utilization
            - Disk Space
            - Windows Processes
            - UNIX Processes
- HP Network Automation
    - The configuration of the HP NNMi–HP NA integration is now done completely through the HP NA integration module configuration. There is no more need for installing an NA Connector on the NNMi management server.
    - Single sign-on support when cross-launching from NNMi to NA
    - Topology synchronization improvements:
        - More reliable node/device identification between the two products.
        - Nodes discovered by NNMi are added to NA based on Node Group membership.
        - Dynamic real-time synchronization.
        - Periodic full synchronization to recover from failures, outages, failovers, and so on.
        - Load balanced with Spiral Discovery to avoid competing for resources. Paced to avoid excessive load on NNMi.
        - Bi-directional synchronization (NNMi adds nodes to NA, NA hints nodes to NNMi). Previously NA seeded nodes to NNMi; now with hinting, nodes from NA are only discovered by NNMi if they pass the NNMi auto-discovery rules.
        - Node deletion synchronization (NNMi delete -> NA unmanaged, NA delete -> NNMi delete). Previously, nodes deleted in NNMi were also deleted in NA; now they are simply unmanaged in NA.

- General
    - The `nnmnodegroup.ovpl` command lists Node Group names or Nodes in a Node Group.
    - The `nnmhealth.ovpl` command has options for filtering by category and severity level.
    - NNMi Application Failover improvements:
        - Increased network throughput for database file transfers.
        - Detect if certificates have not been properly merged to `nnm.keystore` to support application failover.
        - The `$NnmDataDir/log/nnm/nnmcluster-status.log` file shows the current status of the cluster without the need to invoke `nnmcluster -display`.
        - By default, a full database backup is transferred every 6 hours.
        - The new `com.hp.ov.nms.cluster.autofailover` system property is available in the `nms-cluster.properties` file for disabling automatic failover so that users always initiate a manual failover.

- iSPI NET
    - (*NNM iSPI NET* only) The `nnmooflow.ovpl` command supports integrating HP Operations Orchestration flow definitions into NNMi for running diagnostics based on incidents.

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, or the UNIX manpage.
  - 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, or the UNIX manpage.
  - 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.
  - Discovery of connections for unnumbered interfaces. For more information, see the *UnnumberedNodeGroup.conf* and *UnnumberedSubnets.conf* reference pages, or the UNIX manpages.
  - 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.
  - Support for discovery of ESX and ESXi 4.0.
  - 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 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, "9.10" 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.

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 9.0.x information. To obtain a copy of the most current version, go to h20230.www2.hp.com/selfsolve/manuals.

Upgrade Reference

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

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 → NNMi Documentation Library → Installation Guide**.

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

Licensing

NNMi 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 System Information window.

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

HP Network Node Manager i Advanced Software Features

An NNMi Advanced license enables the following features:

- Global Network Management. (The global manager requires an NNMi Advanced license; regional managers do not.)
- IPv6 Discovery and Monitoring (Not supported on Windows operating systems).
- 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 Performance for Metrics path health report.
- MPLS WAN Clouds (RAMS) view from the Inventory workspace, including map views of the MPLS WAN cloud; see *Using Route Analytics Management Software (RAMS) with NNMi Advanced* in the NNMi help.
- VMware ESX and Virtual Machine Capability Discovery.

HP Network Node Manager iSPI Network Engineering Toolset Software Features

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

- NNM iSPI NET Diagnostics - device diagnostics collection and display.
  - When an incident changes lifecycle state (such as Registered or Closed), NNMi can run diagnostics (flows). The diagnostics results are visible on the Diagnostics tab of an Incident form. A diagnostic flow is an SSH or Telnet session that logs on to a network device and performs commands to extract configuration or troubleshooting information. This automation reduces the time a network engineer spends gathering troubleshooting and diagnostic data.
  - Flows can be run manually by selecting a supported node and clicking **Actions → Run Diagnostics** to store baseline data about that node on the Diagnostics tab of the Node form.
  - 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, or the UNIX manpage.
- 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.
- Command line tool to manage HP Operations Orchestration flow definitions. See the *nnmooflow.ovpl* reference page, or the UNIX manpage, for more information.
- 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 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, or the UNIX manpages.

- 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 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, or the UNIX manpage, 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 (plus (+), minus (-), and equals (=) keys) or toolbar buttons to zoom.

- 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_module>` 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. If the MIB definition for the traps has changed, you need to first use the `nnmloadmib.ovpl` command to reload the MIBs before using `nnmincidentcfg.ovpl` to load the traps.

- 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.

- If devices do not respond with required SNMP MIB values, NNMi discovery might not find nodes, Layer 2

connections, or VLANs. See Supported Network Devices in the NNMi 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 `/var/opt/OV/conf/nnm/props/nms-local.properties` file.

- If using LDAP to access your environment's directory services, you must log on to the NNMi console using the same case sensitivity of users as reported by the directory service. If you use uppercase letters in a user name against a 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 logged on. Log on using the same case as shown when you perform Assign Incidents.

- NNMi application failover on Windows systems:

  - Application failover on the Windows platform can have some intermittent issues with Symantec Endpoint Protection (SEP) software that affect NNMi cluster operations. When the Standby node is attempting to receive the database backup, this operation sometimes fails because SEP is not releasing a file lock in a timely manner. The database file is automatically retransmitted on any failure, and this problem eventually clears itself.

  - When application failover is configured for Windows, system reboots or other issues might cause the psql command to fail, generating dialog boxes to the Windows desktop and the event viewer. These dialog boxes do not affect operation and can be ignored.

- 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 a pattern that does 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 results 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, browsing to a second NNMi installation will log you off from the previous NNMi installation when you return to the first system. To fix this problem, do the following:

  1. Edit the following file:
     - *Windows*: `%NnmDataDir%\shared\nnm\conf\props\nms-ui.properties`
     - *UNIX*: `/var/opt/OV/shared/nnm/conf/props/nms-ui.properties`

     in one of the following ways:
     - Disable Single Sign-On by setting `com.hp.nms.ui.sso.isEnabled="false"`.

    - Configure Single Sign-On by ensuring that the `com.hp.nms.ui.sso.initString` and `domain` parameters are the same across all systems. Both systems must also have clocks that are in sync, and the domains of each system's FQDN must match and be configured in `com.hp.nms.ui.sso.protectedDomains` of `nms-ui.properties`.

2. Run `nnmsso.ovpl -reload`.

- (Windows only) Anti-virus and backup software can interfere with NNMi operation if this software locks files while NNMi is running. Any application that locks files should be configured to exclude the NNMi database directory (on Windows Server 2008, `C:\ProgramData\HP\HP BTO Software\databases`).
- The `Query Password` field of a RAMS configuration is only valid when imported into the same NNMi installation on the same system. If imported into a different system, the `Query Password` must be re-entered.
- 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 user logons to the NNMi console. 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.example.com”. This hostname is not resolvable by the DNS server. If the browser is configured with HTTP proxy, the browser ignores the hosts file for NNMi hostname resolution, and uses the proxy for NNMi hostname resolution. Because DNS cannot resolve the NNMi hostname, NNMi console logon fails. To resolve this problem, the user should either disable the proxy setting or add exceptions to the browser proxy settings. To add exceptions to the browser proxy settings, do the following::
    - Internet Explorer:
        1. On the **Internet Options** → **Connections** tab, click LAN Settings.
        2. If the Proxy Server is configured, click Advanced, and then add the non-DNS NNMi hostname into the Proxy Settings Exceptions list.
    - Firefox:
        1. Click **Tools** → **Options**.
        2. In the Options dialog box, select the Advanced pane.
        3. On the Network tab, under Connection, click Settings. If a proxy is configured, add the non-DNS NNMI hostname into the No Proxy for list.
- There might be no status for nodes with down Interfaces. If the active IP Address that responds to SNMP communication is on a down Interface, it is excluded from the list of candidate Management IP Addresses. If the hint or seed address that was used did respond to SNMP, the result is a node with valid system information and Device Profile, but no SNMP Agent. A configuration poll resolves 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.
- The `nnmbackup.ovpl -scope config` command does not correctly back up the configuration for node sensor policies. (This information is backed up as part of the topology scope.) For an updated configuration file that corrects this problem, contact your support representative.
- If NNMi is integrated with NA and single sign-on, when the NA session times out, the user is also logged out of the NNMi console. NA has a much shorter (30 minute) timeout value than does NNMi.

Potential Installation Issues

- See installation prerequisites in the Installation Guide and *Support Matrix* for complete instructions.

If you are installing a localized version of the product, see the Non-English Locale Known Problems section for additional information.

- In addition to the web server port, the NNMi management server uses several ports for process communication as documented in the *NNMi 9.10 and Well-Known Ports* appendix of the Deployment Reference. Before installing NNMi, verify that these ports are not in use.
- Installation on Windows using Terminal Services:
  NNMi installation only works if you are on the machine console. If you use remote logon technology, such as Remote Desktop Connection, verify that you are accessing the Windows console and not a secondary connection.
- 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 and some integrated products).
  - This technology requires that the NNMi management server be accessed with the official fully-qualified domain name (FQDN). The official FQDN is the hostname used to enable single sign-on between NNMi and NNM iSPIs. The FQDN must be a resolvable DNS name.
  - If the domain name of the installation system is a short domain such as "mycompany" without any dot, you must change a configuration file to prevent automatic sign out from the NNMi console.

  For more information, see the *Using Single Sign-On with NNMi* chapter of the Deployment Reference.
- (Windows only) Silent install on non-English locale Windows systems:
  For silent installation on a target system, the Installation Guide 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 a non-English locale machine (for example: Japanese or Chinese), and if you edit this file in the Notepad editor, Notepad adds 3 bytes at the start of the file to specify the encoding as UTF-8. These 3 bytes cause the subsequent silent installation process to fail. 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 9.0x that is running in an NNMi application failover cluster, see *Configuring NNMi for Application Failover* in the Deployment Reference for detailed instructions on this procedure.
- If you plan to upgrade an earlier version of NNMi 9.0x that is running in a High Availability environment, see the *Configuring NNMi in a High Availability Cluster* chapter of the Deployment Reference for detailed instructions on this procedure.
- 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 Performance for Metrics is an exception to the above uninstall requirement.
- NNMi creates a self-signed certificate during installation. This certificate enables HTTPS access to the NNMi console without additional configuration. Because it is a self-signed certificate, your browser does not automatically trust it, resulting in security prompts when using the NNMi console.
  - With Firefox, you can choose to permanently trust the certificate, and you will not be prompted again.
  - With Internet Explorer, you will be prompted multiple times. There are two ways to prevent these prompts:
    - Import the self-signed certificate into each user's browser.
    - Replace the self-signed certificate with a CA-signed certificate that all users' browsers are configured to trust. For more information, see the *Working with Certificates for NNMi* chapter of the Deployment

Reference.

- (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 fail.

Internet Explorer Browser Known Problems

- The telnet:// and ssh:// URLs are not enabled by default with Internet Explorer. See the *Configuring the Telnet and SSH Protocols for Use by NNMi* chapter in the Deployment Reference for instructions on how to enable the telnet and ssh protocols, which requires a registry change on each web browser client. Without this registry edit, selecting the **Actions → Telnet... (from client)** or Secure Shell... (from client) menu item results in a "The webpage cannot be displayed" message.
- When using Internet Explorer, browser settings determine whether the name of an NNMi view or form displays in the title bar. To configure Internet Explorer to display view and form titles:
  1. In Internet Explorer browser, click Tools, and then click Internet Options.
  2. Navigate to the Security tab, Trusted Sites, Custom Level, Miscellaneous section.
  3. Disable the Allow websites to open windows without address or status bars attribute.
- Internet Explorer tracks long running JavaScript operations, and displays a "This page contains a script which is taking an unusually long time to finish" message if a maximum number of JavaScript statements is exceeded. Complex map operations can exceed this maximum default of 5,000,000. To adjust the maximum time, the HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Styles\MaxScriptStatements 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 might not be properly drawn in an Internet Explorer client, which results in either a blank window or a window in which only labels are visible. No errors are reported. A frequent cause is that 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:
    - Verify that the NNMi management server to which you are connecting is in the appropriate Internet Explorer security zone.
      Ideally, the NNMi management server should be assigned to the Local intranet zone.
      It is preferable to add the NNMi management server to your Trusted sites zone rather than to enable privileges in a more restricted zone.
    - Verify that the Binary and script behaviors permission is enabled for the security zone that includes the NNMi management server (as determined in the previous bullet item):
      1. In Internet Explorer browser, click Tools, and then click Internet Options.
      2. Navigate to the Security tab.
      3. Select the icon corresponding to the zone that includes the NNMi management server.
      4. Click Custom level to open the Security Settings dialog box for the selected zone.
      5. In the Security Settings - _____ Zone dialog box, scroll down to the radio buttons for Binary and script behaviors (under ActiveX controls and plug-ins), and then verify that the Enable radio button is selected.
         It is preferable to add the NNMi management server to your Trusted sites zone rather than to enable privileges in a more restricted zone.

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

- Solutions that require Administrator privileges to the machine on which the Internet Explorer client exhibiting the problem is installed:
  - Verify that the latest updates for Internet Explorer are installed on the client machine, using Windows Update or a similar approach. An outdated patch level could be the reason VML is disabled.
  - Verify that vgx.dll is registered. The following command registers the VML vgx.dll if it was not already registered:
    ```
    regsvr32 "%ProgramFiles%\Common Files\Microsoft Shared\VGX\vgx.dll"
    ```
  - Check the Access Control List settings on vgx.dll
    ```
    cacls "%ProgramFiles%\Common Files\Microsoft Shared\VGX\vgx.dll"
    ```

- When launching one application from another that is in a different domain, Internet Explorer blocks the single sign-on session cookie. To fix this problem, add the application servers to the Trusted Sites zone for the web browser:
  1. In Internet Explorer browser, click Tools, and then click Internet Options.
  2. Navigate to the Security tab.
  3. Select the Trusted sites icon, and then click Sites.
  4. In the Trusted sites dialog box, add each application server the websites list.
- A known problem with memory growth exists in Internet Explorer when using the NNMi console. It might be necessary to periodically restart the Web browser if it is using too much memory.
- If Integration URLs are rendered inside a <frame> tag on a page that uses the Internet Explorer "Quirks mode", a JavaScript error occurs.
  - In Internet Explorer, URLs should not be launched in Quirks mode. Quirks Document mode is not standards compliant and NNMi does not support it at this time.
  - This situation might become an issue if an NNMi form or view is placed in an HTML document with other content, such as within a <frame> tag. The <DOCTYPE> tag at the top of the HTML document should be chosen to enable standards document mode. For example, the following DOCTYPE should not be used in a web page containing a frame that references an NNMi Integration URL:
    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
    A better choice would be to use a strict DOCTYPE such as:
    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
  - The Internet Explorer Developer Tools are useful for seeing and changing the browser and document mode.
- Internet Explorer 8 sets a limit to the number of rows that can be shown in table views. A user cannot scroll to see all possible rows. The workaround is the same as when the table is row limited: filter the table to show fewer rows. In practice this limit is about 30,000 rows, though it varies with font size.

Mozilla Firefox Browser Known Problems

- The telnet:// and ssh:// URLs are not enabled by default with Firefox. See the *Configuring the Telnet and SSH Protocols for Use by NNMi* chapter in the Deployment Reference for instructions on how to enable the telnet and ssh protocols, which requires configuring a telnet application, an ssh application, or both on each web client.
- By default, Firefox opens windows in a new tab instead of a new window. This behavior can cause NNMi to open windows that do not pop to the foreground. To change the default setting, under **Tools → Options | Tabs**, do the following:
  - Set New pages should be opened in: to a new window.
  - Select When I open a link in a new tab, switch to it immediately.
    This settings affects web pages that use "_blank" as a target, such as some help content.
- By default, Firefox limits the number of pop-up windows to 20. To adjust this limit, do the following:

1. Type `about:config` in the Firefox address bar.
2. Scroll down to dom.popup_maximum, and then double-click to modify the value.
3. Restart Firefox for this change to take effect.

- After opening and closing more than 50 forms in a single session, Firefox might start blocking pop-up windows, even when popups are enabled, which results in JavaScript errors. The workaround is to increase dom.popup_maximum or restart the browser. A suggested value in this case is a number greater than 500.
- Firefox tracks long running JavaScript operations and displays a "Warning: Unresponsive script" message if that timeout is exceeded. Complex map operations can exceed this maximum default of 5. To adjust the maximum time, do the following:
  1. Type `about:config` in the Firefox address bar.
  2. Scroll down to dom.max_script_run_time, and then double-click to modify the value. The value is in seconds. You can set it to 0 for infinity, however this is not recommended.
  3. Restart Firefox for this change to take effect.
- By default, JavaScript cannot raise a window to the top of the Firefox browser windows, which 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, do the following:
  1. In a new Firefox window, click **Tools → Options**.
  2. In the Options dialog box, select the Content pane.
  3. Next to the Enable JavaScript check box (which should be selected), click Advanced.
  4. Select the Raise or lower windows option.
- Firefox can incorrectly indicate that a request is still in progress while using the MIB Browser or 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 management server. For more information, see Bugzilla defect #383811 at https://bugzilla.mozilla.org/show_bug.cgi?id=383811.
- Using the "F5" refresh key causes a corrupt display of the form. To refresh a form, use the Refresh toolbar button on the form.
- If you have previously created a User Account and later delete and recreate it, the Firefox autocomplete feature fills in the password field for you, without notifying the user interface, causing the create to fail. The workaround is to change the password twice, or turn off form completion in Firefox.

Non-English Locale Known Problems

- NNMi localizes "Drop-down Choice" Code Values (such as Incident Category and Incident Family) at database creation time using the locale of the server. Unlike most other content, if accessed from a client under a different supported locale, the values remain in the locale of the server set at the time of database creation, which is typically installation time. The same is true for any user created "Drop-down Choice" Code Values. Other drop-down choices that are Enumeration Values (such as Incident Severity) are locale-sensitive and appear in the locale of the web browser for supported locales.
- 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, these strings are loaded into the database as English strings. When setting the locale to a supported locale, you must also navigate to the **Control Panel → Regional and Language Options → Advanced** tab, and then select 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. After the WSM is in the desired locale, you can install NNMi.
- For English Internet Explorer to browse an Asian language NNMi management server, the client needs to install the "East Asian Language" on the system. Without this change, tooltips for Priority and other table values appear as squares. You can install the "East Asian Language" from the **Control Panel → Regional and Language Options → Language** tab. Select Install files for East Asian language. This problem only happens with Internet Explorer. Users see similar problems when browsing to any Asian language web site.

- 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 appear properly.
- When displaying the value for MIB variables of type OCTET STRING, NNMi uses the textual conventions defined in the MIB. In the absence of textual conventions, the data will be interpreted based on any character encodings defined by the `com.hp.nnm.sourceEncoding property` defined in the `nms-jboss.properties` file. If this property is not defined, the multi-byte characters will be interpreted with the UTF-8 character encoding. For more information, see "Problems and Solutions" in the Deployment Reference.
- (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 a Japanese language Node Group name parameter, the browser settings might need to be changed. For Firefox, input “about:config” in the address bar; find “network.standard-url.encode-utf8”; change the value to be “true”. For Internet Explorer: "Turn on sending URLs as UTF-8"; see Microsoft document at support.microsoft.com/kb/925261 for details.
- The ovjboss process does not run correctly on HP-UX systems with a Turkish locale (LC_ALL=tr_TR.iso8859-9). For these systems running the Turkish locale, start NNMi processes with the C locale (`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 Sweep for auto-discovery
  - IPv6 Address Fault monitoring through SNMP (not available for IPv4 Addresses either)
  - IPv6 Link Local Address fault monitoring, or as discovery seeds or 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/NNM9.10/devicematrix.htm.

MIB Loader Migration Known Problems

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

Global Network Management (GNM) Known Problems

- If your global manager is running NNMi 9.10 and your regional manager is running NNMi 9.0x, when you run

Actions → Regional Manager Console, you might see a 404 error that the page http://machine/nnm/main does not exist. The workaround is to edit the menu item on the global manager and change it to http://machine/nnm/protected/main.jsp.

HP Software Support

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

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

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

To access the Self-solve knowledge base, visit the Self-solve knowledge search home page.

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

To register for an HP Passport ID, go to: HP Passport Registration.

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

Acrobat® is a trademark of Adobe Systems Incorporated.

Google™ is a trademark of Google Inc.

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

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

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

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

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

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

Acknowledgements

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

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