

CA Nimsoft Monitor Server

Release Notes and Upgrade Guide

6.50



Document Revision History

NMS Version	Date	Changes
6.50	Mar 2013	Revisions for NMS v6.50
6.20	Dec 2012	Revisions for NMS v6.20
6.10	Sep 2012	Updated and revised for NMS v6.10
6.00	Jun 2012	Revisions 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	Revisions for NMS version v5.61
5.60	Dec 2011	Revisions for NSM v5.60

Legal Notices

Copyright © 2013, CA. All rights reserved.

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 Nimsoft

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	7
Component Changes	8
Chapter 2: Requirements	9
Supported Systems.....	9
Nimsoft Infrastructure	9
Additional System Requirements.....	9
Supported Languages.....	10
Chapter 3: Considerations	11
System Sizing.....	11
Installers	11
Required Login Privileges	11
Install Two or More Hubs	12
Deactivate qos_processor before Installing UMP	12
Update the Probe Provisioning Manager (ppm)	12
Chapter 4: Upgrading NMS	13
Before You Upgrade	13
Upgrading the NMS System	14
Upgrading NMS on Windows—GUI Mode.....	14
Upgrading NMS on Linux or Solaris—Console Mode.....	15
Upgrading NMS on Windows, Linux or Solaris—Silent Mode.....	16
Upgrading NMS on a MS Server Cluster.....	17
Updating NMS Clients	17
Update Infrastructure Manager	17
Update Hubs	18
Update Robots	18
Verification of Successful Installation or Upgrade	20
Checking the database upgrade.....	22
Chapter 5: Known Issues	23
Performance, Stability, Scalability.....	23
Automatic Deployment Engine (ADE)	23
Red Hat Enterprise Linux (RHEL)	23

Usability.....	24
"SSL Certificate Not Trusted" message when launching Admin Console.....	24
AdminConsole: Unable to accept SSL certificate within UMP	24
AdminConsole doesn't function after hub restart	25
ADE: Using SSH password authentication with OpenSUSE 12.x	25
ADE: Installing Robots on Debian v6	25
PPM probe not supported on AIX	26
Windows 2008 permission issues	26
Single Time Zone Required.....	26
Hub alarm forwarding and NAS alarm replication affect Fault Correlation	26
UNIX: Robot communication fails due to invalid /etc/hosts.....	27
Localization.....	27
Installation.....	28
Installation Fails Due to Java JRE Version.....	28
Recommended: Deploy PPM to each hub in your domain	28
Some probes may not start after installation	29
UMP Installation on MySQL	29
LDAP authentication: Non-domain admin group users cannot log in to NM Server	29
Silent install with SQL Server: DB_PORT value required with dynamic ports	30
Solaris: Failed installation reduces available swap space	30
Linux with MySQL: access denied for root user	30
Windows: Invalid IP error when installing infrastructure	31

Chapter 6: Defects Fixed **33**

Performance, Stability, Scalability.....	33
Security.....	33
Usability.....	33

Chapter 1: New and Changed Functionality

Nimsoft Monitor Server (NMS) 6.50 is a major release that improves on the stability, scalability, performance, features and functionality of the product, adding these significant new features:

- Web-based **Admin Console**: this new interface provides browser access for managing the Nimsoft Management infrastructure and configurations for select probes:
 - adevl
 - apache
 - cdm
 - dhcp_response
 - iis
 - ntevl
 - ntperf
 - perfmon
 - smsgtw
 - sql_response
 - url_response
- New port assignments: Admin Console is hosted by NMS on **Port 8443**; the **new NMS webpage** is available on port **8080**, previously 8008
- Automated **discovery wizard** for streamlined device discovery setup (wizard is accessed in USM; discovery no longer a part of NMS install)
- **File-based import** to quickly import device information
- New QoS metric **baseline** calculator (baselines displayed with QoS data in UMP graphs)
- Improved **Unified Reporter** look-and-feel, plus improved OOB reports.

Component Changes

- New **baseline_engine** probe calculates baselines for all or selected metrics--forwards the baseline information to the revised **qos_processor** which stores baseline data in the NIS database
- **topology_agent** now bundled in with the standard NMS installation
- **data_engine** provides a new option to compress indexes (MS-SQL only)
- New **cm_data_import** probe handles file-based device information import in conjunction with the new **Discovery Wizard** in USM.

Chapter 2: Requirements

Supported Systems

Note: As of version 6.50, Nimsoft Monitor Server can now 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 document:

<http://support.nimsoft.com/Files/Announcement/current - end of sales announcement.pdf>

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

- If you are using MySQL 5.1, make sure that you are running version 5.1.16 or later. NMS 6.50 requires support for REFERENTIAL_CONSTRAINTS.
- The database must be case *insensitive* when handling queries.
- Database free space check is not implemented for Oracle and MySQL.

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 6.50 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

NMS installation makes use of an InstallAnywhere installer, which unifies installation under Windows, Linux, and Solaris. The legacy InstallShield Windows-only installer is no longer supported.

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 6.50. 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 NMS 6.50 and 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 6.50.

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.

You should upgrade NMS before you upgrade UMP, so that required database schema that UMP depends on 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: either **cd /etc/init.d** or **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 Robots

Use one or more of the following procedures.

Windows, method 1

1. Launch Infrastructure Manager 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

After installation Nimsoft recommends you check the output of the installation process closely in order to detect any failure(s). Two indications of success:

- You see **Nimsoft Server 6.50** 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)
- You see the new probes included in NMS 6.50:
 - service_host probe: container for all components related to the Admin Console; communicates using port 8080 (NMS web page) and port 8443 (Admin Console) by default
 - PPM probe: supports web-based probe provisioning; needs to be distributed to each hub in the Nimsoft domain so that robots and probes under those hubs can be configured through Admin Console
 - cm_data_import probe: imports device discovery information into the NIS database
 - baseline_engine: calculates baselines for QoS metrics.

Note: These tables list the version numbers of probes provided with NMS 6.50. 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 6.50	Prior release
Infrastructure Manager	4.07	4.06
Dr. Nimbus	1.5.3	1.5.3
Backend components	Version 6.50	Prior release
alarm_enrichment	4.20	4.10
audit	1.22	1.21
automated_deployment_engine	1.21	1.20
baseline_engine	1.0	new in NMS v6.50

cm_data_import	6.50	new in NMS v6.50
controller	5.70	5.70
distsrv	5.30	5.30
hdb	5.70	5.70
hub	5.82	5.82
spooler	5.70	5.70
nas	4.20	4.10
robot_update	5.70	5.70
nis_server	2.72	2.71
httpd	n/a	1.49
nimldr	3.57	3.56
data_engine	7.91	7.90
fault_correlation_engine	1.65	1.64
NOD Relay installer	6.50	6.20
PPM	2.00	new in NMS v6.50
qos_engine	2.67	2.65
qos_processor	1.20	1.11
relationship_services	1.68	1.66
service_host	1.02	new in NMS v6.50
sla_engine	3.59	3.58
Discovery components	Version 6.50	Prior release
ace (multiplatform version)	2.72	2.71
assetmgmt	1.24	1.24
cisco monitor	3.32	3.31
cm_data_import	6.50	new in NMS v6.50
cdm	4.70	4.70
discovery_agent	6.50	3.50
discovery_server	6.50	3.50
interface_traffic	5.23	5.23
net_connect	2.90	2.81
rsp	2.92	2.90

topology_agent	1.68	now included in NMS 6.50
Redist	Version 6.50	Prior release
VS-2008 REDIST x86	1.0	1.0
VS-2008 REDIST x64	1.0	1.0

Checking the database upgrade

The best way to check that the database schema update is successful is to use a SQL tool (e.g. **SLM Manager->Tools->SQL Query**) and execute the following statement:

```
select * from tblVersion  
where ModuleName = 'NIS_DATAENGINE'
```

This query should return:

- **4.86** (SQL and MySQL)
- **4.85** (Oracle).

Chapter 5: Known Issues

The following sections describe known issues and workarounds in some cases.

Performance, Stability, Scalability

Automatic 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).

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 when launching Admin Console

A self-signed certificate is created by the service_host process in NMS to encrypt communication between the server and the browser that is running Admin Console. When launching Admin Console stand-alone, you get an 501 error 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 purchase a certificate from a Certificate Authority (CA) and install it on the NMS.

For more information on SSL certificates, refer to the documentation on "Self-signed SSL Certificates" in the UMP online help, available in the Nimsoft documentation [library](#).

AdminConsole: Unable to accept SSL certificate within UMP

Problem:

When launching Admin Console as a portlet within UMP for the first time, you receive a 501 error that the self-signed SSL certificate generated by the service_host probe 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 you will be able to accept the certificate there. 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.

AdminConsole doesn't function after hub restart

Problem:

Occasionally, after a restart of a hub that hosts the service_host probe, you find that you are unable to connect to the Admin Console. Troubleshoot the problem by checking the service_host.log file—look for a recent message that includes the text **failed looking for data_engine on hub**. This issue typically is only seen following a restart of the hub, and is not seen in a system that has been running continuously.

Solution:

Restart your service_host probe. When service_host, the container probe for Admin Console functionality, loses contact to the data_engine, a restart of service_host addresses the issue as a workaround.

ADE: Using SSH password authentication with OpenSUSE 12.x

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

1. Open the /etc/sshd_config file with an editor
2. Locate the entry "PasswordAuthentication no" and change this to "PasswordAuthentication yes"
3. Save the file and close the editor.

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. Documentation is available in the Nimsoft documentation [library](#).

ADE: Installing Robots on Debian v6

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 box after the fact and add the following line to the robot.cfg "robotip = ip_address" where ip_address is the desired ip that the robot should bind to on the target machine.
2. When deploying to a Debian 6.0.5 box using XML, you must specify the "<robotip>ip_address</robotip>" option, where ip_address is the address that the robot should bind to on the target machine.

PPM probe 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.

Hub alarm forwarding and NAS alarm replication affect Fault Correlation

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.

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 may flag an issue for a 32-bit JRE on a 64-bit Solaris platform. In this case we recommend you check your PATH to see if (1) the 64-bit JRE is listed, and (2) listed before the 32-bit JRE. 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.

Recommended: Deploy PPM to each hub in your domain

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.

Some probes may not start 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=0n  
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.

LDAP authentication: Non-domain admin group users cannot log in to NM Server

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: DB_PORT value required with dynamic ports

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.

Solaris: Failed 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;
```

Windows: Invalid IP error when installing infrastructure

Problem:

When you run **NimBUS Infrastructure.exe** to install the Windows Robot, Hub, Distribution server, you may see the following error:

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

Solution:

This error is benign and can safely be ignored. Simply click OK and continue.

Chapter 6: Defects Fixed

This section describes defects (organized by category) that were fixed in NMS 6.50.

Performance, Stability, Scalability

NAS

NAS 4.10 unable to connect to Oracle 11g (DE19920)

NMS Installer

Installer doesn't check for custom archive location (set by distsrv) (DE6509)

data_engine

Database connection alarms do not clear after connection is restored (DE19652)

Maintenance job causes database to grow in size (DE19383)

Maintenance job causes overuse of system resources (DE20215)

rsp probe

Auto-discovery WMI credentials not transmitted correctly (DE16408).

Security

Nimsoft Infrastructure

During DMZ installation, user-specified expiration date for server certificate is not honored (DE19823).

Usability

Alarm Enrichment

<NULL> values added to custom alarm fields (DE20201).