Nimsoft® Monitor™ Server

Release Notes and Upgrade Guide

version 6.00

Document Revision History

NM Server Version	Date	Changes
5.60	12/5/2011	Revisions for v5.60
5.61	1/9/2012	Updated and revised for NMS v5.61
5.61	2/22/2012	Documentation fixes and updates
5.61	3/14/2012	Documentation updates
5.61	4/3/2012	Note on large MySQL DB update scripts
6.00	6/29/2012	Revisions for v6.00

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.

Contact Nimsoft

For your convenience, Nimsoft provides a single site where you can access information about Nimsoft products.

At http://support.nimsoft.com/, you can access the following:

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

Provide Feedback

If you have comments or questions about Nimsoft product documentation, you can send a message to support@nimsoft.com.

Contents

Chapter 1: New and Changed Functionality

Nimsoft Monitor Server (NMS) 6.0 is a quality release that improves upon the stability, scalability, performance, features and functionality released in NMS 5.6.

Component Changes and Fixed Problems

ACE (2.65)

- In groups with multiple device types, templates are only applied to computer systems–not to devices such as printers or routers.
- When a computer system's state is set to **Unmanaged**, any monitors that were applied are automatically removed.

Automated Deployment Engine (ADE)

- ADE probe provides a mechanism and GUI for bulk deployment of robots.

Discovery Server and Agent

- Discovery Server can run a non-primary hub. By default, discovery server runs on the primary hub, where data_engine is running. Discovery server can run on a different hub as long as discovery server can communicate with the data_engine probe and the database server. See the Discovery Server 3.40 Release Notes for details.
- Improved configuration and handling of service definitions for Service Discovery. Discovery Server 3.40 has a pre-defined set of service definitions for well-known network services such as HTTP, FTP, and email. Discovery Agent 3.40 lets you enable or disable individual service definitions and configure how new definitions are handled.
- Discovery Server can now handle up to 200 Discovery Agents.
- The memory footprint for Discovery Server in large environments has been reduced, with support for up to 5000 robots using the default maximum Java heap size of 1 GB.
- Improvements have reduced the number of sockets and database connections.
- Fixed database transaction deadlocks seen with MS SQL Server.
- Fixed SQL error cases.

Installation

- Silent install mode for the InstallAnywhere installer is supported on Windows, Linux and Solaris systems.

nas (4.00)

- Incorporated alarm enrichment functions into nas.

nimldr (3.54) and install_unix (6.00)

- Removed nas support

nis_server (2.00)

- Enhancements to support functionality that will be available with UMP 6.0.

qos_engine (2.65)

- Fixed MySQL non-standard database port defect
- Installed but not started/activated with NMS v6.00 (new install or update); manual activation by the user is necessary.

qos_processor

- The qos_processor probe works with the data_engine probe and the NIS database to maintain the correct origin even with changes to the robot and hub. Prior to NMS 6.0, the origin field of the S_QOS_DATA table was not updated if an origin reassignment occurred at the robot or hub.
- The qos_processor also allows you to modify the origin and other select QoS monitor attributes using script-based enrichment. You can assign the origin field of the S_QOS_DATA table based on the outcome of applying rules to monitor attributes such as QOS, SOURCE, TARGET. If an enrichment script exists for QOS_MESSAGE, it will override an origin change done on the hub. These changes allow UMP portlets such as list viewer to reflect the correct origin associated with QoS data sent from the probes.
- See the qos_processor online documentation for details.

Chapter 2: Requirements

The following sections describe supported environments for Nimsoft Monitor Server (NMS).

Supported Systems

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

- For a list of supported operating systems, databases, and browsers, see the Nimsoft Compatibility Support Matrix:

  http://support.nimsoft.com/downloads/doc/Compatibility_SupportMatrix_current.pdf

- 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 using MySQL 5.1, please ensure that you are running version 5.1.16 or later. NM server 6.00 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

Nimsoft 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 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* available on the Nimsoft support download http://support.nimsoft.com page.

New and Legacy Installers 6.00

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

The installer guides you through installation by means of:

- 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 *NMS Installation Guide* on the Nimsoft support download page http://support.nimsoft.com.

Required Login Privileges

Use a login with Administrator (Windows) or root (UNIX®) privileges when installing or upgrading to NMS 6.0. 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.

Installing one or more Hubs?

It is recommended that at least two Nimsoft Hubs should be installed on the same Domain and network to avoid loss of user/security data--such as Nimsoft user definitions ACLs, etc., in case your Hub computer crashes. With more than one Hub, this information is mirrored between the Hubs.

Chapter 4: Upgrading Nimsoft Server

Following is the recommended sequence of steps involved in upgrading a Nimsoft domain consisting of several hubs and robots.

The upgrade of NM server 5.61 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 you receive system prompts to restart at intermediate points in the process

Before You Upgrade

The NMS Installers (wizard-based, console-based, and silent) let you easily upgrade NMS. When you:

- Upgrade NMS server, your configuration (domain and hub names, IP addresses, user accounts /passwords, etc.), is retained.
- Update secondary hubs and robots, their configurations (hub names, configured tunnels, installed probes, 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.

- **Upgrade NMS before you upgrade UMP**

  When installing or upgrading UMP with NMS 6.00 and MySQL, deactivate the QoS Processor probe before running the UMP installer, then reactivate it after UMP is installed.

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

  http://support.nimsoft.com/downloads/doc/Compatibility_SupportMatrix_current.pdf

Upgrading the NMS System

Updating NMS on Windows with the Install Wizard GUI

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 http://support.nimsoft.com site.
4. Download and run the most recent NMS Install Package for Windows.
5. Follow the prompts to complete the installation. Note that:
   - Where possible, the Installer displays the current configuration values for your confirmation.
   - When specifying MySQL or Oracle database parameters, for improved performance we recommend you **Drop the Columns** (default) unless you use:
     - A version of UMP prior to 2.5.0 or the legacy SDP console
     - Custom dashboards that query against the **inserttime** column. Dashboards and reports that use SQL Views will not function properly if **Drop the Columns** is chosen.

6. When the upgrade is complete, make sure you:
   - Turn the anti-virus scanners running 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.

Upgrade NMS on Linux or Solaris with 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 http://support.nimsoft.com 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. Note that:
   - Where possible, the Installer displays the current configuration values for your confirmation.
   - When specifying MySQL or Oracle database parameters, for improved performance we recommend you **Drop the Columns** (default) unless you use:
     - A version of UMP prior to 2.5.0 or the legacy SDP console
     - Custom dashboards that query against the **inserttime** column. Dashboards and reports that use SQL Views will not function properly if **Drop the Columns** is chosen.

6. When the upgrade is complete, make sure you:
   - Turn the anti-virus scanners running 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 with 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 http://support.nimsoft.com site.
4. Download the:
   1. Most recent NMS Install Package for your operating system and architecture
   2. Silent install template (.zip) package
5. On Linux or Solaris, execute **chmod 755** on the install file to make it executable.
6. Prepare your response file:
   1. Extract the silent install templates.
   2. Locate the **installer.upgrade.properties** file and save it as **installer.properties** in the same directory as the installer.
   3. Make the following edits to **installer.properties**:
      - Add your NMS administrator password to the **NMS_PASSWORD=** line.
      - For improved performance, leave **DROP_COLUMNS** set to **1** (default), unless you have a MySQL or Oracle database AND one of the following: (a) you use a version of UMP prior to 2.5.0, (b) you use the legacy SDP console, or (c) you use custom dashboards that query against the **inserttime** column. Dashboards and reports that use SQL Views will not function properly if the columns are dropped.
   4. 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 NimbusWatcher Service**
   - 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 running 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. See:
   - 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. On the upgraded Nimsoft Server, launch the Nimsoft Server web page by double-clicking the shortcut named **Nimsoft Server** located on the desktop. Make a note of the URL given in the browser window—you will use it in the procedures below.
2. Open an Internet Explorer browser on the machine you want to upgrade Infrastructure Manager, using the URL found in step 1.
3. Click on **Client Installation**.
4. On the web page that appears, choose the link **Infrastructure Manager** to install the new version on that machine.
5. Repeat this procedure to upgrade additional machines.

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).
2. On the client computer, browse to your NMS web page (http://<servername_or_IP_address>:8008).
3. Choose **Client Installation**.
4. On the web page that appears, choose the link **Windows Robot, Hub, Distribution Server, Alarm 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

Do one or more of the following:

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 wish to update.

Windows, method 2

1. Identify other systems which 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>:8008).
3. Choose **Client Installation**.
4. Choose the link **Windows Robot** to install the Nimsoft Robot on that machine.
5. 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.

Warning: Do not drop the robot_update on a Hub icon in the Infrastructure Manager tree! Doing so will include the robot on which the Hub is running and cause a restart of the Hub robot. This will make part of the distribution fail. Other robots belonging to this Hub will failover to a secondary Hub (if present), creating problems for the distribution and you will end up with some robot updates not completing.

Verification of successful installation/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 6.0** 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).

Note: These tables list the version numbers of probes provided with NMS 6.0. 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 http://support.nimsoft.com (**Download** and **Archive** pages) as they are made available.

User Interfaces	**Version 6.00**	**Prior release (5.61)**
Infrastructure Manager	4.04	4.03
NIS Manager	2.2.0	2.2.0
LogViewer	1.1.6	1.1.3
Dr. Nimbus	1.5.3	1.5.3
Backend components	**Version 6.00**	**Prior release (5.61)**
automated_deployment_engine	1.00	
distsrv	5.22	5.21
hdb	5.70	5.52
hub	5.80	5.66
spooler	5.63	5.52
install_unix	6.00	4.71
aix_5	(6.00)	(4. 71)
hpux_11	(6.00)	(4. 71)
linux_22	(6.00)	(4. 71)
linux_23	(6.00)	(4. 71)
solaris_10_i386	(6.00)	(4. 71)
solaris_8_sparc	(6.00)	(4. 71)
tru64	(6.00)	(4. 71)
aix_5_64	(6.00)	(4. 71)
hpux_11_64	(6.00)	(4. 71)
hpux_11_ia64	(6.00)	(4. 71)

	solaris_8_sparcv9	(6.00)	(4. 71)
	solaris_10_amd64	(6.00)	(4. 71)
	linux_23_64	(6.00)	(4. 71)
	linux_23_ppc64	6.00)	(4. 71)
nas		4.00	3.72
robot_update		5.70	2.91 & 5.52
controller		5.70	5.51
as400 robot		5.52	5.52
group_server (MSSQL only, not needed for new installations)		2.66	2.66
nis_server		2.00	1.50
httpd		1.47	1.46
nimldr (removed nas functionality)		3.54	3.54
dashboard_server (MSSQL only, not needed for new installations)		1.71	1.71
variable_server (MSSQL only, not needed for new installations)		3.40	3.40
data_engine		7.88	7.86
report_engine (MSSQL only, not needed for new installations)		7.92	7.90
nod_maint		1.02	
audit		1.20	1.20
qos_engine		2.65	2.63
qos_processor		1.00	
relationship_services		1.64	1.56
sla_engine		3.56	3.52
tcp_proxy		1.10	
fault_correlation_engine		1.64	1.56
Discovery components		**Version 6.00**	**Prior release(5.61)**
cisco_monitor		3.22	3.11
interface_traffic		5.11	5.01
net_connect		2.73	2.71
ace (multiplatform version)		2.65	2.60

assetmgmt	1.24	1.24
discovery_agent	3.40	3.30
discovery_server	3.40	3.28
cdm	4.70	
rsp	2.81	2.72
Redist	**Version 6.00**	**Prior release (5.61)**
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 update is successful is to use a SQL tool (e.g. **SLM Manager->Tools->SQL Query**) and execute the following statement:

```
select * from tbnVersion
where ModuleName = 'NIS_SLM'
```

This query should return:

- **4.82** (SQL and MySQL)
- **4.83** (Oracle).

Chapter 5: Known Issues

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

Performance, Stability, Scalability

- qos_processor has an impact on NMS performance and memory usage. See the qos_processor online documentation for details.
- 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

- **nametoip error may appear**

  When upgrading to NMS 6.0, you may see **nametoip** listed as a fatal error in **ace.log** and **nis_server.log**. This can be ignored. The controller notices that ACE encountered this error and automatically restarts ACE, which corrects the error.

- **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.

- **Robot communication over the network fails due to invalid /etc/hosts file**

  Non-Windows systems only

  Ensure the **/etc/hosts** file on any non-Windows 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.

- **Activating discovery and configuration of an existing interface_traffic probe on the server**

  The Nimsoft discovery function automatically turns on encryption of community strings in the probe configuration file on the discovery computer. Before you activate the discovery function, enable encryption on the interface traffic probe. Failing to do so causes existing configurations to stop working due to invalid community strings. Interface_traffic probes on other robots are not affected.

- **Silent install requires a DB_PORT value if you are using 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.

- **Fault Correlation impacted by configuration of hub alarm forwarding and NAS alarm replication**

  For the Fault Correlation application to provide accurate results, 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 as this would cause alarms to be processed twice and yield unpredictable results.

- **MySQL users must deactivate qos_processor probe before UMP installation/upgrade**

  Once UMP is installed, the QoS Processor can be re-activated.

- **Some probes may not start after installation**

  Some probes might not start after NMS installation 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 http://support.microsoft.com/kb/184802.

- **UMP probes need restarting after an upgrade to NMS 6.0**

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

- **Probes are not activated after Nimsoft Server installation**

  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 and is usually fixed by manually activating the probe.

- **Oracle users must add key to dashboard_engine probe**

  During NMS installation, the installer attempts to set up the connection with the Oracle database.

  Note: When prompted to enter a service name, first enter the SID for the table space you plan to use. If the system prompts you that it cannot connect to the database using the SID, enter a service name instead.

  Then, if you used a service name instead of an SID, at the end of the UMP installation you may see an error message listing probes (which rely on the database connection) that have failed to start. If this occurs, add a **Key** and **Value** to the dashboard_engine probe. This repairs the dashboard_engine database connection and allows any probes that rely on it to start.

Follow these steps:

1. Open Infrastructure Manager, and locate the dashboard_engine probe under the **Service** node.
2. Shift+ right-click on the dashboard_engine in the list of probes to the right to open the **Raw Configure** dialog.
3. Open the **Data** folder and add the following **Key** and **Value**.

   Key: jdbc_url_template

   Value: jdbc:oracle:thin:{1}/{2}@{0}:{7}:{your_SID}
4. Apply the new key and value, then restart dashboard_engine.

- **AIX computers not found by discovery using SNMP**

  When using SNMP, certain types of AIX computers might not be found because the format in the computer description field cannot be read. (AIX sends binary data as description over the SNMP API that NMS uses.)

- **SQLite database problems on Solaris 9**

  You may see SQLITE_BUSY or SQLITE_CORRUPT errors in discovery_agent.log. These errors can be ignored as long as they are sporadic and **discovery_agent** appears to work (for example, it continues to discover new systems and updates the "alive time" of monitored systems).

  A more serious issue is when discovery_agent stops working and you see the following error during startup:

  `Failed to initialize the database file, correct the error and start the probe again.`

  To clear the problem:

  1. Deactivate discovery_agent.
  2. Delete the **.db3** and **.dbz** files from the discovery_agent directory:

     <Nimsoft_install_folder>\probes\service\discovery_agent*.db3

     <Nimsoft_install_folder>\probes\service\discovery_agent*.dbz
  3. Activate discovery_agent.

- **Discovery agent does not work on a passive robot**

  Nimsoft is investigating a possible fix for a future release.

- **ADE probe requires updated RSP probe**

  If you plan to use the Automated Deployment Engine (ADE) probe to deploy robots in bulk, update the RSP probe to version 2.90 throughout your Nimsoft infrastructure. This ensures that the full extent of your Windows environment is found during discovery.

Miscellaneous

UMP probes need restarting after an upgrade to NM server 5.61

For data time-stamping to work correctly across a distributed Nimsoft deployment, the Nimsoft 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.

Installation Fails Due to Java JRE Version

The installer pre-check may flag an issue with the JRE version it finds installed on the system. This occurs if Java 6 Version 29 or 30 (1.6.29 or 1.6.30) is installed.

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 customers install the most recent version of JRE 1.6x, currently JRE 1.6.35 (Java 6 version 35). A supported alternative is JRE 1.7x (Java 7).

distsrv on Solaris fails during package deployment

Valid on Solaris: When distsrv has a large number of probe packages to distribute, it can sometimes fail before distributing all of them, displaying an error message "Extraction failed" or equivalent wording. It appears as if there wasn't sufficient space to unpack/extract the compressed packages, although there is sufficient disk space available. One common scenario for this issue is when installing UMP from Solaris.

Solution: Manually restart the distsrv probe (right-click on the probe in Infrastructure Manager, select deactivate, then select reactivate). After it restarts, the distsrv probe will finish its series of distribution tasks, starting from where the failure occurred.

Failed Installation on Solaris reduces available swap space

Valid on Solaris: If the NMS installation is interrupted, or for some reason fails, then installer files (/tmp/install.*) remain in /tmp. SInce Solaris swap includes the /tmp directory, Nimsoft recommends manually deleting these files before running the installer again.

Linux Installation: Access denied for user 'root'

Valid on Linux: When attempting to install the NM Server to run against a MySQL database, after entering the database server information, the following error (or its equivalent) is received:

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

Cause: Either remote privileges have not been established, or the password identified for remote systems is not consistent with what is set on the database server locally.

Solution: Perform these steps (to set up access from any host):

1. Login to the MySQL database locally (i.e. on the actual server hosting MySQL).
2. Issue these commands:

```
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
```

Or to set up access from a particular host, for example "HostX," issue these commands:

```
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;
```

ADE time out with robot deployment using remote distsrv

Valid on all platforms: With two-tier ADE robot deployment, using a secondary hub (with no local ADE), the primary ADE does not wait long enough for the remotely-installed ADE on the secondary hub to come up.

Impact: Failure to deploy robots from ADE on the secondary hub to designated targets.

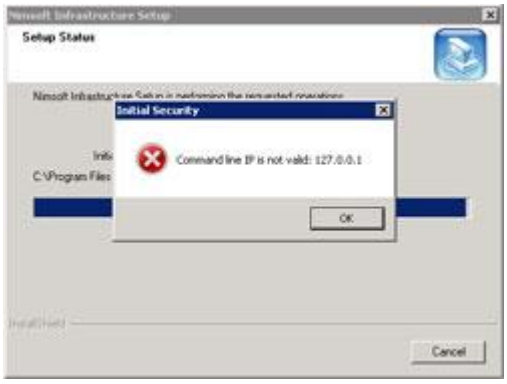
Solution: Disable the secondary (remote) distsrve probe. This is done from the primary distsrv probe by unchecking the “Use remote distsrv on distribution” parameter checkbox in its probe configuration GUI.

Installing NM Server/Hub: "Command Line IP is not valid: 127.0.0.1" popup error

The error screen shown below may be seen installing an NM Server (Hub) using NimBUS Infrastructure.exe and running any of these commands:

- WebPublish (during login)
- Distribution (during login)
- DMZ Setup Wizard (during configuration).

The error screen below is benign may safely be ignored:



Simply click **OK** and continue.

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

An LDAP user cannot log into NM Server unless the Active Directory user is a member of the LDAP domain admin group. The LDAP group policy on NM Server does not matter--it can be users, admins, guests, but unless the active directory user is part of the domain admins group, he or she will not be able to log in.

Uninstalling Nimsoft Server fails, using Add/Remove Programs in the Control Panel

Uninstalling Nimsoft from the Add/Remove Programs control panel applet may sometimes fail. The problem is that the path to Ctor.dll does not have quotes, even though there is a space in the path.
To solve this, you should find the path to Ctor.dll in the registry and add quotes as shown below:

```
"C:\PROGRA~1\COMMON~1\InstallShield\engine\6\Intel 32\Ctor.dll"
```

Then attempt to uninstall Nimsoft again.

Activating discovery and configuration of an existing interface_traffic probe on the server

The Nimsoft discovery function will automatically turn on encryption of community strings in the probe configuration file on the discovery computer. Prior to activating the discovery function, please enable encryption on the interface traffic probe. Failing to enable encryption will cause existing configurations to stop working due to invalid community strings. Interface_traffic probes on other robots are not affected.

Chapter 6: Defects Fixed

This section describes defects (organized by category) that were fixed in NMS 6.00.

Performance, Stability, Scalability

- ACE:
  - Did not connect to SQL DB on nonstandard port
  - Produced an exception when you add default templates to default groups
  - Would not configure routers and switches via remote probe (SOC)
  - ACE probe failed on database conversion after upgrade
- Alarms that existed prior to replication setup were not forwarded
- Binding an IP address to a robot crashed the robot in Windows
- Cursor leaks caused lost database connection with Oracle and configurations with large groups of systems
- data_engine:
  - Delete was single transaction, which caused the transaction log to grow excessively large and blocked inserts
  - Inserts were blocked during maintenance
  - Maintenance scheduling defect fixed
  - SQL Server partitioning and indexing defect fixed
- Distsrv failed to process multiple **request.cfg** requests
- High memory usage for **discovery_agent** on Solaris 10 sparc
- If you modified the partition configuration for a specific RN table, the wrong values were used when the table is re-partitioned in SQL server
- Java exception when the silent NoD Relay installer was configured with a port out-of-range
- Multi-day operating periods were not applied correctly to Weekly and Monthly SLA calculations
- NAS:
  - Had a memory leak when flood protection is turned on
  - Did not automatically start after deployment
  - Replication queue grew too large to transmit
  - Copy function of Triggers worked abnormally

- nis_server:
  - Did not start after NMS install with MySQL running on non-standard port
  - Failed to connect to CI database after upgrade to NMS 6.0
  - Did not connect to SQL DB on nonstandard port
- Origin changes were not persisted in S_QOS_DATA by data_engine
- Probe information from passive robot was not updated in all hubs
- Raw data aging failed if there were unexpected indexes on the RN table
- SLA/SLM was not functional in UMP 2.6.1
- sla_engine:
  - Failed on asynchronous data calculations
  - Started slowly on MySQL
  - MySQL and SQL Server did not operate correctly on non-standard ports
- Some library checks took too long on Linux
- Probe defects:
  - ace did not start after NMS install with MySQL running on nonstandard port
  - qos_engine did not start after NM install with MySQL running on nonstandard port
  - sla_engine did not start after NM install with MySQL running on nonstandard port
  - sla_engine reported 100% compliance despite being in violation for five hours
- Tool to fix Variant units skipped over certain SNMPGET QoS monitors
- With NOD implementations, if archive was fully populated, distsrv continuously restarted itself when you deployed a probe

Security

- Could not give permissions to new user on MySQL 5.1
- **sla_engine** 3.55 could not start with Windows authentication.

Usability

- ace probe could not deploy **net_connect** to primary hub (**nametoip** problem reported in ace log)
- ACE service catalogs were not getting set during silent installation
- New robot AAI 32bit .MSI failed to set first probe port.

Localization

- Spanish and Portuguese: **quit** function did not work in console installation mode.