CA Nimsoft Monitor Server

Release Notes and Upgrade Guide

7.10

Document Revision History

NMS Version	Date	Changes
7.10	Dec 2013	Revised for NMS v7.10
7.00	Sept 2013	Revised for NMS v7.00
6.50	Mar 2013	Revised for NMS v6.50
6.20	Dec 2012	Revised for NMS v6.20
6.10	Sep 2012	Updated and revised for NMS v6.10
6.00	Jun 2012	Revised for NMS v6.00
5.61	April 2012	Note on large MySQL DB update scripts
5.61	Mar 2012	Documentation updates
5.61	Feb 2012	Documentation fixes and updates
5.61	Jan 2012	Revised for NMS version v5.61
5.60	Dec 2011	Revised for NSM v5.60

Legal Notices

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Nimsoft LLC disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Nimsoft LLC shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Nimsoft LLC and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Nimsoft LLC as governed by United States and international copyright laws.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Nimsoft LLC's standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Trademarks

Nimsoft is a trademark of CA.

Adobe®, Acrobat®, Acrobat Reader®, and Acrobat Exchange® are registered trademarks of Adobe Systems Incorporated.

Intel® and Pentium® are U.S. registered trademarks of Intel Corporation.

Java(TM) is a U.S. trademark of Sun Microsystems, Inc.

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

Netscape(TM) is a U.S. trademark of Netscape Communications Corporation.

Oracle® is a U.S. registered trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of the Open Group.

ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

For information on licensed and public domain software, see the *Nimsoft Monitor Third-Party Licenses and Terms of Use* document at: http://docs.nimsoft.com/prodhelp/en_US/Library/index.htm?toc.htm?1981724.html.

Contact CA

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

Send comments or questions about CA Technologies Nimsoft product documentation to nimsoft.techpubs@ca.com.

To provide feedback about general CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: New and Changed Functionality

Nimsoft Monitor Server (NMS) 7.10 is a quality release that improves on the stability, scalability, performance, features and functionality of the product.

Component Changes

Discovery Agent and the Discovery Wizard support the discovery of IPv6 systems.

Chapter 2: Requirements

Supported Systems

Note: With version 6.50 and later, Nimsoft Monitor Server can only be installed on *64-bit* versions of supported operating systems. Details on migration of an existing NMS installation from a 32-bit system to a 64-bit system are not covered in this guide; please contact Nimsoft Support.

To provide the most current information possible, NMS system requirements are provided at the Nimsoft Support site, support.nimsoft.com.

- For a list of supported operating systems, databases, JRE versions, and browsers, see the Nimsoft Compatibility Support Matrix.
- For information on components that are being deprecated or are no longer supported, see the Nimsoft *End of Sale* (http://support.nimsoft.com/downloads/doc/Current_-_End_of_Sales_Announcement.pdf) document.

Nimsoft Infrastructure

Nimsoft Infrastructure is part of the Nimsoft Server installation. If you want to install just the Nimsoft Infrastructure (hubs, robots, or probes) on an additional UNIX® system, the following UNIX® systems are supported:

- AIX
- HP-UX
- Linux
- Solaris

More information is also available online from the Nimsoft Compatibility Support Matrix, which is updated regularly.

Additional System Requirements

- Data Engine requires libstdc++.so.5 { libstdc++-3.3.4-11.x86_64.rpm } on OpenSUSE Linux distributions
- The database must be case *insensitive* when handling queries.
- Database free space check is not implemented for Oracle and MySQL.
- If you want Discovery to locate IPv4 and IPv6 systems, discovery_agent must run on dual-stack IPv4/IPv6 system.

Supported Languages

CA Nimsoft Monitor Server is available in these languages:

- English
- Simplified Chinese
- Japanese
- Spanish
- Brazilian Portuguese

Chapter 3: Considerations

This section describes characteristics found in this release that affect version 7.10 of NMS installation, upgrade, localization, or general behavior.

System Sizing

For the latest sizing information, please refer to the section Hardware Recommendations in the *NMS Server Installation Guide*, this document is also available on the Nimsoft support download page.

Installers

The NMS installer provides these installation options:

- A **graphical user interface** (GUI) on Windows, Linux and Solaris systems
- **Console mode** on Linux and Solaris systems
- **Silent mode** on Windows, Linux and Solaris systems (you specify installation parameter values in a file that is used to complete the install with no user interaction)

For details, see the section on Server Installation in the *NMS Installation Guide,* also available on the Nimsoft support download page.

Required Login Privileges

Use a login with Administrator (Windows) or root (UNIX®) privileges when installing or upgrading to NMS 7.10. Note that if the database is:

- **Created prior to NMS installation**, the login used during installation or upgrade must map to the valid database dba credentials.
- **Created by the NMS installer**, the resulting database credentials will be automatically mapped to the login used during installation.

Install Two or More Hubs

Nimsoft recommends that you install at least two Nimsoft hubs on the same domain and network to avoid loss of user/security data (Nimsoft user definitions ACLs, etc.) in the event your primary hub system fails. With more than one hub, this information is mirrored between the hubs.

Deactivate qos_processor before Installing UMP

When installing or upgrading UMP with MySQL, deactivate the qos_processor probe before running the UMP installer. Once UMP is installed, the QoS Processor can be re-activated.

Update the Probe Provisioning Manager (ppm)

Following the completion of an NMS update:

Either using Admin Console or in Infrastructure Manager, CA Nimsoft highly recommends to *download the latest version of the ppm probe* (probe provisioning manager) from the probe archive located on the CA Nimsoft Support website (support.nimsoft.com). Updating your system to the latest ppm probe ensures that you have access to the latest Admin Console functionality.

Chapter 4: Upgrading NMS

This section explains how to upgrade to NMS 7.10.

This process consists of a chain of updates to the modules you currently have installed. Do **NOT** restart your system until all modules have been installed, even if the system prompts you to restart at intermediate points in the process.

Before You Upgrade

The NMS installers (GUI, console, and silent) let you easily upgrade NMS. When you upgrade, your configuration (domain and hub names, IP addresses, user accounts, passwords, etc.), is retained.

Before you run the installer:

- **Disable package forwarding and clear the distsrv job queue**

  Package forwarding is configured in the distsrv probe GUI. To view the queue, select Tools > Distribution in Infrastructure Manager. The upgrade will fail if the distsrv job queue has jobs pending. After a successful upgrade, re-enable package forwarding in distsrv if desired.

- **Remove customized probes in your probe archive (recommended)**

  Move or delete customized probes in your probe archive; leave the basic infrastructure probes. After all installations and upgrades are complete (especially those for UMP and Unified Reporter), you can selectively move the probes back into the archive.

- **Backup the Hub configuration (advised)**

  Save a copy of the hub.cfg file in the Nimsoft\hub folder. Optimal timeout parameters for the updated Hub are set during the update, overwriting existing timeout settings. Nimsoft recommends running the updated Hub with these optimal values for improved performance. However, if you wish to revert to the old timeout settings for any reason, keep a backup of the old Hub configuration file.

Upgrade NMS before you upgrade UMP. This ensures that UMP's required database schema is in place.

For supported upgrade paths, refer to the compatibility support matrix on the Nimsoft Support site.

Upgrading the NMS System

Upgrading NMS on Windows—GUI Mode

When you update the NMS system your existing configuration is retained, making an upgrade much simpler than a new installation.

Important: All fields in the installer dialogs are case-sensitive.

1. Turn off any anti-virus scanners running on the server (these scanners can significantly slow down the installation).

   Note: Turn the anti-virus scanners on again immediately after installation.

2. Ensure you have disabled package forwarding and cleared the distsrv job queue (required) and removed customized probes in your probe archive (recommended).
3. Log in to the Nimsoft Customer Support site.
4. Download and run the most recent NMS Install Package for Windows.
5. Follow the prompts to complete the installation. Where possible, the Installer displays the current configuration values for your confirmation.
6. When the upgrade is complete, make sure you:
   - Turn the anti-virus scanners on again if necessary
   - Enable package forwarding
   - Move customized probes back into your probe archive if necessary
   - Update other components (hubs, robots, management consoles, etc.) in your Nimsoft deployment.

Upgrading NMS on Linux or Solaris—Console Mode

When you update the NMS system your existing configuration is retained, making an upgrade much simpler than a new installation.

Follow these steps:

1. Turn off any anti-virus scanners running on the server (these scanners can significantly slow down the installation).

   Note: Turn the anti-virus scanners on again immediately after installation.

2. Ensure you have disabled package forwarding and cleared the distsrv job queue (required) and removed customized probes in your probe archive (recommended).
3. Log in to the Nimsoft Customer Support site.
4. Download and run the most recent NMS Install Package for Linux or Solaris (the package is over 1 GB, so this could take several minutes).
5. Execute **chmod 755** on the install file to make it executable.
6. Run the installer. From a command line, execute:
   - Linux: **installNMS_linux.bin -i console**
   - Solaris: **installNMS_solaris.bin -i console**
7. Follow the prompts to complete the installation. Where possible, the Installer displays the current configuration values for your confirmation.
8. When the upgrade is complete, make sure you:
   - Turn the anti-virus scanners on again if necessary
   - Enable package forwarding
   - Move customized probes back into your probe archive if necessary
   - Update other components (hubs, robots, management consoles, etc.) in your Nimsoft deployment.

Upgrading NMS on Windows, Linux or Solaris—Silent Mode

When you update the NMS system your existing configuration is retained, making an upgrade much simpler than a new installation.

Follow these steps:

1. Turn off any anti-virus scanners running on the server (these scanners can significantly slow down the installation).

   Note: Turn the anti-virus scanners on again immediately after installation.

2. Ensure you have disabled package forwarding and cleared the distsrv job queue (required) and removed customized probes in your probe archive (recommended).
3. Log in to the Nimsoft Customer Support site.
4. Download the:
   - Most recent NMS Install Package for your operating system and architecture
   - Silent install template package (.zip file)
5. On Linux or Solaris, execute **chmod 755** on the install file to make it executable.
6. Prepare your response file:
   a. Extract the silent install templates.
   b. Locate the **installer.upgrade.properties** file and save it as **installer.properties** in the same directory as the installer.
   c. Add your NMS administrator password to the **NMS_PASSWORD=** line in **installer.properties**.
   d. Save the file, ensuring the file type is still **PROPERTIES**. If the file type is **Text Document**, remove the **.txt** extension (which may not be displayed in the folder).
7. Run the installer. From a command line, execute:
   - Windows: **installNMS.exe -i silent**
   - Linux: **installNMS_linux.bin -i silent**
   - Solaris: **installNMS_solaris.bin -i silent**
8. The installer unpacks the files and completes the installation. This process can take several minutes or more. To see the progress of the installation, execute:
   ```
   tail -f /tmp/ia/iaoutput.txt
   ```
9. NMS launches. If for some reason it does not, execute:
   - Windows: **net start Nimsoft Robot Watcher**
   - Linux or Solaris: **cd /etc/init.**d then **nimbus start (**or **/etc/init.d/nimbus start**)

10. When the upgrade is complete, make sure you:
    - Turn the anti-virus scanners on again if necessary
    - Enable package forwarding
    - Move customized probes back into your probe archive if necessary
    - Update other components (hubs, robots, management consoles, etc.) in your Nimsoft deployment.

Upgrading NMS on a MS Server Cluster

On an MS Server 2003/2008/2008 R2 Failover Cluster:

1. Upgrade NMS on the primary (active) node using one of the Windows upgrade procedures. Refer to:
    - Upgrading NMS on Windows with the Install Wizard GUI (see page 14)
    - Upgrading NMS on Windows, Linux or Solaris with Silent Mode (see page 16)
2. Make the secondary (passive) node active, then upgrade NMS using the same process you used on the primary node.

This ensures that registry keys on both the primary (active) and secondary (passive) nodes are updated for the new version.

Updating NMS Clients

Update Infrastructure Manager

On all servers and workstations that have Infrastructure Manager installed (verify by checking **Start > All Programs > Nimsoft Monitoring**), you should upgrade to the newest version.

1. Open a web browser on the machine you want to upgrade Infrastructure Manager, and access the Nimsoft Monitor Server web page at the URL: <servername_or_server_IP_address>:8080.
2. On the web page that appears, choose the link **Legacy Infrastructure Manager** to install the new version on that machine.
3. Repeat this procedure to upgrade additional machines.

Note: **Nimsoft Monitor Admin Console** is a new management console that provides a platform-independent alternative to Infrastructure Manager. It can be launched stand-alone in a browser using the link provided above the link for installing **Legacy Infrastructure Manager.** Alternatively, it can be installed as a portlet running within UMP.

Update Hubs

1. Identify any systems which contain a secondary Hub and Infrastructure (view in Infrastructure Manager; confirm by checking **Control Panel->Add/Remove** programs on the client system itself).

   Note: Updating secondary hubs may be necessary only if updating from two or more versions back. Check the section Verification of Successful Installation or Upgrade (see page 20) for hub and component versions included in this release, and compare to your currently installed secondary hubs.

2. Save a copy of the hub.cfg file in the Nimsoft\hub folder on the system. Optimal timeout parameters for the updated Hub are set during the update, overwriting existing timeout settings. Nimsoft recommends running the updated Hub with these optimal values for improved performance. However, if you wish to revert to the old timeout settings for any reason, having a backup of the old Hub configuration file makes this possible.
3. On the client computer, browse to your NMS web page (http://<servername_or_IP_address>:8080).
4. On the web page that appears, choose the link **Windows Robot, Hub, Distribution Server** to upgrade the Nimsoft Hub and Infrastructure on that machine.
5. Follow the prompts to complete the installation.
6. Repeat this procedure for additional hub upgrades.

Update Hub Queues for Discovery

After an upgrade, ensure that information from any distributed probes that are involved in discovery can reach the discovery_server. To do this:

1. Create an *attach* queue for the **probe_discovery** subject on all secondary hubs that host discovery_agent, vmware, or cm_data_import.
2. Configure a *get* queue with subject **probe_discovery** on each hub, except for those at the bottom of the hub hierarchy.

Refer to the *Discovery User Guide* for details on configuring queues for discovery.

Note: If all discovery components are located under the primary hub, this communication is handled automatically. No manual queue configuration is required.

Update Robots

Use one or more of the following procedures.

Windows, method 1

1. Launch Infrastructure Manger on your upgraded server (or another hub with an updated archive). Within the Archive, locate the **robot_update** package.
2. Drag and drop this package from the Archive onto the icon of the robot you want to update.

Windows, method 2

1. Identify other systems that contain a Nimsoft Robot (view with Infrastructure Manager, confirm with **Control Panel > Add/Remove** programs on the client system itself.)
2. On the client computer, browse to your NMS web page (http://<servername_or_server_IP_address>:8080).
3. Choose the link **Windows Robot** to install the Nimsoft Robot on that machine.
4. Repeat this procedure for additional robot upgrades.

Linux or Solaris

1. Similar to the procedure for Windows systems described above, drop the **robot_update** package from an updated Archive onto the icon of the Robot you wish to update.
2. Repeat the procedure for additional robots upgrades.

Mass-deploy robot updates

You can build a group or groups of non-Hub robots in Infrastructure Manager, then mass-deploy the robots.

Hub robots

Update hub robots individually by dropping **robot_update** on each robot icon.

Verification of Successful Installation or Upgrade

Nimsoft recommends you check the results of the installation process in order to detect any failure(s). Three indications of success:

- You see **Nimsoft Server 7.10** on the NMS web page.
- You have current versions of all components in the Infrastructure Manager main window and for the user interfaces (select **Help > About** to check the version).
- The new mpse probe shows up either in Infrastructure Manager or Admin Console.

Note: These tables list the version numbers of probes provided with NMS 7.10. On occasion, Nimsoft provides newer versions of certain probes between server package releases. The latest probe updates are placed on the Nimsoft Support website http://support.nimsoft.com (**Download** and **Archive** pages) as they are made available.

Important: Normal operation of running the Nimsoft installer during an upgrade is to overwrite currently installed probes and components. In some cases, when "hot fix" probes or special/updated versions of components were installed previously to solve issues or support customized requirements, updating can result in component downgrades. If this happens, the required components and probe versions can be restored by locating them in the NM Server Archive, and installing them in place of what the upgrade provided.

User Interfaces	**Version 7.10**	**Prior release**
Infrastructure Manager	4.08	4.08
Admin Console	7.10	7.00
Dr. Nimbus	1.5.3	1.5.3
Backend components	**Version 7.10**	**Prior release**
alarm_enrichment	4.20	4.20
audit	1.22	1.22
automated_deployment_engine	1.24	1.23
baseline_engine	1.10	1.0
cm_data_import	7.00	7.00
controller	7.10	7.00
data_engine	7.92	7.91
distsrv	5.30	5.30
fault_correlation_engine	1.66	1.65
hdb	7.10	7.00

hub	7.10	7.00
nas	4.20	4.20
nimldr	3.57	3.57
nis_server	3.10	3.00
mpse	1.10	1.00
ppm	2.20	2.12
qos_engine	2.67	2.67
qos_processor	1.21	1.20
relationship_services	1.69	1.69
robot_update	7.10	7.00
service_host	1.10	1.03
sla_engine	3.61	3.60
spooler	7.10	7.00
Discovery components	**Version 7.10**	**Prior release**
ace (multiplatform version)	3.10	3.00
assetmgmt	1.24	1.24
cisco monitor	3.35	3.35
cm_data_import	7.00	7.00
cdm	4.76	4.73
discovery_agent	7.10	7.00
discovery_server	7.10	7.00
interface_traffic	5.33	5.33
net_connect	2.94	2.94
rsp	3.07	3.05
topology_agent	1.68	1.68

Chapter 5: Known Issues

This section describes known issues and workarounds in some cases.

Performance, Stability, Scalability

Potential Impact of Inactive Queues

When used a tunnel server, the number of resources used for Windows file handles and Unix file descriptors may grow steadily over time. The growth rate increases greatly when the tunnel server is servicing one or more *get* queues that carry little or no data, and therefore reset regularly. To limit exposure, we highly recommend that you:

- Configure only get queues you expect to carry data.
- Set the process file descriptor limit to at least 2048 for tunnel servers (Unix platforms).

As the number of resources in use becomes large, the hub may need to automatically restart. No data loss is expected during these restarts, and the system should automatically return to normal operation. If time taken by this restart proves unacceptable, it can be decreased by setting the probe_alive_check parameter in robot raw configuration to 30 seconds. In extreme cases, the hub's built-in therapeutic restart capability can be used to ensure fast periodic restart. Contact Nimsoft support for more information about therapeutic restart.

Automated Deployment Engine (ADE)

ADE robot distribution to Windows targets sometimes fails to activate the hdb and spooler probes.

To resolve this issue, go to the affected machine and do a **validate security** on the affected probes (hdb and spooler).

Slow Restart of discovery_server on MySQL

When Discovery Server starts, it executes a script to check/create tables in the NiS database. In version 5.5 of MySQL there is a bug (see http;//bugs.mysql.com/bug.php?id=63144 and http://dev.mysql.com/doc/relnotes/mysql/5.6/en/news-5-6-13.html) that causes this script to run slowly.

Upgrading MySQL to version 5.6.13 or later resolves the issue.

When using the 5.5 stream of MySQL, the workaround is to turn off dashboard_engine and terminate any outstanding queries when restarting discovery server--this allows the discovery creation script to proceed.

Red Hat Enterprise Linux (RHEL)

Nimsoft processes on RHEL 6.1 x86-64 consume more memory than on other Linux platforms.

- **RHEL v6 64-bit systems**

  Processes can take up to three times the amount of virtual and resident memory per process compared to previous releases of RHEL or other operating systems.

- **RHEL v6 32-bit systems**

  Processes can take several times more virtual memory, but resident memory per process are roughly equivalent.

Usability

"SSL Certificate Not Trusted" Message in Admin Console

If you configure the service_host probe to use secure communication between server and the browser that is running Admin Console, a self-signed certificate is created by the service_host process. When launching Admin Console stand-alone (not within an UMP portlet), you may see an 501 error informing you that the certificate is untrusted. You can either choose to ignore this message and continue, or configure the browser to trust the certificate. Alternatively in some cases, it may advantageous to provision a certificate from a Certificate Authority (CA) and install it on the NMS. If the certificate is from a known commercial source, browsers will recognize it without additional configuration.

An ssl certificate will be coded to a specific host name (foo.bar.com), or a range of hosts in a domain (*.bar.com). If one were to contact the server by IP address (for example, https://1.2.3.4:8443), the browser displays an untrusted certificate warning. Contacting the server with https://foo.bar.com:8443 does not receive such a warning because the URL used matches the host name in the SSL certificate. Specify the hostname in the **DNS name** field in the service_host configuration GUI. See the service_host online help -- under the topic titled "Configuration Details" -- for more reference information.

For procedural information on configuring SSL certificates for Admin Console in service_host, refer to the section on "Managing Security" in the online documentation for Admin Console, also available in the Nimsoft documentation library.

Admin Console Cannot Accept SSL Certificate in UMP

Problem:

This issue is seen when Admin Console is configured to use a self-signed SSL certificate for communication with the service_host process on NMS.

When launching Admin Console as a portlet within UMP for the first time, you receive a 501 error that the self-signed SSL certificate is untrusted, but are not provided with any means to accept the certificate and continue. This is due to a limitation on how some browsers handle SSL-certificates within a secure iframe.

Solution:

To work around this issue, first open Admin Console stand-alone in a web browser (https://<NMS_host>:8443) where you will see the same security message, but are be able to accept the certificate. Afterwards Admin Console will open within UMP (on the same browser at the same IP address) without this issue.

Alternatively, in the error dialog within UMP that the browser shows ("certificate is not trusted; unable to establish communication to <URL>"), copy the URL given and paste into another browser window or tab (in the same browser as is running UMP) and accept the certificate there. Return to UMP and reload the page to clear the 501 error.

NIS Manager Link in Infrastructure Manager Does Not Work

Symptom

When I click on the NIS Manager link in Infrastructure Manager, I get an error message: "Error executing command: C:\Program Files (x86)\Nimsoft\bin\NiSmgr.exe."

Cause

The NIS Manager application has been removed from NMS. To configure discovery components, use the Discovery Wizard located in the USM portlet.

Using SSH Password Authentication wtih OpenSUSE 12.x

By default OpenSUSE disables password authentication for SSH. If you wish to use password authentication for SSH, you must:

- Change the **PasswordAuthentication no** entry to **PasswordAuthentication yes** in the /etc/sshd_config file.

If you do not use password authentication, you must use RSA public key authentication. Refer to the section "Parameter Values for host-profiles.xml" in Appendix A: Bulk Deployment with Automated Deployment Engine in the NMS Installation Guide (available in the Nimsoft documentation library).

PPM Not Supported on AIX

The PPM probe will not run on AIX hubs. To configuring robots and probes on, or under AIX hubs, use the web-based raw configure or legacy Infrastructure Manager.

Windows 2008 Permission Issues

Write privileges are required for writing to the Nimsoft program files folder. If you log on as a user without administrator privileges after installation, you must manually set these write privileges.

Single Time Zone Required

For data time-stamping to work correctly across a distributed Nimsoft deployment, the NMS server, the UMP server, and the database server must all be set to the same time zone, regardless of the geographic locations of the servers.

Fault Correlation Affected by Alarm Forwarding and Replication

Problem:

Fault Correlation is impacted by the configuration of hub alarm forwarding and NAS alarm replication.

Solution:

For the Fault Correlation application to provide accurate results, you must ensure that alarms and interface_poller messages from hubs in the applicable areas of your network topology are being forwarded to the hub where the Fault Correlation Engine (FCE) probe is running. You must use hub queues that include subjects alarm and interface_poller to forward the messages FCE requires. Use either POST or GET queues based on whether you want to push or pull messages from one hub to the next.

Important: Do not enable NAS alarm replication or forwarding when using FCE. Doing so causes alarms to be processed twice and yields unpredictable results.

UNIX Robot Communication Fails Due to Invalid /etc/hosts

Problem:

On non-Windows systems, robot communication over the network fails due to invalid /etc/hosts file.

Solution:

Ensure the **/etc/hosts** file on any system hosting a Nimsoft robot, hub, server, or UMP instance contains a valid entry for the local machine. This must be a fully qualified hostname and IP address pair. If only loopback is defined (for example, localhost 127.0.0.1), then the Controller probe on that machine will be unaware of its own IP address, resulting in network communication failure.

Unable to Find Device in USM by IP Address

As part of 7.0 discovery server and discovery agent enhancements, a device with multiple IP addresses is now shown as a single device in Unified Service Manager (USM), not as multiple distinct devices per IP address. If you can't locate a device in USM by an IP address, try searching for it by name.

Localization

Translated strings are garbled in the installation log file (iaoutput.txt).

Installation

Installation Fails Due to Java JRE Version

The installer pre-check may flag an issue with the Java Runtime Environment (JRE) if it finds Java 6 version 29 or 30 (JRE 1.6.29 or 1.6.30).

Note: There is a known issue with JRE versions 1.6.29 and 1.6.30 (Java 6 versions 29 and 30) when working with MS SQL Server (See: http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=7105007).

Nimsoft recommends that you install the most recent update of either JRE SE 6 or SE 7, depending on which version you are using. For JRE 6, this is currently JRE 1.6u43 (Java 6 update 43). For JRE 7, this is 1.7u17 (Java 7 update 17).

Note: Installing on Windows Server 2012 requires JRE 1.6u38 / 1.7u6, or later, so that the operating system platform is properly detected.

Solaris-only:

The installer pre-validation flags when a 32-bit JRE is installed on a 64-bit Solaris platform. With Solaris, use of 64-bit JRE as the reference JRE for NMS is mandatory.

- Ensure you have a 64-bit JRE installed before running the installer.
- Further, check your PATH to see if (1) a 64-bit JRE is listed, and (2) listed before any 32-bit JRE.

Note: Solaris differs from other platforms in that the 64-bit JRE is located one directory deeper.

On AMD64 systems, the full path to the 64-bit JRE directory is typically:
`/usr/java/jre/bin/amd64`

On SPARC systems, the full path to the 64-bit JRE directory is typically:
`/usr/java/jre/bin/sparcv9`

- Verify the PATH includes the 64-bit JRE directory and then re-run the installer.

Discovery Agent and Other Probes Issue Alarm on Update

Symptom

Discovery Agent and some other probes may send a single informational alarm when upgrading to the latest version of NMS. This alarm is benign and can be safely ignored.

Cause

Discovery Server creates a bus queue that these other probes depend on. The queue may not be entirely operational when these probes activate, which causes the informational alarm to be sent. The queue will come up in a short period of time.

NMS Installation fails on CentOS, OpenSuse, and RHEL

Symptom

NM Server installation fails on CentOS, OpenSUSE version 12, or RHEL 32-bit.

Cause

The Data Engine requires libstdc++.so.5 { libstdc++-3.3.4-11.x86_64.rpm }

Installing the compatible lib resolves the problem.

Issue this command:

```
yum install compat-libstdc++-33
```

Remote Web-based Configuration Requires PPM

To use web-based configuration for any remote hub, or robots/probes under that hub, PPM needs to be distributed to that hub. Nimsoft recommends that PPM be deployed to each hub within your domain.

Probe Restart Fails After Installation

- **NMS installation on Windows**

  After NMS installation on Windows systems, some probes may not start due to lack of available system resources.

  To fix this, edit registry key HKEY_LOCAL_MACHINE\System \CurrentControlSet \Control \Session Manager\SubSystems\Windows:

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512,Windows=On
SubSystemType=Windows ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
```

  Change the value 512 (in **bold** text in the example above) to **1024**.

  For more information, see the article at http://support.microsoft.com/kb/184802.

- **NMS installation on all platforms**

  Several components are distributed and configured during NMS installation. On slower systems, some probes might not be started after installation. This can be detected in Infrastructure Manager or Admin Console and is fixed by manually activating the probe.

- **NMS upgrade on all platforms**

  If you upgrade NMS and you have UMP installed, restart the **wasp** and **dashboard_engine** probes to avoid any issue logging into UMP after the upgrade.

UMP Installation on MySQL

MySQL users must deactivate the QoS_processor probe before installing or upgrading UMP on NMS 6.50. Once UMP is installed, the QoS Processor can be re-activated.

Name Resolution Conflicts on Debian v6 with ADE

By default Debian v6 uses the address 127.0.1.1 as the name resolution address. When a robot is deployed to a Debian 6 system using ADE, after system restart the robot will attempt to bind to 127.0.1.1 as the address it is available at. Use the following workaround to avoid contention for 127.0.1.1 on your Debian 6 system:

1. When installing the robot *manually*, or with *ADE*, you must go to the target system after the fact and add the following line to the robot.cfg file:

   ```
   robotip = ip_address
   ```

   where **ip_address** is the desired IP address that the robot should bind to on the target machine.

2. When deploying to a Debian 6.0.5 box using *XML*, you must define the **<robotip>ip_address</robotip>** option, where **ip_address** is the IP address that the robot should bind to on the target machine.

LDAP User and Group Requirements for NMS Login

An LDAP user cannot log into NMS unless the Active Directory user is a member of the LDAP domain admin group. The LDAP group policy on NMS does not matter.

Silent Install with SQL Server and Dynamic Ports Requires DB-PORT

If you are installing with MS SQL Server named instances or SQL Server Express and you are using dynamic ports, you cannot use the default port number (1433), as this will prevent data_engine from connecting to the database.

Data_engine will be green in Infrastructure Manager (because it is running) but the lack of connection will cause its queue to grow in size continuously.

If the default port was used:

1. In Infrastructure Manager, open the data_engine probe configuration GUI by double-clicking the data_engine object.
2. On the **Database** tab, delete the comma and port number (**,1433**) appended to the database server name.
3. Specify the correct port, then restart the probe.

Failed Solaris Installation Reduces Available Swap Space

If NMS installation is interrupted or fails for any reason, the installer files (/tmp/install.*) are not deleted. Because Solaris swap includes the /tmp directory, Nimsoft recommends that you manually delete these files before running the installer again.

Linux with MySQL: access denied for root user

Problem:

When attempting to install NMS with a MySQL database, you may see the following error (or its equivalent) after you enter the database server information:

```
ERROR 1045 (28000): Access denied for user 'root'@'<your Nimsoft hostname>' (using password: YES)
```

This occurs either because remote privileges have not been established, or because the password identified for remote systems is not consistent with what is set on the database server locally.

Solution:

Perform these steps:

1. Login to the MySQL database locally (i.e. on the actual server hosting MySQL).
2. To set up access from any host, execute:

```
mysql> use mysql;
mysql> UPDATE user SET password=PASSWORD("<your password>") where User = 'root';
mysql> GRANT ALL PRIVILEGES ON *.* TO root@'%' IDENTIFIED BY '<your password>' WITH GRANT OPTION;
mysql> GRANT TRIGGER ON *.* TO root@'%' IDENTIFIED BY '<your password>';
mysql> GRANT SUPER ON *.* TO root@'%' IDENTIFIED BY '<your password>';
mysql> FLUSH PRIVILEGES
```

To set up access from a particular host, execute these commands, replacing *HostX* with the name of your host:

```
mysql> use mysql;
mysql> UPDATE user SET password=PASSWORD("<your password>") where User = 'root' AND Host = 'HostX';
mysql> GRANT ALL PRIVILEGES ON *.* TO root@'HostX' IDENTIFIED BY '<your password>' WITH GRANT OPTION;
mysql> GRANT TRIGGER ON *.* TO root@'HostX' IDENTIFIED BY '<your password>';
mysql> GRANT SUPER ON *.* TO root@'HostX' IDENTIFIED BY '<your password>';
mysql> FLUSH PRIVILEGES;
```

Invalid IP Error when Installing Windows Intrastructure

Problem:

When you run **NimBUS Infrastructure.exe** to install the Windows robot, hub and dstribution server, you may see the following error:

```
Command Line IP is not valid: 127.0.0.1
```

Solution:

This error is harmless and can safely be ignored. Click OK and continue.

Chapter 6: Defects Fixed

This section describes defects (organized by category) that were fixed in NMS 7.10.

Performance, Stability, Scalability

- Discovery Server failed on MySQL during startup when there were duplicate entries in DS_ROBOT_XREF.
- Discovery Server 7.0 did not respond appropriately to origins with spaces/commas.
- Unknown information was shown from a Windows 2012 R2 system.
- XML logging flooded the log on anything above level 3.

Usability

- Administrators could not change the *dedicated* field on a switch discovered as router.