HP Network Node Manager i Software Release Notes

Software Version: 9.21/ 26 August 2012

This document provides an overview of the changes made to HP Network Node Manager i Software (NNMi) version 9.20.
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/NNM9.20/releasenotesupdate.htm.

For a list of supported hardware platforms, operating systems, and database, see the HP Network Node Manager i Software System and Device Support Matrix. For the list of supported network devices, see the *HP Network Node Manager i Software (NNMi) Device Support Matrix* at sg-pro-ovweb.austin.hp.com/nnm/NNM9.20/devicematrix.htm.

What's New In This Version

Overview of the NNMi 9.21 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 Upgrade Reference). Single system upgrades of NNMi 9.0x and NNMi 9.1x to NNMi 9.2x are supported (see the Upgrade Reference). NNMi 8.x installations must be upgraded to NNMi 9.0x before being upgraded to NNMi 9.2x.

NNMi 9.21

- **User Interface**
  - NNMi permits User Accounts assigned to the NNMi Operator Level 2 User Group to run Status Poll and Configuration Poll on nodes to which they have access. See the *Maintaining NNMi* chapter in the 9.21 Deployment Reference for more information.
  - NNMi permits User Accounts assigned to the NNMi Operator Level 2 User Group to edit maps and node groups. See the *Maintaining NNMi* chapter in the 9.21 Deployment Reference for more information.
- **Events**
  - The trap server now starts sooner and begins capturing traps earlier after restarting NNMi.

The Incidents View now includes Tenant and NNMi Management Server Columns.

- Remote site unreachable incidents (Management Incident Configuration IslandGroupDown) have been updated to include custom incident attributes (CIA) cia.incidentDurationMs, cia.timeIncidentDetectedMs, and cia.timeIncidentResolvedMs. See the help topic "Custom Incident Attributes Provided by NNMi" for a description of these CIAs.

- **SNMP Communication and MIBs**
  - NNMi now supports the discovery of its EngineID, which is used in processing SNMPv3 traps and informs. Devices can discover NNMi's EngineID using the standard SNMPv3 EngineID discovery algorithm:
    a. A device sends an empty SNMP-GET request to NNMi's configured trap port (typically port 162).
    b. NNMi generates and sends an SNMPv3 report PDU response to the device. NNMi's response contains NNMi's EngineID.

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

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

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

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

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

ArcSight

- Out-of-the-box Support for ProCurve syslog messages
- Out-of-the-box support for H3C syslog messages

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

NNMi 9.20

- **Upgrade Notes**
  - Read the new *NNMi 9.20 Upgrade Path Requirements* document for supported paths for upgrading to NNMi 9.20.
  - For important notes about upgrading to NNMi 9.20, see the Upgrade Reference. It is important to read these notes before performing the upgrade. The Upgrade Reference now includes information about upgrading from the following NNM and NNMi versions:
    - NNM 6.x and 7.x
    - NNMi 8.0x and 8.1x
    - NNMi 9.0x and 9.1x
  - The NNMi Action Server has been updated to Jython version 2.5.2. Check your Jython scripts for required changes.
  - The deprecated `nnmnetloadnodeattrs.ovpl` and `nnmnetdeletenodeattrs.ovpl` scripts have been removed. Use the `nnmloadattributes.ovpl` and `nnmdeleteattributes.ovpl` scripts instead.
  - Objects that are not monitored always show a state of **Not Polled**. (Previously they might have shown a State of **No Polling Policy.**)
  - The **NeighborDisabled** incident is no longer generated.
  - The **ManagementAddressICMPResponseTimeAbnormal** incident is now enabled by default.
  - The `nnmchangeembdbpw.ovpl` script does not correctly update password information on the secondary node if upgrading from NNMi 9.0x in a High Availability (HA) environment.

    On systems that were configured for HA while under NNMi 9.0x, the `nnmchangeembdbpw.ovpl` script does not properly copy the password information to the shared disk so that it can be replicated on the secondary node. Upon failover to the secondary node, the `nmsdbmgr` process is unable to connect to the database, and the resource group will fail to successfully start.

    The workaround is to move the resource group to the system where the `nnmchangeembdbpw.ovpl` script was run and perform the following steps:

    1. `mkdir <HA_mount_point>/NNM/dataDir/shared/nnm/conf`
    2. `chown bin:bin <HA_mount_point>/NNM/dataDir/shared/nnm/conf`
    3. `chmod 755 <HA_mount_point>/NNM/dataDir/shared/nnm/conf`
    4. Rerun the `nnmchangeembdbpw.ovpl` script
  - (Linux only) If you plan to upgrade a Linux NNMi management server from NNMi 9.0x to NNMi 9.20, you must import the HP public key into the Linux RPM database before installing NNMi 9.20. Please see the *NNMi 9.20 Interactive Installation Guide* for more information.

- (HP-UX only) To ensure that maintenance mode is properly enabled when upgrading an HA cluster, carefully follow the HA upgrade instructions in the Upgrade Reference.
- (NNMi Advanced only) NNMi requires special upgrade procedures for Global Network Management environments. When upgrading NNMi management servers configured in a Global Network Management environment to NNMi 9.20, the connections between the Global Network Manager and the Regional Managers disconnect until both the Global Network Manager and Regional Managers are upgraded to 9.20. To minimize the total downtime, HP recommends you upgrade all of the servers at approximately the same time. See the "Upgrading Global and Regional Managers from NNMi 9.0x/9.1x" section in the Upgrade Reference for more information.
- (NNM iSPI Performance for Metrics only) The following incidents are now enabled by default:
  - InterfaceFCSLANErrorRateHigh
  - InterfaceFCSWLANErrorRateHigh
  - InterfaceInputDiscardRateHigh
  - InterfaceInputErrorRateHigh
  - InterfaceInputQueueDropsRateHigh
  - InterfaceInputUtilizationAbnormal
  - InterfaceInputUtilizationHigh
  - InterfaceInputUtilizationLow
  - InterfaceOutputDiscardRateHigh
  - InterfaceOutputErrorRateHigh
  - InterfaceOutputQueueDropsRateHigh
  - InterfaceOutputUtilizationAbnormal
  - InterfaceOutputUtilizationHigh
  - InterfaceOutputUtilizationLow
- Connections between tenants (other than the Default tenant) are deleted during an upgrade.
- NNMi no longer generates the `Non-SNMP Node Unresponsive` incident.
- Configuration Exchange is now more efficient. You can view detailed error messages in the `nnm.log` file.
- If you plan to upgrade an earlier version of NNMi 9.0x or NNMi 9.1x to NNMi 9.20, and if that same system had been running NNMi 8.1x at some time in the past, the upgrade might incorrectly set the `HostNameMatchManagementIP` propertyl to `false`. The `HostNameMatchManagementIP` property exists in the `nms-disco.properties` file. In most cases, you will prefer the value of this property to be `true`. If you want it to remain `true`, check this file after the upgrade completes, and correct the value if necessary. The `nms-disco.properties` file is located in the `%nnmdatadir%\shared\nnm\conf\props` folder (Windows) or `$NnmDataDir/shared/nnm/conf/props` directory (UNIX).

- **Changes to Supported Environments**
  - Adds support for Internet Explorer 9.
  - Adds support for 64-bit versions of Internet Explorer 8 and Internet Explorer 9.
  - Adds support for Firefox 10.x ESR.
  - Adds support for Red Hat Linux 6.
  - Adds support for ESXi 5.x.
  - Adds support for Veritas HA for SUSE Linux
  - Adds Veritas 5.1 HA support for Solaris Zones.

- Service Pack 1 is now required for Windows Server 2008 R2.
- Firefox 3.6 is no longer supported.
- Red Hat Linux 5.2 and 5.3 are no longer supported.

- **Documentation Changes**
  - The *Upgrading from NNMi 9.0x* section of the Deployment Reference has been moved to the Upgrade Reference.
  - Each of the integration sections in the Deployment Reference has been moved to a separate document.
  - The *NNMi 9.20 Interactive Installation Guide* is now delivered as an interactive document. See the `nnmi_interactive_installation_en_README.txt` file on the NNMi installation media for more information.
- **Overlapping Address Domains (OAD)**
  - Overlapping Address Domains (OADs) with duplicate IP addresses can be managed in various NAT environments. See the NNMi online help and the "Managing Overlapping IP Addresses in NAT Environments" section of the *HP Network Node Manager i Software Deployment Reference* for details.
  - NNMi supports the following address translation protocols:
    - Static Network Address Translation (NAT)
    - Dynamic Address Translation protocols:
      - Dynamic Network Address Translation (NAT)
      - Port Address Translation (PAT) / Network Address Port Translation (NAPT)
  - OADs are defined by assigning nodes to Tenants. Each OAD's member Nodes belong to one Tenant.
  - A standalone NNMi management server can manage multiple *static* NAT domains
  - Devices that belong to the Default Tenant can have Layer 2 Connections to any device in any Tenant. Devices within any Tenant *other than* Default Tenant can have Layer 2 Connections *only* to devices within the same Tenant or the Default Tenant. L2 connections are discovered between the Default Tenant and each of the other Tenants to allow a shared network infrastructure connecting the tenants.
  - Overlapping Address Mappings for *Static* NAT
    - Mappings between internal (typically private) and external (typically public) IP addresses can be defined. These mappings are optional.
      - These mappings can be defined in the NNMi console using the Overlapping Address Mappings area of the Configuration workspace's Discovery group. Mappings are associated with a particular Tenant.
      - The `nnmloadipmappings.ovpl` script can also be used to load the address mappings.
    - These address mappings allow the user to view the external (or public) IP address associated with an internal (or private) IP address on the IP Address form. The external address is shown at the Mapped Address attribute.
  - Each Node within non-Default Tenants (OADs) must be discovered through a seed. Auto-Discovery is not permitted within non-Default Tenants, and hints about neighboring devices are not gathered.
  - In an OAD environment, a trap may have additional CIAs:
    - `cia.internalAddress` – the internal address if there is a mapping defined for the external address
    - `cia.agentAddress` – the agent address field value of an SNMPv1 trap
  - (*NNMi Advanced*) In a Global Network Management (GNM) deployment, NNMi Regional Managers can use Tenant assignments to manage static NAT, dynamic NAT, and dynamic PAT/NAPT domains.
    - For dynamic NAT and PAT/NAPT, one NNMi Regional Manager is required for each domain. The

NNMi Global Manager is deployed outside any OAD domain, can directly manage any number of *static* NAT domains, and can receive and combine information about multiple dynamic OAD domains from NNMi Regional Managers. While the managed devices may be accessible only via dynamic NAT or PAT/NAPT outside the network, the NNMi Regional Manager needs to have a *static* NAT or a routable address for communication with the NNMi Global Manager.

- For static NAT, the NNMi Regional Manager can be deployed either inside or outside the static NAT domain.
- Each NAT or PAT domain must be assigned to unique non-Default Tenant. When the tenants from different regional managers are replicated on the NNMi Global Manager, NNMi handles OAD by tracking address/Tenant pairs (an address can be used within each Tenant)
- Traps forwarded from NNMi to the Regional Manager include Tenant assignment information so the Global Manager properly resolves OAD issues.

- You can use ICMP monitoring of the external addresses in an OAD environment if you use overlapping address mappings.
- The External address is used in preference to the internal address if ICMP fault polling is configured. This is an important reason for doing the mappings.

- **User Interface**
  - Icon customization for map views
    - The new **Configuration** workspace **User Interface** → **Icons** view enables you to view, create, and delete icons used for map views
    - The `nnmicons.ovpl` script can also be used to list, create, and delete these icons.
    - Icons are stored in the NNMi database and so will be preserved with backup/restore and application failover. Icons can also be exported and imported with the `nnmconfigexport.ovpl` and `nnmconfigimport.ovpl` scripts.
    - Through Device Profile configuration, the administrator can set or change the icons for device categories, device families, and device vendors.
    - The icon for a particular node can also be set explicitly using the custom attribute **NNM_ICON**.
  - The menu items under the **Actions→Node Group Membership** menu can be used to quickly create a new Node Group from a list of selected nodes (on a table or map view), add nodes to an existing Node Group, and remove nodes from a Node Group.
  - The menu items under the **Actions→Custom Attributes** menu can be used to quickly add a custom attribute to multiple nodes or interfaces and remove a custom attribute from multiple nodes or interfaces.
  - View changes
    - The **System Object ID** attribute column was added to the Node analysis pane and the **Nodes (All Attributes)** table view.
    - The **ifIndex** attribute column was added to the interface views.
    - The names of the Custom Nodes, Custom Interfaces, and Custom IP Addresses views have changed to Nodes (All Attributes), Interfaces (All Attributes), and IP Addresses (All Attributes).
  - Configuration workspace changes
    - Added a new **Monitoring** tree node, which has the following child nodes: **Monitoring Configuration...** and **Custom Poller Configuration...**.
    - Added a new **Object Groups** tree node, which has the following child nodes: **Node Groups** and **Interface Groups**.
    - Added a new **Trap Server** tree node under the **Incidents** tree node, which has the following child nodes: **Trap Forwarding Configuration...** and **Trap Logging Configuration**.

        - Moved the **Custom Correlation Configuration...** under the **Incidents** tree node.
    - Required fields on forms are indicated with a red asterisk.

- **Events**
    - Load incident configuration from a formatted configuration file
        - The `nnmincidentcfgload.ovpl` script provides a way to load Incident Configurations into the NNMi database from a formatted configuration file. You can also use the `nnmincidentcfgload.ovpl` script to validate an Incident Configuration file before it is loaded into the NNMi database.
        - The `nnmincidentcfgdump.ovpl` command permits you to create a configuration file of existing Incident Configurations in a non-XML format. You can then edit this file before loading them into the NNMi database via the `nnmincidentcfgload.ovpl` command.
        - See the `nnmincidentcfgload.ovpl`, `nnmincidentcfgdump.ovpl`, and `nnmincidentcfg.format` reference pages and "Help for Administrators" for more information.
    - Pairwise Configuration improvements
        - You can use Payload Filters (for example, with trap varbinds) to identify the first and second incidents in a Pairwise Configuration.
        - You can specify the same incident (for example, the same trap OID) as both the first and second incident configuration for a Pairwise Configuration.
            - Using the Payload Filter to distinguish the first and second incidents (the first could represent a non-normal state and the second a normal state), different instances of the same incident configuration can cancel one another.
            - You can also set up the Payload Filters such that the same incident instance cancels itself.
        - You can use the same incident configuration in multiple Pairwise Configurations. For example:
            - Incident configuration A cancels both incident configuration B and incident configuration C
            - Incident configuration A cancels incident configuration B and incident configuration B cancels incident configuration C.
        - A single incident instance can cancel multiple incident instances (for example, one link up trap cancels multiple instances of a link down trap)
            - Use the Duration time to specify the time in which the second incident configuration cancels the first incident configuration. This Duration is calculated from the `originOccurrenceTime` of the second incident backwards in time, canceling any number of first incidents within the Duration specified.
            - You can also specify whether to delete any incidents that were canceled according to the Pairwise Configuration and that occurred within the time period specified by the Duration attribute.
        - The **Matching Criteria** tab for the **Pairwise Configuration** form documents the matching criteria automatically added for different incident configurations.
    - Trap logging
        - NNMi provides trap logging in two different formats and trap logging files:
            - `trap.csv` - CSV format
            - `trap.log` - readable text format similar to trapd.log in NNM 6.x/7.x
        - Use the nnmtrapconfig.ovpl script to set global trap logging parameters.
            - The default mode is to only log traps to `trap.csv`. You can change the mode to log to both files, neither, or one or the other.
            - See the `nnmtrapconfig.ovpl` reference page for other global trap logging parameters.

- You can configure trap logging details for individual traps through the **Trap Logging Configuration** view in the **Configuration** workspace under **Incidents → Trap Server**.
  - This configuration includes enabling or disabling the trap logging and setting the log message format. The log message format can include trap varbind values.
  - You can either inherit logging values from the Trap Incident Configuration (for example, severity and category) or override those values in the Trap Logging Configuration.
  - You can also override the Trap Logging Configuration for nodes in a specified Node Group.
- You can export and import Trap Logging Configuration using the `nnmconfigexport.ovpl` and `nnmconfigimport.ovpl` scripts.

- Incident logging
  - NNMi permits you to configure incident logging so that incoming incident information is written to the `incident.csv` file in CSV format. This feature is useful when you want to track and archive your incident history.
    - Note: It is more efficient to do continuous incident archiving with incident logging than to do archiving when you are automatically trimming SNMP traps (using either the `nnmtrimincidents.ovpl` script or the Auto-Trim feature described in the Deployment Reference).
  - You can configure incident logging through the **Incident Configuration** form in the **Configuration** workspace under **Incidents**.
  - The `nnmtrimincidents.ovpl -archive` command has been modified to use the same CSV formatting used by Incident Logging.
- Trap storm detection
  - In addition to global trap storm detection, NNMi now also provides trap storm detection for more specific cases:
    - Per SNMP trap OID
    - Per node
    - Per "hosted object" (for example, an interface or card on a node)
  - NNMi permits you to modify the thresholds for trap storm detection and suppression using the `nnmtrapconfig.ovpl` script. See the `nnmtrapconfig.ovpl` reference page or the UNIX manpage, and the "Trap Storm" help topic in "Help for Operators" for more information.
  - For trap storm detection for objects, such as interfaces, hosted on nodes, see the reference pages for `nnmtrapconfig.ovpl` and `hosted-object-trapstorm.conf` and the "Blocking Trap Storms using the hosted-on-trapstorm.conf File" section in the the Deployment Reference.
    - The **Hosted Object Trap Storm** incident indicates that the number of traps from an object hosted on a node has exceeded the threshold for a hosted object.
- NNMi generates a **Node Deleted** incident to indicate a Node was deleted from the NNMi topology. See the "Node Deleted" help topic in "Help for Operators" for more information.

- **SNMP Communication and MIBs**
  - Priority for trying different SNMPv1/v2 Read Community Strings
    - An optional **Ordering** attribute was added for Read Community Strings in both Default and Regions configuration forms.
    - During the Discovery process, NNMi tries Read Community Strings in priority order (lowest to highest). Then, NNMi tries all unordered Read Community Strings (treated as though they had the same Ordering number). These unordered SNMP requests are sent in parallel, with NNMi using the first Read Community String that gets a response.

- The `nnmcommload.ovpl` script supports configuration of Communication Regions. See the `nnmcommload.ovpl` reference page, or the UNIX manpage, for details.
- MIBs can be unloaded using **Tools → Load/Unload MIB...**
  - Select any row in the **MIBs → Loaded MIBs** or **MIBs → MIB Variables** view, then click **Tools → Load/Unload MIB...** to display the **MIBs Available to Load/Unload** Web page to either load or unload a file from the NNMi database.

- **Discovery**
  - To prevent doing an SNMP query on all interfaces on large devices, you can specify a subset of interfaces (based on `ifIndex` range) to query based on the MIB `sysObjectID` prefix of the device. This configuration is done using the **Included Interface Ranges** tab on the **Discovery Configuration** form.
  - NNMi determines Layer 2 Connections using multiple discovery protocols per node in mixed environments (for example, both CDP and LLDP).
    - You can specify whether to prefer the standard Link Layer Discovery Protocol (LLDP) or the vendor-specific discovery protocol for particular devices through the **Prefer LLDP** attribute on the **Device Profile** form.
  - You can specify that some nodes be rediscovered at a different interval from the default Rediscovery Interval setting (for example, to rediscover certain important devices more frequently). This is specified using the **Node Group Interval Settings** section of the **Schedule Settings** tab on the **Discovery Configuration** form.
  - You can specify that some nodes not have any Layer 2 Connections created based on Forwarding Database (FDB) information. This is specified using the **Node Group to disable FDB** attribute on the **Discovery Configuration** form.

- **State Poller and Monitoring Configuration**
  - You can disable SNMP monitoring for a node through monitoring configuration. This can be done using the **Enable SNMP Polling on Node** attribute on **Node Settings** and **Default Settings** for **Monitoring Configuration**.
  - To enable more timely detection of device changes, monitoring configuration includes the polling of additional MIB values that can trigger node rediscovery. These are configured in the **Default Change Detection Monitoring** section on **Node Settings** and **Default Settings** for **Monitoring Configuration**.
    - Number of interfaces (`ifNumber`)
    - Last time entity changed (Entity MIB `entLastChangeTime`)

- **Custom Poller**
  - NNMi supports incidents on Custom Polled Instances as an alternative to the incidents on Customer Node Collections
    - You can specify the per instance incidents by selecting the **Custom Polled Instance** value for the **Incident Source Object** attribute on the **Custom Poller Collection** form.
    - A new **Custom Polled Instance Out Of Range** incident indicates a Custom Polled Instance has reached or exceeded a Comparison Map value or Threshold configured for the associated Custom Node Collection.
  - NNMi enables you to change the type of a MIB OID from what is reported by the device. For example, you can force something reported as an `Integer` to be interpreted as a `Counter`. This configuration is done using the **MIB OID Types** view under **MIBs** in the **Configuration** workspace.
    - These MIB OID Type configurations are used by Custom Poller, the NNMi Line Graph, and the Analysis Pane Gauges.
    - In addition to changing the primitive type of an OID, you can specify whether the OID has multiple instances grouped in a MIB table.

- **Causal Engine**
  - A non-SNMP node that is not reachable generates a **Node Down** or a **Node or Connection Down** incident. The **Non-SNMP Node Unresponsive** incident is no longer generated.
  - NNMi provides new Custom Incident Attributes (CIAs) for the **Island Group Down** incident:
    - `cia.island.name` – the name NNMi uses to identify the island. NNMi administrators can use this CIA value in Launch Actions to display the associated table view or topology map. See the "Help for Administrators" for more information.
    - `cia.island.numberOfNodes` – the number of nodes in the island
- **Security**
  - NNMi provides a way for non-root UNIX users to start and stop NNMi. See "Allowing Non-Root UNIX Users to Start and Stop NNMi" in the Deployment Reference for more information.
  - An administrator can disable HTTP and other unencrypted access from the network to NNMi by editing the `server.properties` file. See "Configuring NNMi to Require Encryption for Remote Access" in the Deployment Reference for more information.
  - The new **NNMi Global Operators** User Group provides access to all NNMi topology objects without giving full **NNMi Administrators** access. If you need to use this User Group, it should be assigned in addition to the **NNMi Guest Users**, **NNMi Level 1 Operators**, or **NNMi Level 2 Operators** User Group assignment to ensure NNMi console access. The Global Operators User Group does not change any other aspect of their NNMi Guest User, NNMi Level 1 Operator, or NNMi Level 2 Operator User Group assignment. See the "Help for Administrators" for more information.
  - An Embedded Database (postgres) password is required for local access. To run embedded database tools (such as `psql`), NNMi requires a password. NNMi provides a default password, which the user should change using the `nnmchangeembdbpw.ovpl` script. You must be logged in as Administrator on Windows systems or root on UNIX systems to run the `nnmchangeembdbpw.ovpl` script. For more information, see the `nnmchangeembdbpw.ovpl` reference page, or the UNIX manpage.
  - You can specify a privacy protocol to use for communication with SNMPv3 devices on the **SNMPv3 Settings** form in the NNMi console. The AES-192, AES-256, and TripleDES protocols are available for selection only when the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files library is installed on the NNMi management server. This library is automatically installed with the NNMi product. See the Deployment Reference for more information.
- **Integrations**
  - HP Network Automation
    - You can configure a Secure Socket Layer (SSL) connection between HP NNMi and HP Network Automation (NA). See the *HP Network Node Manager i Software—HP Network Automation Integration Guide* for more information.
    - For NNMi Nodes and Interfaces that are also managed by NA, the Analysis Pane shows additional tabs with NA configuration information. NA Analysis Pane information is also available for certain Incidents. See "NA Node and Interface Information Displayed in NNMi Analysis Panes" in the *HP Network Node Manager i Software—HP Network Automation Integration Guide* for more information.
  - HP ArcSight
    - The HP NNMi–ArcSight integration adds syslog message information to NNMi, so that NNMi users can view these syslog messages and investigate potential problems. After the ArcSight integration is enabled, NNMi receives `ArcSightEvent` traps that contain syslog message data. NNMi then maps this syslog information to a Syslog Message incident configuration and treats it as a syslog message in NNMi. See the *HP Network Node Manager i Software—HP ArcSight Logger Integration* Guide and the Deployment Reference for more information.
    - You can configure NNMi to forward SNMP traps and management events to HP ArcSight Logger.
    - You can cross-launch to the HP ArcSight Logger user interface from NNMi Nodes, Interfaces, and

Syslog Message incidents.

- Syslog Messages received from HP ArcSight Logger can also be sent through the NNMi Northbound Interface. See the “NNMi Northbound Interface” chapter in the the Deployment Reference for more information.

- **Application Failover**
  - To keep the standby server in sync with the active server, Application Failover uses a streaming replication feature that sends database transactions from the active server to the standby server. Streaming replication eliminates the need for database transaction logs to be imported on the standby server on failover (as was the case in earlier NNMi versions). This feature also greatly reduces the time needed for the standby server to take over as the active server. This feature is enabled by default, even in the case of upgrading from an existing Application Failover cluster.
  - The **NNMi Cluster Setup Wizard** automates the process of configuring a cluster within NNMi for use with Application Failover. The URL for this wizard is `http://<node>/cluster`. See "Configuring your Cluster with the NNMi Cluster Setup Wizard (Embedded Database User only)" in the Deployment Reference for more information.
  - Information about the health of the Application Failover cluster is now included in **NNMi System Health** (available from the **Health** tab of **Help→System Information**).
- **General**
  - NNMi supports 10,000 Node Groups
  - NNMi supports 1500 configured users
  - The port for the embedded (Postgres) database is configurable. See the `nnm.ports` reference page, or the UNIX manpage, for details.
  - Full re-synchronization of polled object states and status ensures that all state values are current and that status is consistent with the state.
    - NNMi automatically performs a full re-synchronization in the following cases:
      - When upgrading an NNMi management server from an earlier NNMi release.
      - After restoring an NNMi management server from a backup.
      - After failover in an NNMi Application Failover cluster.
    - You can use the `-fullsync` flag with the `nnmnoderediscover.ovpl` script to synchronize all polled object States and Status (although this takes more time and causes a greater load on the systems). For more information, see the `nnmnoderediscover.ovpl` reference page, or the UNIX manpage.
    - See "Resolve Inconsistencies between State and Status" in the "Help for Administrators" for more information.
- **Global Network Management (*NNMi Advanced required*)**
  - NNMi Analysis Pane gauges for nodes and interfaces are available on the global manager for nodes managed by regional managers.
  - For discussion of full re-synchronization in a GNM environment, see "Node Synchronization Issues" in the "Help for Administrators."
- **Performance Management (*NNM iSPI Performance for Metrics required*)**
  - You can use Custom Attributes to include additional Node or Interface information in NNM iSPI Performance for Metrics reports. The Custom Attribute Name must be **NPS Annotation**. NPS (Network Performance Server) is the database server installed with the NNM iSPI Performance for Metrics software.
  - NNM iSPI Performance for Metrics data for incidents and topology objects is displayed in the NNMi Analysis Pane on the **Performance** tab.

NNMi automatically synchronizes Interface Group and Node Group configuration changes between NNMi and NNM iSPI Performance for Metrics. However, in some cases, additional configuration changes that affect Node Group or Interface Group membership might take longer to synchronize.

- If you do not see one or more nodes in an NNMi Performance for Metrics report that is filtered by a group but that you would expect to see based on group membership in NNMi, use the **Actions → HP NNM iSPI Performance → Sync Interface and Node Groups** menu item. This menu item forces NNMi to synchronize the Interface and Node Group information between NNMi and NNM iSPI Performance for Metrics more quickly than the default time period.

- **Maintenance**
  - The nnmbackup.ovpl script supports overwriting the previous backup to conserve disk space by using the `-noTimeStamp option.`
- **NNMi System Health**
  - NNMi System Health enhancements (new JMS and Service health agents; improvements to Memory and Database health agents).

NNMi 9.1x Patch 2

- **Product Changes**
  - You can use the `nnmcommload.ovpl` script to load communication configuration options for ICMP Enabled, ICMP Timeout and ICMP Retries. See the `nnmcommload.ovpl` reference page, or the UNIX manpage for more information.

NNMi 9.1x Patch 1 (9.11)

- **Product Changes**
  - The `nnmfindattachedswport.ovpl` script permits you to find the attached switch port for an end node. The end node does not have to be in the NNMi database; however, the switch does need to be in the database. This functionality is similar to the **Tools → Find Attached Switch Port...** action. See the `nnmfindattachedswport.ovpl` reference page, or the UNIX manpage for details.
  - Custom Poller enhancements
    - The **Display Attribute** that is specified in the **Instance Display Configuration** for a MIB Expression is available as an attribute on **Custom Polled Instances**.
    - The following new CIAs are now available for Custom Node Collection incidents:
      - cia.custompoller.mibInstance
      - cia.custompoller.instanceDisplayValue
      - cia.custompoller.instanceFilterValue
  - Integrations
    - The HP ArcSight integration adds syslog message support to NNMi.
    - For topology synchronization in the HP Network Automation integration, nodes are synchronized to NA partitions having names that match the node's NNMi security group. If such a partition does not exist, a new NA partition is created. The NNMi "Default Security Group" is mapped to the NA "Default Site" security group.
    - For the HP BSM Topology integration, select **Only synchronize managed objects** if you want to exclude unmanaged objects and unconnected interfaces from the topology synchronization for the integration.
  - Performance Management (*NNM iSPI Performance for Metrics required*)
    - Collect and report on additional WAN Performance Monitoring metrics:

- ATM Interfaces
- Frame Relay Interfaces

- To collect performance metrics for ATM and Frame Relay, you must select **Enable Discovery of ATM/Frame Relay Interfaces for Performance Monitoring** in **Discovery Configuration**.

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, "9.20" product version, and then choose your operating system. From the search results, open the Documentation List and click the link for the appropriate version of a document.

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

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

Deployment Reference

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

Upgrade Reference

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

Integration Guides

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

Reference Pages

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

Documentation Errata

No documentation errata.

Installation Guide and Support Matrix

To obtain an electronic copy of the most current version of the *NNMi 9.20 Interactive Installation Guide*, go to http://h20230.www2.hp.com/selfsolve/manuals.

Installation requirements, as well as instructions for installing NNMi, are documented in an interactive version of the *NNMi 9.20 Interactive Installation Guide*. The *NNMi 9.20 Interactive Installation Guide* is included on the NNMi installation media as `nnmi_interactive_installation_en.zip` or `nnmi_interactive_installation_en.jar` files. For instructions explaining how to extract and view the *NNMi 9.20 Interactive Installation Guide*, see the `nnmi_interactive_installation_en_README.txt` file located at the root of the NNMi installation media.

For a list of supported hardware platforms, operating systems, and databases, see the HP Network Node Manager i

Software System and Device Support Matrix.

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

Licensing

NNMi installs with an instant-on 60-day/250-node license. This license also temporarily enables the NNMi Advanced features and the NNM iSPI Network Engineering Toolset Software for the 60-day trial period.

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

For information about installing and managing licenses, see the *NNMi 9.20 Interactive 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 Interface form.
- HP Route Analytics Management Software (RAMS) integration for RAMS traps and path information from RAMS, enhancing the path displayed in Path View.
- Extension of path visualization (for example, Equal Cost Multi-Path). When multiple paths are possible, the user interface provides for selection of specific paths for opening an NNM iSPI Performance for Metrics path health report.
- MPLS WAN Clouds (RAMS) view from the Inventory workspace, including map views of the MPLS WAN cloud; see *Using Route Analytics Management Software (RAMS) with NNMi Advanced* in the NNMi help.
- VMware ESX and Virtual Machine Capability Discovery.

HP Network Node Manager 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.

- 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

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

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

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

  ```
  "%NnmInstallDir%\nonOV\perl\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:
     a. Value name: InheritConsoleHandles
     b. Data type: REG_DWORD
     c. Radix: Decimal

d. Value data: 1

5. Quit the Windows Registry Editor

- Cross-launch to NNM 7.x using an NNMi Management Server 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 stop responding when the system starts running low on memory in very large environments. See the HP Network Node Manager i Software System and Device 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 *HP Network Node Manager i Software System and Device Support Matrix*.
- If the NNMi management server has a firewall blocking incoming HTTP requests, you cannot start the NNMi console remotely.

  The Linux firewall is enabled by default. You can either disable the firewall completely, or more specifically add other ports:
  161:udp, 162:udp, *<HTTPPORT>*:tcp
  where *<HTTPPORT>* is the NNMi web server port as defined by the `jboss.http.port` value in the `/var/opt/OV/conf/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. When the case sensitivity differs between what is returned from the directory service and the name with which you logged on, you cannot assign incidents to your user name and the My Incidents view does not work. Use **Actions** > **Assign Incidents** to view the list of valid user names, including the required case for each.
- NNMi application failover on Windows systems:
  - Application failover on the Windows platform can have some intermittent issues with Symantec Endpoint Protection (SEP) software that affect NNMi cluster operations. When the Standby node is attempting to receive the database backup, this operation sometimes fails because SEP is not releasing a file lock in a timely manner. The database file is automatically retransmitted on any failure, and this problem eventually clears itself.
  - When application failover is configured for Windows, system reboots or other issues might cause the psql command to fail, generating dialog boxes to the Windows desktop and the event viewer. These dialog boxes do not affect operation and can be ignored.
- When you perform an online backup of NNM, the database password is included in the backup. If you change the database password using the `nnmchangeembddbpw.ovpl` script after a backup is completed; then restore NNMi from the backup that includes the outdated password, the NNMi database fails to start.

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

  A workaround is possible using the following sequence:

  a. If you are not able to delete the Custom Node Collection, try to delete each Custom Poller Policy on the Custom Node Collection individually.
  For each Custom Poller Policy that fails to delete:

  a. If the policy has a MIB Filter value, change its value to a pattern that does not match any MIB filter variable value. Check the Custom Node Collection table to ensure that all nodes for that Custom

Poller Policy have completed discovery. All Custom Polled Instances for this Custom Poller Policy should be removed.

b. If the Custom Poller Policy does not have a MIB filter value, change the Custom Poller Policy's Active State to **Inactive**. This action should cause all Custom Polled Instances associated with the Custom Poller Policy to be deleted. If it does not, edit the associated Node Group to remove nodes from the group. This causes NNMi to delete the associated Custom Node Collections and their Custom Polled Instances.

b. It should now be possible to delete the policy successfully.

c. When all Custom Poller Policies for a Custom Node Collection are deleted, delete the Custom Node Collection.

- If you are browsing between multiple NNMi installations, browsing to a second NNMi installation logs you off from the previous NNMi installation when you return to the first system. To fix this problem, do the following:

  1. Open the following file:

     a. *Windows*: `%NnmDataDir%\shared\nnm\conf\props\nms-ui.properties`

     b. *UNIX*: `/var/opt/OV/shared/nnm/conf/props/nms-ui.properties`

     Edit the file in one of the following ways:

     a. Disable Single Sign-On by setting `com.hp.nms.ui.sso.isEnabled="false".`

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

  2. Run `nnmsso.ovpl -reload`.

- (Windows only) Anti-virus and backup software can interfere with NNMi operation if this software locks files while NNMi is running. Any application that locks files should be configured to exclude the following NNMi database directory on Windows Server 2008: `C:\ProgramData\HP\HP BTO Software\databases`.

- The `Query Password` field of a RAMS configuration is only valid when imported into the same NNMi installation on the same system. If imported into a different system, the `Query Password` must be re-entered.

- On Linux, if you are using IPv6 and forwarding NNM 6.x/7.x events, ovjboss communication with PMD can be lost. This is 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 a non-DNS hostname can prevent a user from logging on to the NNMi console. For example, if the NNMi server's FQDN is not resolvable in DNS, and the user wants to use an FQDN on the box, a user could add an entry such as `192.168.0.100 myhost.example.com` to local system hosts file. This hostname is not resolvable by the DNS server. If the browser is configured with HTTP proxy, the browser ignores the hosts file for NNMi hostname resolution, and uses the proxy for NNMi hostname resolution. Because DNS cannot resolve the NNMi hostname, the NNMi console logon fails.

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

  - Internet Explorer:

    1. On the **Internet Options** → **Connections** tab, click **LAN Settings**.

    2. If the **Proxy Server** is configured, click **Advanced**, and then add the non-DNS NNMi hostname into the **Proxy Settings Exceptions** list.

  - Firefox:

    1. Click **Tools** → **Options**.

    2. In the **Options** dialog box, select the **Advanced** pane.

3. On the **Network** tab, under Connection, click **Settings**. If a proxy is configured, add the non-DNS NNMI hostname into the **No Proxy for** list.

- Nodes with down Interfaces might have a Status of **No Status** under the following conditions:
  - If the active IP Address that responds to SNMP communication is on a down Interface, it is excluded from the list of candidate Management IP Addresses.
  - If the hint or seed address that was used did respond to SNMP, the result is a node with valid system information and Device Profile, but no SNMP Agent.

  To resolve the problem use the **Configuration Poll** option from the **Actions** menu.
- When using the **Actions** → **Custom Attributes** menu items from a Node or Interface form, saving the form can overwrite Custom Attributes that have been added. The workaround is to close the form instead of using Save and Close or use the **Actions** → **Custom Attributes** menu items only from a table view.
- (NNM Performance iSPIs) It is important for you to synchronize the NNMi management server clock and the NPS server clock. This ensures that the analysis panes that retrieve data from the NPS server yield accurate results. If you experience blank analysis panes, check that your clocks are synchronized between the two servers. NPS (Network Performance Server) is the database server installed with any of the NNM Performance iSPI products.

Potential Installation Issues

- See installation prerequisites in the NNMi 9.20 Interactive Installation Guide and HP Network Node Manager i Software System and Device Support Matrix for complete instructions.
- If you are installing a localized version of the product, see the Non-English Locale Known Problems section for additional information.
- In addition to the web server port, the NNMi management server uses several ports for process communication as documented in the *NNMi 9.20 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 *NNMi 9.20 Interactive Installation Guide* instructs the user to run an installation using the user interface on another system. This approach creates a `%TEMP%\HPOvInstaller\NNM\ovinstallparams_`*`DATETIME`*`.ini` file. This file can be copied to another system as `%TEMP%\ovinstallparams.ini` and then installed using the silent installer.

Use Wordpad (or some other editor) instead of Notepad to modify the `ovinstallparams.ini` file.
If this `.ini` file is generated on a non-English locale machine (for example: Japanese or Chinese), and if you edit this file in the Notepad editor, Notepad adds 3 bytes at the start of the file to specify the encoding as UTF-8. These 3 bytes cause the subsequent silent installation process to fail.

- (Windows only) Do not use non-English characters in the path name of the installation directory.
- If you plan to upgrade an earlier version of NNMi 9.0x or NNMi 9.1x that is running in an NNMi application failover cluster, see the Upgrade Reference for detailed instructions on this procedure.
- If you plan to upgrade an earlier version of NNMi 9.0x or NNMi 9.1x that is running in a High Availability environment, see the Upgrade Reference for detailed instructions on this procedure.
- If you have NNM iSPIs installed on the NNMi management server, and plan to remove NNMi and NNM iSPIs, uninstall the NNM iSPIs before uninstalling NNMi. Otherwise, when you reinstall NNMi, the NNM iSPIs no longer work until you reinstall each one.
  Note: NNM iSPI Performance for Metrics is an exception to the above uninstall requirement.
- NNMi creates a self-signed certificate during installation. This certificate enables HTTPS access to the NNMi console without additional configuration. Because it is a self-signed certificate, your browser does not automatically trust it, resulting in security prompts when using the NNMi console.
  - With Firefox, you can choose to permanently trust the certificate, and you will not be prompted again.
  - With Internet Explorer, you will be prompted multiple times. There are two ways to prevent these prompts:
    - Import the self-signed certificate into each user's browser.
    - Replace the self-signed certificate with a CA-signed certificate that all users' browsers are configured to trust. For more information, see the *Working with Certificates for NNMi* chapter of the Deployment Reference.
- (Linux only) Setting the `/opt` or `/var/opt` directory with inherited permissions might cause problems if the inherited permissions are too restrictive.
  The inherited permissions are created by enabling the set-groupId bit on the directory itself, for example the "2" in the `chmod 2755` command.
  An example of an inherited permission that is too restrictive is "2750". This permission strips world read-access. Some NNMi processes run as non-root user (for example the database and the action process). These processes need read access to files below `/opt/OV` and `/var/opt/OV`. If the inherited directory permission strips world read, these processes fail.
- (Linux only) If the NNMi public key import or a product install fails with the following error:

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

  Complete the following steps:

  a. Run the following command to save a copy of the rpm database: **tar cvzf /var/tmp/rpmdbtar.gz /var/lib/rpm**
  b. **rm /var/lib/rpm/__db.00***
  c. **rpm –rebuilddb**

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

  a. **rpm –q –a**
  b. **rpm –import pk.pub**

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

Internet Explorer Browser Known Problems

- The telnet:// and ssh:// URLs are not enabled by default with Internet Explorer. See the *Configuring the Telnet and SSH Protocols for Use by NNMi* chapter in the Deployment Reference for instructions on how to enable the telnet and ssh protocols, which requires a registry change on each web browser client. Without this registry edit, selecting the **Actions → Node Access → Telnet... (from client)** or **Secure Shell... (from client)** menu item results in a "The webpage cannot be displayed" message.
- When using Internet Explorer, browser settings determine whether the name of an NNMi view or form displays in the title bar. To configure Internet Explorer to display view and form titles:
  1. In Internet Explorer browser, click **Tools**, and then click **Internet Options**.
  2. Navigate to the **Security** tab, **Trusted Sites**, **Custom Level**, **Miscellaneous** section.
  3. Disable the **Allow websites to open windows without address or status bars** attribute.
- Internet Explorer tracks long running JavaScript operations, and displays a "This page contains a script which is taking an unusually long time to finish" message if a maximum number of JavaScript statements is exceeded. Complex map operations can exceed this maximum default of 5,000,000. To adjust the maximum time, the HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Styles\MaxScriptStatements 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.
- (Internet Explorer 8 only) 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 Vector Markup Language (VML) is disabled in your Internet Explorer browser. VML 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 sets a limit to the number of rows that can be shown in table views. A user cannot scroll to see all possible rows. The workaround is to filter the table to show fewer rows. In practice this limit is about 30,000 rows, although it varies with font size.
- (Internet Explorer 8 only) When NPS is installed on a different machine from NNMi, a red cross appears in the Performance panel of the analysis pane instead of the expected graphs. This can be fixed with the following configuration change:
  1. In Internet Explorer browser, click **Tools**, and then click **Internet Options**.
  2. Navigate to the **Security** tab.
  3. Select **Trusted sites**.
  4. Click on **Sites** and add the NPS and NNMi servers to the trusted sites list.
  5. Click **Custom level** to open the **Security Settings** dialog box for the Trusted sites.
  6. In the **Miscellaneous** section of the **Security Settings** dialog box, select **Enable** for **Access data sources across domains**

Mozilla Firefox Browser Known Problems

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

do the following:

- Set **New pages should be opened in:** to **a new window**.
- Select **When I open a link in a new tab, switch to it immediately**.
  This settings affects web pages that use "_blank" as a target, such as some help content.

- By default, Firefox limits the number of pop-up windows to 20. To adjust this limit, do the following:
  1. Type `about:config` in the Firefox address bar.
  2. Scroll down to **dom.popup_maximum**, and then double-click to modify the value.
  3. Restart Firefox for this change to take effect.
- After opening and closing more than 50 forms in a single session, Firefox might start blocking pop-up windows, even when popups are enabled, which results in JavaScript errors. The workaround is to increase **dom.popup_maximum** or restart the browser. A suggested value in this case is a number greater than 500.
- Firefox tracks long running JavaScript operations and displays a "Warning: Unresponsive script" message if that timeout is exceeded. Complex map operations can exceed this maximum default of 5. To adjust the maximum time, do the following:
  1. Type `about:config` in the Firefox address bar.
  2. Scroll down to **dom.max_script_run_time**, and then double-click to modify the value. The value is in seconds. You can set it to 0 for infinity, however this is not recommended.
  3. Restart Firefox for this change to take effect.
- By default, JavaScript cannot display a window on top of the Firefox browser windows. This behavior 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 display previously opened windows on top of the Firefox browser window, do the following:
  1. In a new Firefox window, open the **Options** dialog box.
  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 Graphs, even though the request is complete. You will see "Transferring data from <NNMi Server>" in the Firefox status bar, where <NNMi Server> is your NNMi management server. For more information, see Bugzilla defect #383811 at https://bugzilla.mozilla.org/show_bug.cgi?id=383811.
- Using the "F5" refresh key causes a corrupt display of the form. To refresh a form, use the **Refresh** toolbar button on the form.
- If you have previously created a User Account and later delete and recreate it, the Firefox auto-complete feature fills in the password field for you, without notifying the user interface, causing the create to fail. The workaround is to change the password twice, or turn off form completion in Firefox.
- In certain deployments, the Performance panel in the analysis pane for a selected object in the NNMi Console may show a login prompt the first time the user signs in to the NNMi Console using Firefox. If this happens, enter the NNMi username and password.

Non-English Locale Known Problems

- Do not install NNMi on a server configured with the `ko_KR.eucKR` locale on HP-UX. NNMi does not support the `ko_KR.eucKR` locale. Instead, configure the server to use the `ko_KR.utf8` locale before installing NNMi.
- 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.

- 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.
- When displaying the value for MIB variables of type OCTET STRING, NNMi uses the textual conventions defined in the MIB. In the absence of textual conventions, the data is interpreted based on any character encodings defined by the `com.hp.nnm.sourceEncoding property` defined in the `nms-jboss.properties` file. If this property is not defined, the multi-byte characters will be interpreted with the UTF-8 character encoding. For more information, see "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`).
- The Autopass Licensing GUI (`nnmlicensing.ovpl <ProductName> -gui`) is only localized for Japanese. In all other locales, including Chinese and Korean, only English text is displayed.

Domain Name System (DNS) Configuration Known Problems

- Spiral Discovery depends on a well-configured Domain Name System (DNS) to convert discovered IP Addresses to hostnames. An improperly configured name server results in significant performance degradation. See `Help → Help for Administrators` and view the topic *Discovering Your Network → Prerequisites for Discovery.*

IPv6 Known Problems and Limitations

- IPv6 features are not supported on any Windows operating system.
- The Management Server IPv6 Address is not displayed on the Server tab in Help → System Information on HP-UX.
- Unsupported IPv6 features; the following are not available in NNMi:
  - IPv6-only management server
  - IPv6 Network Path View (Smart Path)
  - IPv6 Subnet Connection Rules
  - IPv6 Ping Sweep for auto-discovery
  - IPv6 Address Fault monitoring through SNMP (not available for IPv4 Addresses either)
  - IPv6 Link Local Address are not supported for fault monitoring, as discovery seeds, or as Auto-Discovery hints

Device Support Known Limitations

- Device support known limitations can be found in the *HP Network Node Manager i Software (NNMi) Device Support Matrix* at sg-pro-ovweb.austin.hp.com/nnm/NNM9.20/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 9.20 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.

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)