Service Level Management...within reach

NimBUS Server 3.60 Upgrade Guide

GA

Document updated March 12, 2009

Table of Contents

Revision history

Revision Date	Description
18.11.2008	Initial version - Beta 01.
26.11.2008	Added “Known Issue”: On Vista with SP1 and IE7: Problems with launching dashboards from the NimBUS Server main window.
03.12.08	Added information about the option to have multiple NimBUS robots installed on the same server.
17.12.08	Added “Known Issue”: “Installing on AIX version 6” and “Installing on LINUX with glibc version 2.8 or 2.9”. Updated the component list in the section “Verification of successful installation/upgrade”.
12.03.09	Added “Known Issue”: “Missing servers in Dynamic Dashboards after upgrading to NimBUS Server 3.60”.

NimBUS Server

Introduction

This document describes functionality implemented in NimBUS Server 3.60.
This is a new cumulative release of NimBUS software server modules.
The previous official release was NimBUS Server 3.50, and several of the modules which constituted that release have later been replaced by newer modules, which contain a combination of new features and corrections of bugs.

Please take notice of the steps described later in this document in order to safely install this software on your system(s).

Overview

The NimBUS Server 3.60 contains a number of new features and component modifications.
These are the main changes compared to NimBUS Server 3.50.

- **Support for multiple NimBUS robots installed on the same server**
  It is possible to install additional NimBUS robots on a server where already one NimBUS robot is installed and running.
  Note
  - *Not all* NimBUS probes are verified to work properly when multiple instances of the same probe are running on the same server.
  - It is not possible to install more than one NimBUS hub on each server.

- **Service Level Manager version 4.3X**
  - Added support for NimBUS Hub with LDAP authentication.

- **NimBUS Manager**
  - *Maintenance mode*
    Selected Robot(s) can be set in Maintenance mode.
  - Introduced LDAP user support/management.
  - Introducing all new support for alarm notes management.

  See Appendix 1 for further information.

- **NimBUS Enterprise Console**
  - Introducing all new support for alarm notes management.
  - Introducing LDAP user support/management.
  - Extended Table object for dashboards.

- New memory storage model for dashboard panel initialization.
- Central/Login Subscription mechanism implemented in order to scale large number of hub subscribers.
- Web Publish: Central hub can be specified to achieve quicker startup.

See *Appendix 1* for further information.

- **NimBUS LDAP solution**
  The NimBUS LDAP solution makes it possible to log on the NimBUS consoles as a LDAP user. This means that it is no longer necessary to be defined as a NimBUS user to log on and use these consoles. See Appendix 2 for further information.
  Note: Avoid creating NimBUS Users and LDAP users with identical user names.

- **Native 64-bit support** for core components and system probes on the Unix, Linux and Windows platforms. See Appendix 3 for further information.

The NimBUS Server 3.60 also contains several corrections and updates on different components. A list of detailed list of fixed bugs and changes from NimBUS Server 3.50 to 3.60 is found in Appendix 4.

The known issues for NimBUS Server 3.60 are presented in Appendix 5.

Prerequisites

Nimbus Server can be installed on computers running operating systems:

- Microsoft Windows 2000 (Min. Service Pack 2, Service Pack 4 recommended).
- Microsoft Windows XP.
- Microsoft Windows 2003.
- Microsoft Windows Vista (SR1).
- Microsoft Windows 2008.
  Please note that certain tasks require Administrator privileges on Microsoft Windows Vista and Microsoft Windows 2008 computers. See the section *Known issues in NimBUS Server 3.60* for further descriptions.

Installation requirements

Use a login with sysadm privileges when installing or upgrading
Please use a login with sysadmin privileges when installing or upgrading to NimBUS Server 3.60:

- If using an existing database, make sure that the login used for installation/upgrade maps to the database's dbo.
- If database is created by the NimBUS Server installation, the database's dbo will automatically be mapped to the login used in the installation.

Installing on one or two machines?
When installing a small system, you may install the components involved on one machine, otherwise we recommend installing on two servers.
As a rule, if your NimBUS installation shall handle more than 1000 QoS messages per **minute**, we recommend to install on two servers; one for the NimBUS components and one for the database.

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

System requirements

Big system
SQL Server:
- 2 CPUs
- 3+ GHz
- 2-4 GB RAM
- Raid 10 disk system 100+ GB *

NimBUS Server:
- 1 CPU
- 3+ GHz
- 1 GB RAM
- 100 GB Disk *

Small system
NimBUS Server and SQL Server:
- 1 CPU
- 3+ GHz
- 1 GB RAM
- 100 GB Disk *

* Recommended disk configuration:
- Operating system on a separate disk.
- Transaction log on a separate disk.
- Data on a separate disk (or Raid 10).

Installation note

The installation contains three main components:

- NimBUS Availability Server
- NimBUS SLM Server
- NimBUS Discovery ACE Components

During the Setup Wizard, you have the option to install one or more of them.

You must ensure you can access Microsoft SQL Server 7.0/2000/2005 (if you are planning to install a production system) or Microsoft MSDE 2000A, Microsoft MSDE 8 2000 or Microsoft SQL Express (if you are planning to install an evaluation/demo system).

Note: If you want to install the Service Level Manager component on windows, you also need MDAC 2.8 or newer installed.

The database must be **case insensitive** when handling queries.

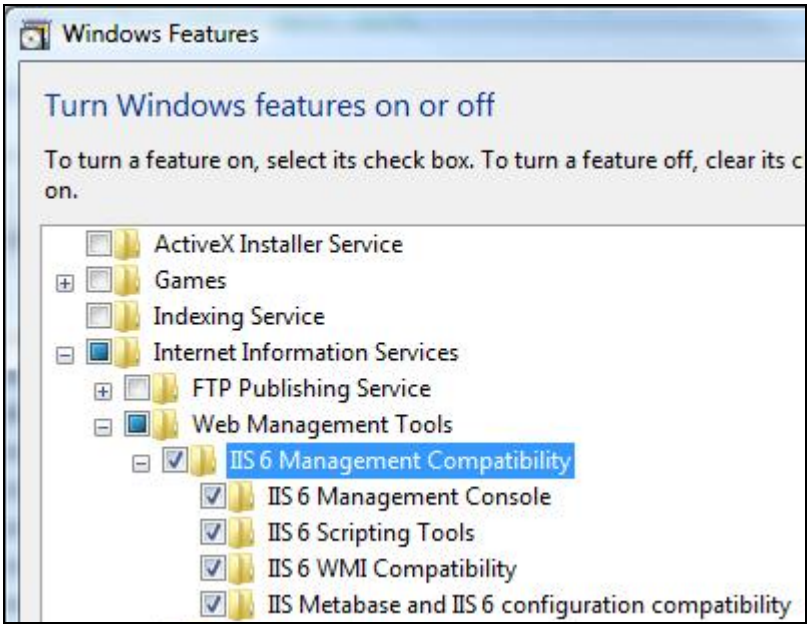
Installation of NimBUS Infrastructure is part of the NimBUS Server installation for Windows systems. If you want to install NimBUS Infrastructure on a UNIX system, the following UNIX systems are supported:

- AIX
- HP-UX
- Linux
- IRIX
- SPARC Solaris
- TRU64

Webservice 3 installation issues

Installing the NimBUS Web Service on Windows Vista.
Before installing the Web Service on Vista, IIS 6.0 Management Compatibility must be enabled:

- Open the Control Panel.
- Select *Uninstall a program* under the Programs category (in default view) or Programs and features (in classic view).
- Under Tasks, select Turn Windows features on or off.
- Expand the Internet Information Services node in the window that is opened.
- Expand the Web Management Tools node.
- Enable IIS 6 Management Compatibility and the underlying sub-modules.



See the *Nimbus Installation Guide* for further details.

Note:
Increased memory usage when using Dynamic Reports
Provided that the Dynamic Reports option is activated in the Report Engine probe, this probe will generate Dynamic Reports based on QoS data found in the Dynamic groups defined in the new Group Server Probe. These reports will

be made available in the NimBUS Service Level Manager and in the NimBUS Server application.
Be aware that this will result in increased memory usage.

Preparation

NOTE: Before preparing for the installation/upgrade, make sure you've read and understood the contents of Appendix 5 – Known issues!

If you intend to utilize an existing database for a new installation or an upgrade of NimBUS version 3.35 / 3.35 SR1 or earlier, please make sure that you make a backup of your database. The NimBUS Server 3.60 contains **a non-reversible upgrade script** that changes the database structure of some tables.

The database upgrade may take a long time to finish if the database contains many QoS objects. It is difficult to estimate the duration of an upgrade, since the duration depends on a number of different factors. A database upgrade with 5000+ tables with a size of 25 GB may consume 5-6 hours. A database upgrade with the same amount of data, but with less than 1000 tables may consume only 30-45 minutes.

Another example from a site with a database of size 120GB with approximately 20000 QoS objects showed that the database upgrade were running approximately 8 hours.

If you have a database similar to the first example, you may consider upgrading during a weekend and stop the probes *sla_engine* and *report_engine* during the upgrade.

Installation/upgrade

The installation of NimBUS Server 3.60 consists of a chain of installations of the associated modules. Some of these modules may request that the system should be restarted. DO NOT restart your system until all modules have been installed.

All existing modules will be replaced when installing NimBUS Server 3.60 as an upgrade.

You may choose more freely which modules you want to install when installing NimBUS Server for the first time on a system.

Note: If you want to install the Service Level Manager component on windows, you also need MDAC 2.8 or newer installed. If not, the installation wizard will be stopped, and you must upgrade to MDAC 2.8 or newer before starting the installation wizard again.

This is the recommended sequence of steps involved in upgrading a NimBUS domain consisting of several hubs and robots:

- Identify the NimBUS systems containing *NimBUS Server* and upgrade these systems by starting NimBUS Server.exe. In most cases, the NimBUS server is running on the same computer as the NimBUS Hub.
- On one of the upgraded NimBUS Servers, find the URL to the NimBUS Server web page by double-clicking the icon named "NimBUS Server" on the desktop.
- Identify other systems which contain *NimBUS Infrastructure* (Control Panel->Add/Remove programs) and upgrade these systems by starting Internet Explorer browser with the URL in previous step and choose 'Client Installation'. On the appearing web page, choose the link 'Windows Robot, Hub, Distribution Server, Alarm Server' to install the NimBUS Infrastructure.
- Updating the NimBUS Robot:
  Note: Do not drop the Robot update on a Hub node!

  On Windows systems
  Simply drop the Robot_Update from an upgraded hub.

  OR: Identify other systems which contain *NimBUS Robot* (Control Panel->Add/Remove programs) and upgrade these systems by starting Internet Explorer browser with the URL in previous step and choose 'Client Installation'. On the appearing web page, choose the link 'Windows Robot' to install the NimBUS Robot.

On UNIX systems:
Drop the Robot_Update from an upgraded hub.

Check the appropriate check-box for NimBUS Dashboard Viewer if desired during upgrade.

See the *Nimbus Installation Guide* for further details.

Upgrading your NAS 2.xx

If upgrading from NimBUS version 3.35 / 3.35 SR1 or earlier, NAS 3.0x will automatically, during the initial startup, convert your current open alarms located in the *nas.db* file. Old transaction-logs will not be automatically converted. You may convert the transaction-logs manually by following the sequence described in the section below. Please note that "old" transaction records contain less information than transactions created by NAS 3.2x. Existing import/export configurations will be converted into a replication profile.

Converting transaction-logs created by NAS 2.xx

The files in the nas/logs directory and the nas/transaction.log will be converted. You may manually remove old files that contain transactions outside your needed scope. Keep in mind that the current transaction logfile is nas/transaction.log. All converted files will receive a .cvt extension.

1. De-activate the NAS using the NimBUS Manager.
2. Start a command window (shell) on the server hosting the NAS.
3. Change directory to NimBUS/probes/service/nas
4. Start the NAS in convert mode: **nas –d 1 –l stdout –u administrator –p mypassword –c**
5. Converting will now start, approximately 1 MB per 15 sec.
6. Check the output for progress information.
7. Activate the NAS using the NimBUS Manager, check the log-viewer for information.

Converting NAS 2.xx import/export into NAS 3.2x replication.

The existing import/export configuration is converted during the initial startup sequence. The following rules apply to the conversion:

1. Import and export will create a bi-directional alarm replication.
2. Import without export will create a uni-directional replication from the exporting NAS.
3. Export without import will (as in 2) create a uni-directional replication from the exporting NAS.

Please note that pre NAS 3.2x versions allowed a scenario where no import (or a restrictive export) configurations were present. This could result in unsynchronized alarm servers. Hence, this functionality is not allowed in the replication services provided by NAS 3.1x.

Verification of successful installation/upgrade

The installation procedure does not leave an "all is installed correctly" mark, so one has to follow the output from the installation process closely in order to detect failure(s).
One indication that the installation was successful is that one can read the text "**NimBUS Server 3.60"** in the main browser window after double-clicking on the "NimBUS Server" icon on the desktop.
Another indication is that all your probes/components in the main windows of the NimBUS Manager have the following versions:

Check the installed user interfaces (Help->About) for the following versions:

User Interfaces	
Enterprise Console	3.31.5
NimBUS Manager	3.71.5
Service Level Manager	4.31
Alarm Subconsole	2.50
Dashboard Viewer	1.24
Web Service	3.11
Webpublish	2.81
LogViewer	1.1.3
Dr. NimBUS	1.5.0.0
Web Service for Mobile Solution	2.12
Mobile Panel Client	2.10

Backend components	
distsrv	4.72
hdb	3.12
hub	4.73
spooler	3.12
install_unix	4.12
aix_5	(4.12)
hpux_11	(4.12)
linux_23	(4.12)
solaris_10_i386	(4.12)
solaris_8_sparc	(4.12)
tru64	(4.12)
aix_5_64	(4.12)
hpux_11_64	(4.12)
hpux_11_ia64	(4.12)
solaris_8_sparcv9	(4.12)
solaris_10_amd64	(4.12)
linux_23_64	(4.12)
linux_23_ppc64	(4.12)
nas	3.22
robot	2.91 & 3.12
controller	3.12
as400 robot	2.66
group_server	2.53
httpd	1.34
nimldr	3.12
dashboard_server	1.62
mobile_panels	-

variable_server	3.31
data_engine	7.11
report_engine	7.57
sla_engine	2.00

Discovery components	
NIS Manager	1.0.2
cisco_monitor	2.05
interface_traffic	4.36
net_connect	2.01
ace	1.13
discovery_agent	1.15
discovery_server	1.12
rsp	1.19

Checking the database upgrade (if upgrading from 3.35 or earlier)

Some large databases may require an extended upgrade time (see *Preparation*). 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 S_SLM_VERSION

If this query returns ”4”, the installation has completed successfully.

Another check to verify if an upgrade is successful is to verify the contents of the log-file for the *data_engine*. It should contain the following sentence when the update is finished:

slm_40_update_thread - start tz_offset update on tables
slm_40_update_thread - used <xxx> seconds on <xxxxx> tables

Be aware that the log-file is circular and that the message may have been overwritten by later log entries.
(Tip: Set Log-level to 0 if loosing some log info does not represent a problem).

If the query returns ”3.99”, then problems have arisen during upgrade.

Check the log from DataEngine. If the only error messages it holds are as shown below, it indicates that some data has been rejected.

Month D HH:MM:SS:MS [1552] de: [update] ExecuteNoRecords - X errors
Month D HH:MM:SS:MS [1552] de: (1) ExecuteNoRecords [Microsoft OLE DB Provider for SQL Server] Cannot insert the value NULL into column 'COLUMN_NAME', table 'DATABASE_NAME.dbo.RN_QOS_DATA_XXXX'; column does not allow nulls. INSERT fails.
Month D HH:MM:SS:MS [1552] de: (2) ExecuteNoRecords [Microsoft OLE DB Provider for SQL Server] The statement has been terminated.

If you accept that the data is rejected, you need to perform the steps listed under ‘Manually moving from 3.99 to 4.00’ (see below).
Otherwise please contact NimSoft for further guidance.
Also if the query returns any other value, please contact NimSoft

Manually moving from version 3.99 to 4.00

If the upgrade encountered problems, you’ll find that it now has version 3.99 instead of the required version of 4.00. You need to perform the following steps in order to set the version to 4.00.

select * from S_QOS_DATA where (r_table is null or r_table like ‘R_QOS_DATA%’) and qos_def_id > 0

For each row returned (this represents tables not converted), please perform the following update:
update S_QOS_DATA set r_table = ‘RN_QOS_DATA_<XXXX>’, h_table = ‘HN_QOS_DATA_<XXXX>’ where qos_def_id = <YYYY>
(<XXXX> is the qos_def_id (from step 1.) left-padded with zeros to make 4 digits, while <YYYY> is the qos_def_id as a number).

Restart the data_engine (deactivate + activate) and see that the situation is corrected.
To verify that all is well, please wait some minutes before running the following query:
SELECT * FROM s_slm_version
If it returns 4, all is ok.

Failure

Nimsoft stands ready to help its customers manage complex networked systems with an advanced performance and service-level management solution built on a flexible architecture.
We will therefore be happy to receive your input – problems or any other kind of expression – through any of the following channels:

Phone (Scandinavia):	+47 99609387
Phone (Europe):	+44(0)1932 577766
Phone (USA):	+1 650 570 5401 (press 3)
Fax:	+47 22627161
Email:	support_nor@nimsoft.com

Appendix 1

Feature changes to NimBUS Manager and NimBUS Enterprise Console

NimBUS Manager

- *Maintenance mode*
  Selected Robot(s) can be set in Maintenance mode and this will be reflected by the icon coloring in the Robot and Probe lists.
- Introducing all new support for alarm notes management.
- *Introduced user LDAP support/management.*
  LogLevel under Options in Registry can be used to set log level detail.
- Archive Import dialog can now handle a large number of files.
- Unnecessary push of hub actions removed causing faster startup.
- Extended ACL alarm filter for login user. Also implemented for EC and Dashboard Server.
- Move Robot now support DNS lookup feature.

NimBUS Enterprise Console

- *Extended Table object for dashboards*
  A mapping feature has been introduced making it possible to map numeric column values to some text value with a specific text color and background color. This will make the actual table output far more customizable in terms of what is being shown and attention can be given certain values by assigning colors.
- *Alarm Details permission for dashboard Alarm objects*
  A property can be set by the dashboard designer to prevent users with no general access permission to view alarm details, to see the details for a particular Alarm object. The general permission can be granted using the ACL permission settings. If a user has this set, he will be able to see the alarm details for any alarm object and thus override this property.
- *Dashboard database reconnection logic*
  This has been modified for dashboard objects. The objects retrieving data from some database at some poll interval, will share connection status between them to minimize the possibility for the dashboard not running properly after the database has been unavailable for some period of time.
- Introducing all new support for alarm notes management.
- Introduced user LDAP support/management.
- LogLevel under Options in Registry can be used to set log level detail.
- New memory storage model for dashboard panel initialization.
- Central/Login Subscription mechanism implemented in order to scale large number of hub subscribers.

- Extended ACL alarm filter for login user. Also implemented for SubConsole and Dashboard Server.
- Dashboard request object queries have better trace and increased default timeout.
- Dashboard multi-threading may be turned off in Registry for Console viewing.
- Web Publish: Central hub can be specified to achieve quicker startup.

APPENDIX 2

NimBUS LDAP Authentication solution

NimBUS Server 3.60 introduces the NimBUS LDAP solution, making it possible to log on the NimBUS consoles as a LDAP user. This means that it is no longer necessary to be defined as a NimBUS user to log on and use these consoles.

Supported platforms:

- Windows
- Linux

We have implemented an authentication forwarding mechanism between NimBUS and the supported LDAP implementations. Currently two server types are supported; Microsoft's Active Directory and Novell's eDirectory.

We strongly recommend using separate LDAP-groups for NimBUS users.

Thus the LDAP group structure can be used, and it is no longer necessary to define the users as NimBUS users. Using ACLs (Access Control Lists), users belonging to different groups in LDAP can be assigned different permissions in NimBUS.

The HUB can be configured to point to a specific LDAP server, and the Hub will supply a list of LDAP groups found in the container specified.

ACL Management, accessible from the menu bar in NimBUS Manager, lets you associate ACLs with specific LDAP groups. The HUB can be configured to supply a list of groups found in the container specified in the HUB. The users in the LDAP group will then be assigned the privileges for the ACL the group is associated with.

When a LDAP users logs on a console (for example NimBUS Manager), the request will be directed to the LDAP server for authentication. The user can be found in one or more LDAP groups. If the name is found in one or more groups attached to an ACL, the user will be assigned privileges in NimBUS as defined in the ACL.

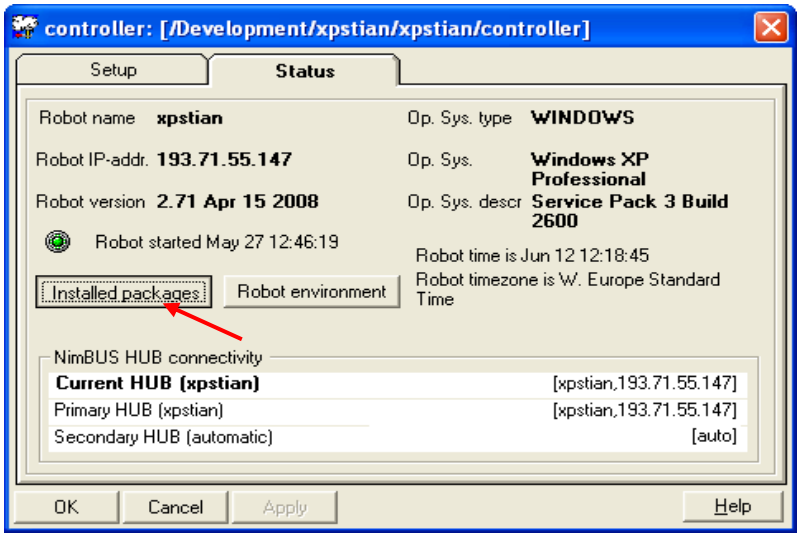
If the user belongs to multiple groups connected to ACLs, the user will be assigned the privileges from the ACL with the most extended privileges.

APPENDIX 3

Native 64-bit support for core components and system probes

NimBUS Server 3.60 includes native 64-bit support for core components (robot, nas, hub and distsrv) and system probes on the Unix, Linux and Windows platforms.

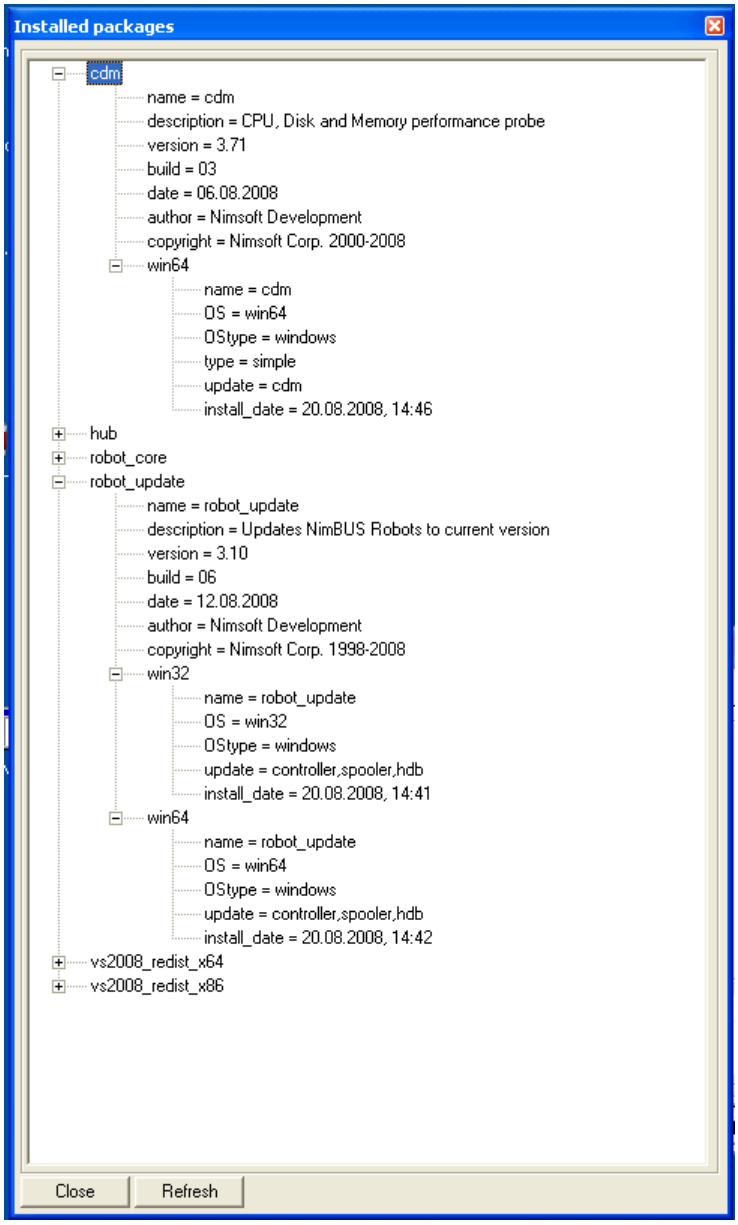
To verify that the upgrade was successful on your 64-bits systems, please open the controller GUI in the NimBUS Manager.



Click the *Installed Packages* button.
Select each of the system probes installed in the list popping up and check that they have a win64 section and a new install_date.

The NimBUS system probes with 64-bits support:

- cdm 3.72
- dirscan 2.52
- logmon 2.54
- ntevl 2.21
- ntperf 1.41
- ntservices 2.41
- perfmon 1.32
- printers 2.21
- processes 2.71
- reboot 1.11


Installed packages
cdm
name = cdm
description = CPU, Disk and Memory performance probe
version = 3.71
build = 03
date = 06.08.2008
author = Nimsoft Development
copyright = Nimsoft Corp. 2000-2008
win64
name = cdm
OS = win64
OStype = windows
type = simple
update = cdm
install_date = 20.08.2008, 14:46
hub
robot_core
robot_update
name = robot_update
description = Updates NimBUS Robots to current version
version = 3.10
build = 06
date = 12.08.2008
author = Nimsoft Development
copyright = Nimsoft Corp. 1998-2008
win32
name = robot_update
OS = win32
OStype = windows
update = controller,spooler,hdb
install_date = 20.08.2008, 14:41
win64
name = robot_update
OS = win64
OStype = windows
update = controller,spooler,hdb
install_date = 20.08.2008, 14:42
vs2008_redist_x64
vs2008_redist_x86
Close
Refresh

APPENDIX 4

Component changes and fixed problems from 3.50 to 3.60

This section contains a list of fixed problems and product changes from NimBUS Server 3.50 SR1 to 3.60
Note that Appendix 1-3 describes the new main features of NimBUS Server 3.60

NimBUS Enterprise Console

Fixed problems:

- Regression error due to 3.26.3 release caused invalid poll values for dashboard objects.
- Dynamic Views tables will now filter on origin.
- Locate Probe and Configure Probe will now use hub value in alarm.
- The Notes edit dialog window caption has been changed to Edit Note.
- The New Note dialog window will now always contain a Category field.
- No longer possible to create a note with no name assigned.
- When adding Notes comments, the Enter key will no longer trigger the OK button.
- The Notes Comment dialog window now contains vertical scrollbars.
- Notes URL not parsed correctly when followed by a new line.
- Hold mode will no longer be turned ON automatically when total number of alarms in nas is more than 500.
- Could not read values of type double from Oracle databases.

NimBUS Manager

Fixed problems:

- Locate Probe and Configure Probe will now use hub value in alarm.
- The Notes edit dialog window caption has been changed to Edit Note.
- The New Note dialog window will now always contain a Category field.
- No longer possible to create a note with no name assigned.
- When adding Notes comments, the Enter key will no longer trigger the OK button.
- The Notes Comment dialog window now contains vertical scrollbars.
- Notes URL not parsed correctly when followed by a new line.
- Hold mode will no longer be turned ON automatically when total number of alarms in nas is more than 500.
- A message box will be displayed if Maintenance mode features are attempted on a robot where that is not supported.

NimBUS Service Level Manager

- Added support for NimBUS Hub with LDAP authentication.
- Improved SQL queries used when launching SLA's.
- Improved error handling in Query window.
- Removed QoS object element from list when delete QoS is selected from database status window.
- Added support for Delete key (Delete QoS object)

- Fixed problem with showing the correct unit in the QoS graph browser when launched from SLA/SLO.
- Fixed issue when recalculating SLA on user's request.

Webpublish

Central hub can be specified to achieve, resulting in quicker startup

httpd

- Added support for 64bit UNIX install packages on the client install page.

data_engine

- Added option of automatic re-indexing of QoS data tables that will run at the same time as the other maintenance routines. This operation could take some time but will improve performance for all the applications that consumes QoS data, including the *delete expired data* routines.

report_engine

- Fixed:
    - Some settings were not changed when saving Email setup.
    - Error when copying reports with more than 2 graphs fixed.

ace

Now takes advantage of new itf checksum algorithm from ift 4.36 probe.
Each "plugin" can now decide whether they want the plugin engine to get the probe version.
Each plugin will now share probe configs for 1 run. This means we only call probe_get_config for each probe once every interval. Previously this was done per plugin run. They share an ace_dist_cfg object, which accumulates hubs and probe configs (including probe versions).
Currently only interface traffic requires special handling (ver 4.36 introduced a new checksum).

hub

- Added support for 64-bit platforms.
- Added support for LDAP bridging.
- The internal worker queues and subscriber queues are given some time to finish on shutdown.
- Added Robot states for maintenance and offline mode.

distsrv

- Support for *no_shutdown* and *temp_directory* when creating a probe from an existing probe.
- Included Archive Configure option that will work with logmon 2.20.
- Changed default configuration tool window placement.
- Configurable alarm messages for distribution completion.
- Added option to forward licenses.
- Improved performance of archive scan after add/remove operations.
- 64bit support (64-bit UNIX support).

- Fixed problem with configuration file not being saved when using archive configuration on a package with a version number.
- Fixed problem with deleting package without version, where the package with the highest version would be deleted.
- Fixed problem with setting probe security.
- Fixed license forwarding.

robot/spooler/hdb

- Resolved CRLF problem with configuration packages distributed from Linux/UNIX.
- Added "controller/" to suppression key of internal alarm messages to avoid conflict with hub alarms.
- Added support for maintenance mode.
- Added support for specifying primary and secondary hubs by dns name.
- Modified configuration file merge on probe distribution so that modified sections are moved to the end of the containing section.
- Added the proxy probe to the list of probes to be started first.
- On restart - added _restart call to local hub to make it use updated user tag information.
- Set robot install dependency for Windows to version 2.90, which is a special upgrade robot to ensure successful upgrade on Windows.
- Added 64bit Unix ports.

- Fixed package so that hdb configuration file setup is not lost on robot_update deployment on UNIX/Linux.
- Fixed package installation problem on LINUX systems (note does not apply to systems with gLibc 2.3 or higher).

dashboard_server

- Reduced log level output for regular operations to improve clarity.
- Simplified ACL alarm filter now supports filtering on message and severity fields for an alarm.
- Introduced LDAP user support.
- Reintroduced restart logic and added thread synchronization on stop.

variable_server

- Removed nimbus.dll dependency.
- Added memory locking to avoid problems on probe restart.
- Added support for 64-bit Windows (x64).

cisco_monitor

- Added SNMP Timeout and Retries options.

interface_traffic

- Changed interface checksums to MD5.
- Added utility "Generate Checksums" (update checksums on multiple profiles).
- Added alarm when ifSpeed is unknown and probe is configured to alarm on Traffic in % of ifSpeed.
- Added critical sections around SNMPQueryCreate if SNMPv3
- Added terminating -1 to SNMPQueryCreate.
- Added platforms (missing in v4.30) LINUX and SOLARIS 8,9,10 (sparc).
- Added support for privacy (SNMPv3).
- Added SNMPv3 support in "bulk-configure". Added SNMPv3 support in "add-range".

- Fixed "No Traffic" alarm when ifSpeed is unknown.
- Fixed remapping of interfaces where ifName is used instead of ifDescr.
- Fixed 'Rediscover Interfaces' and 'Query Agent' for SNMPv3 AuthPriv agents.
- Fixed fetching of operstate on inactive (in probe config) interfaces for SNMPv3 AuthPriv agents.
- Fixed 'Monitor' window for SNMPv3 AuthPriv agents. Added logging of thread id's.
- Fixed saving of default interface definitions.

net_connect

- Port challenge response feature added.
- Ability to paste into the IP Address field added.
- Contact info field added to host properties, to be used in alarm messages.
- ICMP packet loss feature added.
- Added ability to add Services in the Bulk configurator.
- Added ability to enter ip addresses with leading zeros.
- Added search button to find IP or Name. The Port scan windows can be resized.

- Fixed: Default value of ip address 0.0.0.0 removed.

nas

- Ability to serve large data-chunks in queries against the transaction-log.
- Support for custom pre-processing script.
- Decreased the frequency of alarm_stats events during event storms.
- Added support to allow users to save the grid column headers.
- Native 64bit support.
- Improved replication over low-bandwidth communication lines.
- Added support for visibility in match criteria for AO profiles and filters.
- Improved the data filtering in alarm history.
- Added a pattern/regexp validation for match criteria fields.
- Added two columns to AO profile list (Action arguments and visibility).
- Added EMAIL subject as target for AO variable expansion.
- Added confirmation box for nameservice delete, and ability to use the Delete key.
- Added support for transaction summary housekeeping.
- Added transaction database compression to housekeeping procedure.

- Fixed problems with AO profiles using the on_interval or on_ao_interval primitives causing the profile to kick in during restart.
- Fixed problem with note.find() in the scripting engine.
- Fixed a problem with AO profile using on_trigger and operating period / schedule.
- Fixed issues with AO schedules being scheduled wrongfully upon restart.
- Fixed problems with AO schedules that activated or deactivated AO profiles and/or filters.
- Fixed variable expansion for suppression id in AO new_alarm method.

- Fixed problem in UI with increasing severity level on new_alarm.
- Fixed problem with operator period crossing Sunday night.
- Fixed compatibility problem with old AO time-specifications.
- Fixed problem with user1/user2 tags in filters for AO profiles and triggers.
- Fixed Alarm Notifier subconsole/filter compatibility issue.
- Fixed nimbus.alarm() so suppression_key is optional.
- Fixed name-resolution issues due to lookup aging.

rsp

- Fixed problem: Os names with more than 64 characters may cause the group_server to stop when receiving data from the rsp. Now Os names with up to 64 characters can be handeled.

discovery_agent

- Fixed a problem with WMI discovery, where discovery sometimes failed when the response time from the device was very low.

group_server

- Fixed problem: Os names with more than 64 characters may cause the group_server to stop. Now Os names with up to 64 characters can be handeled.

APPENDIX 5

Known issues in NimBUS Server 3.60

Missing servers in Dynamic Dashboards after upgrading to NimBUS Server 3.60

- When upgrading to NimBUS Server 3.60, you may experience that servers are missing in your dynamic dashboard after the upgrade. The problem can be solved by upgrading your **report_engine** to version **7.60**.

Upgrading NimBUS systems with a slave configuration

- If your NimBUS system consists of a slave configuration (including sla_engine and/or report_engine), and upgrading from NimBUS Server 3.35 SR1 or earlier, make sure you deactivate the slave probe(s) prior to upgrading the system. This is necessary because NimBUS Server 3.50/3.60 implements a new database scheme, which isn't compatible to the old SLM probes.
  After the upgrade has been completed, you can upgrade the slave probes and activate them. Your system should then be fully operational again with its slave probe(s).

Microsoft Vista and Windows 2008 issues

- Problems when launching dashboards from the NimBUS Server main window. The problem can be solved by adding the site as a *trusted site* (Internet Options > Trusted sites).
- When designing dashboards with the NimBUS Enterprise Console, logged on as a user without Administrator privileges, it is not possible to exit design mode.
- Administrator privileges are required both to install NimBUS Server components and to run Nimbus Manager.
- Administrator privileges are required for write access to the NimBUS Program Files folder.
- Administrator privileges are required to be allowed to add *New Page* in Nimbus Web Publish.
- If using the raw configure tool in NimBUS Manager to rename a Robot by editing the *robotname* key for the controller probe, logged on as a user without Administrator privileges, the new name will not be reflected by the Nimbus Manager UI.

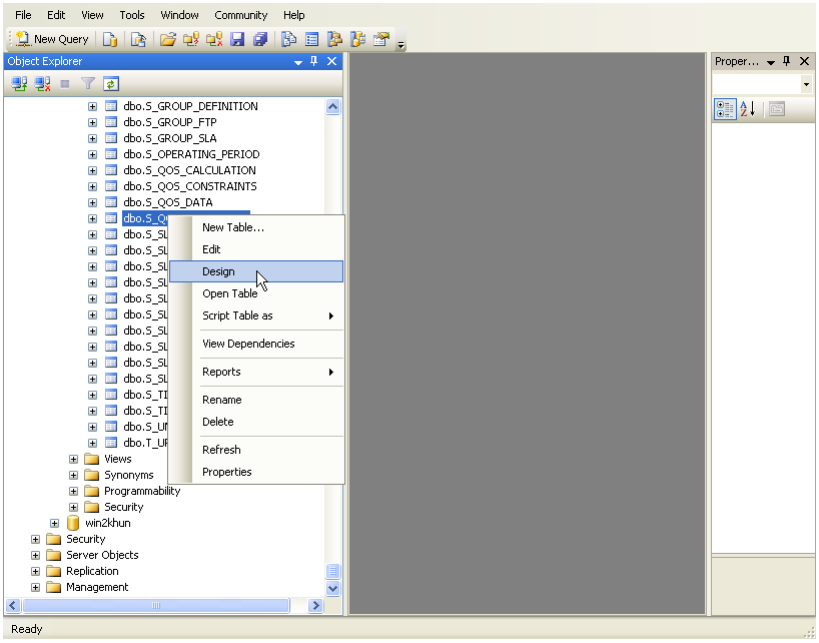
SLM

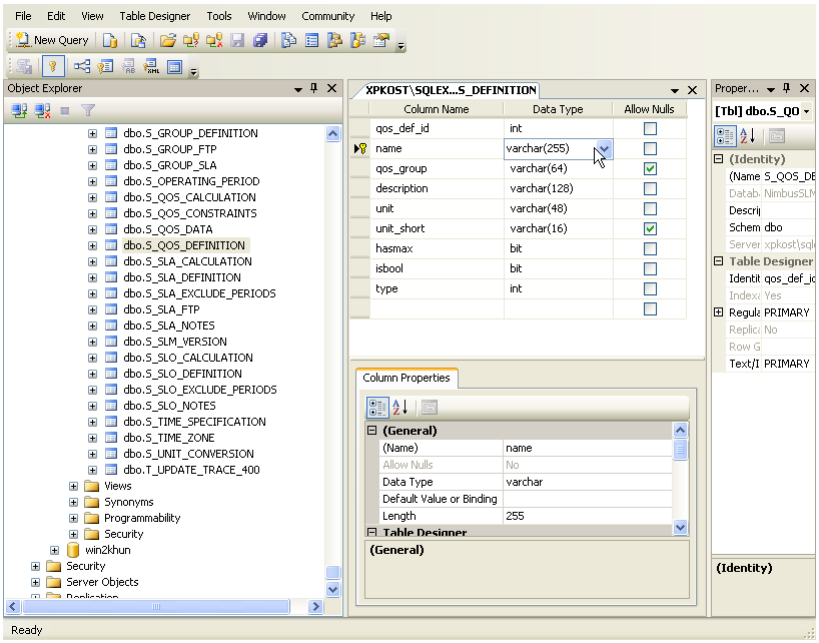
- Using the wizard in the SLM to create SLAs, and only selecting *Services* does not work properly.
- The *Right-click* > *Recalculate* option should just work on the **SLAs** in the *SLA* > *Accounts* > *Account* and *SLA* > *Accounts* > *Account* > *Group* nodes , not on the higher levels in the structure.

- Using the "Create SLA on Service" wizard/tool to build SLA reports for servers, we have seen that the wizard includes every monitored service – even if selecting only one service from the list.

Incorrect size of the ”name” field in the S_QOS_DEFINITION table in the SLM database

- When upgrading to NimBUS Server 3.60 from a version which has been upgraded to 3.35 (or earlier), the “name” column (which is the first column) in the S_QOS_DEFINITION table in the SLM database has a size of 64 characters. The size should be 255 characters.
  If this size isn’t changed, QoS definitions from probes which have a length greater then 64 characters will be discarded by the data_engine. This issue will be resolved by changing the size of the column to 255 characters.
  This change can either be done manually with a database tool:





Or by running the following query on the database (note this query will not work on SQL Server 2000)

Query code to change field width of the name column of the S_QOS_DEFINITION table

```
-- A constraint needs to be dropped first to be allowed to do so
 declare @const varchar(500),@sql varchar(500)

-- Remove temp table, if exists.
 IF Exists(SELECT * FROM tempdb.dbo.sysobjects WHERE [ID] = OBJECT_ID('tempdb.dbo.##Objects')) DROP TABLE
##Object

-- Create new temp table.
 create table ##Objects (iname varchar(255),is_pk int)

-- Insert indexes that are primary key on the table.
 insert into ##Objects SELECT [name],is_primary_key FROM sys.indexes WHERE object_id =
OBJECT_ID(N'[dbo].[S_QOS_DEFINITION]')

-- Add values to variables.
select @const = iname from ##Objects where is_pk = 1 set @SQL = 'ALTER TABLE [dbo].[S_QOS_DEFINITION] DROP
CONSTRAINT [' + @const + ']'

-- Drop the PK constraint.
 EXEC (@SQL)

-- Clean up temp table.
 drop table ##Objects

-- Alter table, modify name, and add new PK.
 ALTER TABLE [S_QOS_DEFINITION] ALTER COLUMN [name] [varchar](255) not null
 ALTER TABLE [dbo].[S_QOS_DEFINITION] ADD PRIMARY KEY CLUSTERED (
  [name] ASC
 ) ON [PRIMARY]
```

NimBUS Watcher

- The NimBUS Watcher service will by default log on and run as 'Local System'. If changing to another account, this will be reset to 'Local System' again when upgrading to NimBUS 3.60.

Installation Issues

- The license is not validated during the installation process, so even if the license key is not valid, no warning will be given. If entering a invalid license key during the installation wizard, you will be notified when starting the NimBUS Manager, where the Hub will be marked with <No License>.
- Installing on AIX version 6:
  You must use updated version of Install_aix_5* (minimum version 4.13) from the Internet archive. If you have already installed version 4.12, you must uninstall this in order to be able to install version 4.13.
- Installing on LINUX with glibc version 2.8 or 2.9:
  You must use updated version of nimldr (minimum version 3.14) and Install_Linux* (minimum version 4.13) from the Internet archive.

NAS Ver. 3.x Issues

- Not match on message text containing **"\"** in AO profiles
  Note that '\' means escape in the pattern-matching/regexp world. If for example using the text string *Average (4 samples) disk free on C:\ is now 93%, which is below the error threshold (95%*) as matching criteria, you should substitute the '\' with for example a '*' in the text string.

List views for the subconsole not available after upgrading from nas ver 2.x to 3.x

- The list views for the subconsole will not be available after upgrading from nas version 2.x to version 3.x. The list views have not been deleted, they are just not compatible with nas version 3.x and the new list columns.

Dashboard Viewer

- On Vista and Vista and Windows Server 2008, you must run as administrator when starting and running the Dashboard Viewer application. Otherwise the application will not start.
- Applikasjonen har heller ikke 64-bits support.

Unable to delete network definitions in the NIS Manager

- It is not possible to delete network definition while SSH or Telnet authentication information exists in the definition.

Interfaces monitored by the interface_traffic probe may result in “none existing interfaces” in dynamic dashboards

- Interfaces monitored by the interface_traffic probe including a hyphen (-) in their names and aggregated traffic QoS enabled will result in “none existing interfaces” in dynamic dashboards. The interface name will not be recognized by the group_server probe.
  Solve the problem by renaming the interface names (avoid hyphens in the name) in the interface traffic probe.
  Example:
  If you have an interface named "-Ether" and configure interface_traffic probe to send QoS's on aggregated traffic, you will get a dashboard created on a "non existing interface" called "Ether", including the aggregated traffic data.
  If you select "interface and aggregated traffic", the IN/OUT traffic will be visible in the "-Ether" dashboard, and the aggregated traffic will be visible in the "Ether" dashboard.

NimBUS Manager - GUI

- Existing URL http://support.nimsoft.com no longer launches in a separate window. To fix, right-click the link and select *Options > Launch URL in separate window when double-click.*
- Unable to drag and drop licenses or probes on Vista, due to the UAC (User Access Control) in Vista.

Library limitations may result in empty trend graphs in the Enterprise Console

- The NimBUS library used to transfer data breaks if the total data size transferred exceeds 500K.
  This will result in empty trend graphs in Enterprise Console dashboards. Typically this might happen if the time period set up for the trend graph spans over several weeks.
  A way to avoid this problem is to add a new raw configuration parameter *max_db_rec_count* to the variable_server probe, setting an upper limit of number of records returned from the generic query command. Add the new key max_db_rec_count with a value of for example 1000.

AIX computers not found by discovery, using SNMP

- Certain types of AIX computers might not be found when running discovery, using SNMP. The reason is that the format in the computer description field can not be read (AIX sends binary data as description over the SNMP API that we use).

Discovery limitations

- The discovery scope for one Discovery Agent is 256 IP-addresses. The ACE creates monitoring profiles for the probes distributed during the installation process. Up to 1000 profiles can be created for each of the probes, except the rsp probe which can have a maximum of 40 profiles.

Discovery Agent

- The NetBIOS scan performed by the discovery_agent will not work on Vista and Windows Server 2008. The reason is that the NetBIOS API is not supported on these platforms.

NIS limitations on SNMP

- The NIS might not be able to communicate with all SNMP devices. The reason is that not all of the NimBUS probes distributed during the installation process yet support all security mechanisms in SNMP ver. 3.

Uninstalling NimBUS, using Add/Remove Programs in the Control Panel

- Uninstalling NimBUS 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 NimBUS again.

WebService 3.11 installation

- If you are installing NimBUS Webservice 3.11 together with NimBUS Webservice 2.0 or 2.1, you need to make sure that the WebService 3.11 installation is set up with Microsoft .NET Framework 2.0 version under IIS administration.
- To use the User/SetAdministratorPassword service with Account/Login's functionality, you need to make sure that the process the IIS is running under got write access to the directory you installed into (the User/SetAdministratorPassword service needs to create a file where it stores the encrypted password).
- **Vista and Windows Server 2008 specific**
  Before installing the Web Service on Vista, IIS 6.0 Management Compatibility must be enabled (see description under the *Prerequisites* section).

Report Engine

- Occasionally we have seen that dynamic reports do not appear after a NimBUS Server upgrade. This can be solved by restarting the report_engine probe, which will re-establish the get_qos_urls list properly (CR).
- Occasionally we have seen that copy/paste of report elements when creating reports in the report_engine GUI may result in GUI problems.

Probes not activated after NimBUS Server installation

- During Server installation several components are distributed and configured. On slow systems we have occasionally seen situations where some of the probes were not started during the installation. This can be detected in NimBUS Manager, and can be fixed simply by activating the probe.

Temporary files erroneously generated by the installer into the system root directory instead of the temp directory

- A number of temporary files are erroneously generated by the installer into the system root directory instead of the temp directory. These files are unnecessary and can be safely deleted from the system. The

functioning of the runtime library will not be affected by this.
Its a known bug and is planned to be fixed in VS2008 SP1.
See http://support.microsoft.com/kb/950683 for details.