Nimsoft Monitor Server

Installation Guide

v6.00

Document Revision History

Version	Date	Changes
1.0	6/30/2010	Initial version *Nimsoft Server Installation and User Guide*
2.0	10/24/2011	New title: *Nimsoft Server Installation Guide.* Contains only content and procedures for new installs of Nimsoft Server. Updated to include the InstallAnywhere Windows installer. Added section on Bulk Robot Deployment. Previous manual's user guide content migrated to new document: *Nimsoft Server Configuration Guide*.
3.0	12/16/2011	Minor revisions and documentation fixes for Nimsoft Server 5.61
3.1	1/4/2012	Documentation bug fixes; "AAI robot installer packages" relabeled as "robot_msi_rpm installer packages."
3.2	2/22/2012	Documentation fixes and hardware capacity planning figures revised.
3.3	3/12/2012	Documentation fixes; added content for remote access and authentication when installing with a MySQL database.
4.0	6/29/2012	Revised for NMS 6.00.

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:

- 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.

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.

Contents

Chapter 4: Nimsoft Client Installation 65

Appendix A: Bulk Robot Deployment with the Automated Deployment Engine (ADE) 80

Appendix B: Installing NMS in an Active/Passive Microsoft Cluster 92

Appendix C: MySQL Windows Installation 97

Appendix D: Installation Modifications to Windows Systems 102

Chapter 1: Introduction

This section contains the following topics:

About This Guide

This guide helps you successfully install the Nimsoft Monitor Server (NMS) software. It contains the following sections:

- **Introduction**—an overview of the installation phases
- **NMS Pre-installation**—pre-installation computer and database configuration
- **NMS Installation**—NM server installation
- **Nimsoft Client Installation**—deployment of client software into your monitored infrastructure
- Other sections cover bulk/remote robot installation (robot_msi_rpm installer packages), legacy Windows installation, installation on a Microsoft Cluster, and MySQL installation on Windows.

Note: The Nimsoft Unified Management Portal (UMP), Unified Reporter (UR) and Service Desk (NSD) products have their own installation guides, available from the **Downloads** tab at support.nimsoft.com.

Note: For upgrade installations, see the *NMS Release Notes and Upgrade Guide*, available from the **Downloads** tab at support.nimsoft.com.

Installation Overview

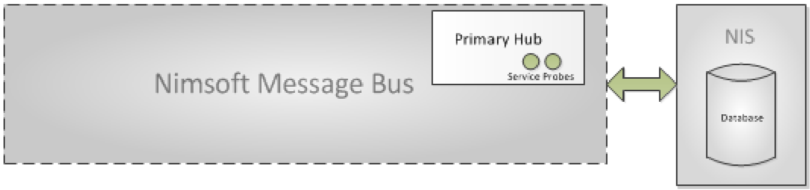
Basic Installation

NMS is made up of a number of distributed and loosely coupled software modules. The process of installing these modules to build out a full system can be divided into three phases:

1. **Preparation and pre-installation.** Properly configuring the operating system and database generally leads to a smooth software installation process. Refer to **Chapter 2: NMS Pre-installation** (page 14).

2. **NM server installation**. In this phase you install the foundation for Nimsoft Monitor, which consists of:

   - Nimsoft Message bus
   - Nimsoft Domain
   - Nimsoft Primary Hub
   - Server robot and probes
   - Server web page, which has links to installers for client systems
   - Nimsoft Information Store (NIS) database, also referred to as the SLM database
   - User accounts on the NM server and database server that are needed by Nimsoft Monitor

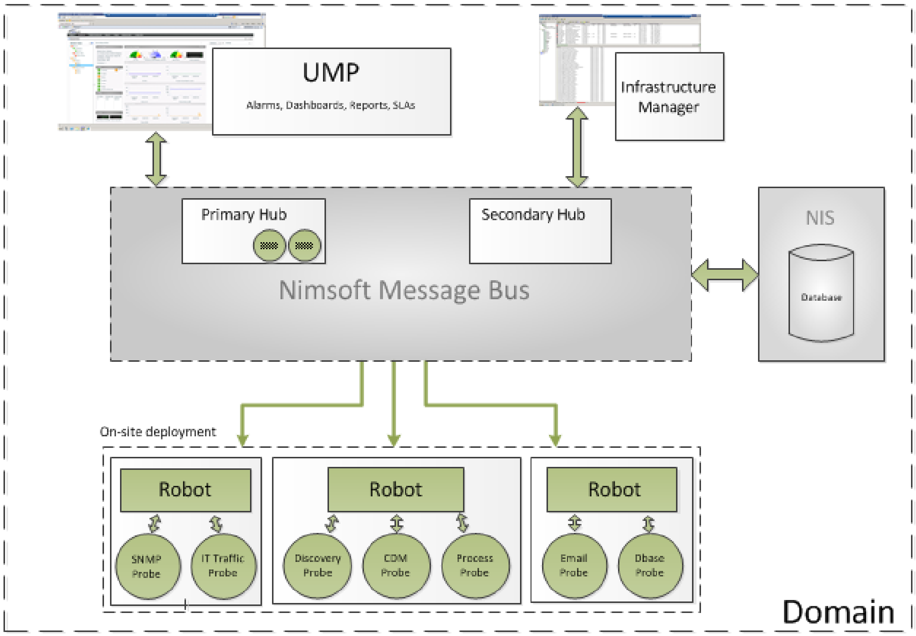
   Refer to **Chapter 3: NMS Installation** (page 50).

3. **Client installation.** You install Nimsoft infrastructure (hubs, robots and probes) on client systems to monitor devices and services and to allow management consoles (such as Infrastructure Manager) to be run from other systems.

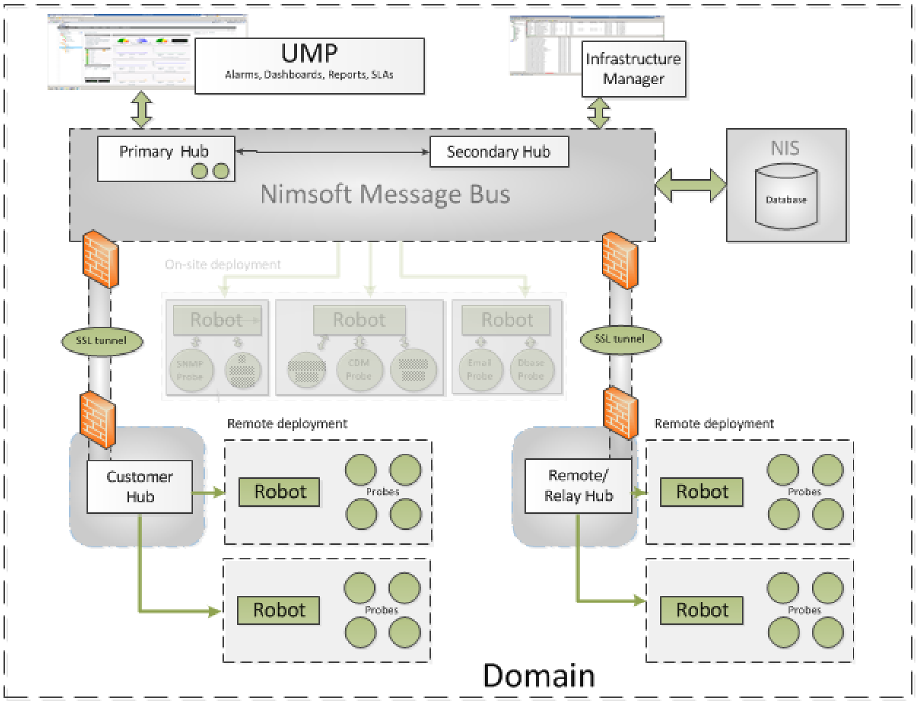
   Note: After installation, most users install Unified Management Portal (UMP). See the *UMP Installation Guide* available for download at Nimsoft support.

You can install infrastructure:

- **Locally** into your IT environment to monitor and manage on-premise devices and services.



- **Remotely** to extend the managed domain by deploying infrastructure to remote sites. This may require you to create secure tunnels between Hubs.



Required Ports

The ports required for a successful infrastructure installation depend on how Hubs are set up. If we assume the default port of 48000 is used for the first port assigned, port usage is as follows.

- Single-hub infrastructure or multi-hub infrastructure that does NOT use tunnels
  - **48000** for robot's controller probe
  - **48001** for the robot's spooler probe
  - **48002** to allow robot-to-hub and manager-to-hub communications
  - A port for each probe you install; these ports start at **48004** and are assigned to each probe as the probe is activated
- Multi-hub infrastructure that uses tunnels that are NOT SLL tunnels
  - All ports used in a single-hub installation
  - **48003**, the port to the tunnel server (this also can bet set to **443**)
- Multi-hub infrastructure that uses Nimsoft SSL tunnels
  - **48000** (controller) and **48002** (hub)
  - **48003** to allow the tunnel client to access the tunnel server
  - **8008** (httpd) to allow users to access web components

  To learn more about Nimsoft SSL tunnels and required ports, refer to:

  - Working with Firewalls and DMZs (page 10)
  - Required Ports for SSL Tunnels (page12)

Working with Firewalls and DMZs

Most companies today have one or more firewalls in their network, both internally between different networks and externally against the Internet or a DMZ (derived from the term *demilitarized zone*, an area between nation states in which military action is not permitted).

Network administrators are often reluctant to open a firewall for a lot of IP addresses and ports in order to make it possible for Management applications to work. This makes it difficult to administer and monitor the whole network from a central location.

The solution is to set up a secure shell (SSH) tunnel between two Hubs that is separated by a firewall. The tunnel sets up a VPN-like (Virtual Private Network) connection between the two Hubs and enables all requests and messages to be routed over the tunnel and dispatched on the other side. This routing will be transparent to all the users within the Nimsoft Monitor domain.

You can set tunnels between any Nimsoft Hubs. Note that a hub in the DMZ must have a public IP address if you want to access it from the Internet.

Security

Security is handled in two ways: *certificates* to authenticate the tunnel client and *encryption* to secure the network traffic.

- **Authorization and Authentication**
  Certificates provide authorization and authentication. Both the client and the server need valid certificates issued by the same CA (Certificate Authority). The system receiving the connection (the server) is its own CA and will only accept certificates issued by itself.
- **Encryption**
  Encryption settings range from *None* to *High*. No encryption means that the traffic is still authenticated and is therefore recommended for tunnels within LANs and WANs. Higher encryption level since are more resource intensive for the systems at both ends of the tunnel.

Which Hub Should Be the Server?

Because the tunnel server uses a fair amount of computing power, the hub with the lower load should be the server. If you have central hub and several remote hubs attaching to the central hub, it is better for the remote hubs to be the tunnel servers so that each incremental remote hub only adds a tiny amount of overhead to the central hub.

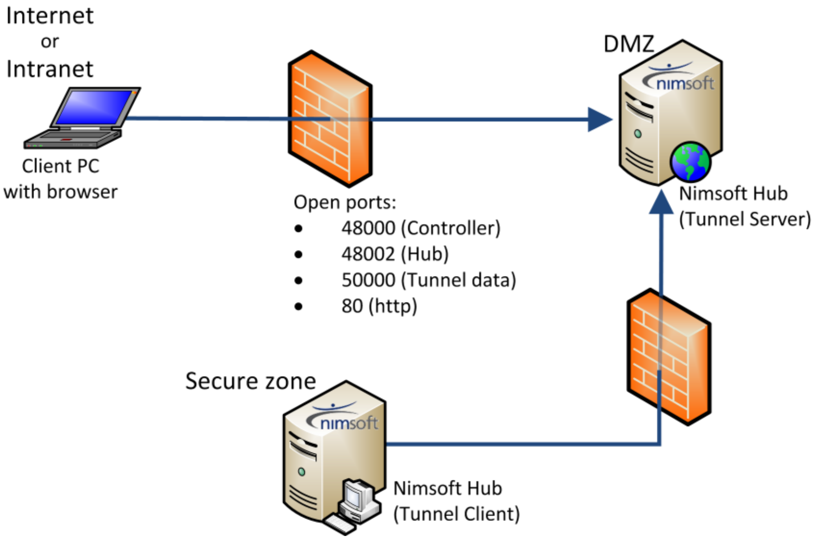
Required Ports for SSL Tunnels

The following ports are required.

- **48000** (controller) and **48002** (hub)
- A configured tunnel server port (default is 48003, this also can bet set to 443) allows the tunnel client to access the tunnel server. How this is set up in the firewall is firewall-dependent. If necessary, refer to your firewall documentation on how to open a connection between the two systems.
- **Port 8008** (httpd) is required if you want users to access web components, such as SLA reports and dashboards. A web server can be used.

Note: After you have opened the external firewall for the listed ports, you must make Dashboards and SLA reports available on the DMZ system. This can be accomplished using the WebExport utility for Dashboards and by setting up an FTP profile in the SLA system.

The example below shows the components installed and the ports that need to be opened in a scenario with a DMZ and two firewalls.



Tunnel Setup Overview

You must first set up the tunnel server (which generates the client certificate), then set up the tunnel client (where the certificate must reside).

You can set up tunnels:

- **During installation**. The Hub installation processes include option to set up DMZ tunnel servers and clients. For details refer to:
  - **Installing Windows Robot, Hub and Distribution Server** (page 70)
  - **Linux or Solaris** (page 73)
- On existing Hubs after installation. For details, refer to the online help in Infrastructure Manager.

Post-installation Tasks

After installation, you will configure the various Nimsoft infrastructure components within your environment. This includes:

- Tuning thresholds so that alarms are raised appropriately
- Setting up actions in response to alarms
- Setting up SLAs
- Configuring dashboards to view QoS information

For instructions and details, refer to the:

- *NMS Configuration Guide* available from the Nimsoft support website
- *O*nline help available with each component probe, package, or product

Chapter 2: NMS Pre-installation

A correct configuration of the host computer and database helps ensure a successful installation.

NMS is supported on Windows, Linux, and Solaris platforms, with certain supported databases for each of these platforms. For details, see the Nimsoft Compatibility Support Matrix, which is updated regularly.

All pre-installation information for a particular operating system/database combination is in one section. Refer to the section that applies to your choice of OS and database.

This chapter contains the following topics:

Note: Because disk compression reduces I/O performance, NMS does not support compression on Windows. The Nimsoft Hub message queue is stored on disk, and is constantly undergoing read and write activity.

Pre-installation Planning

Determining Hardware Requirements

Assessing the hardware requirements for any large and complex software system is a challenge. Oversizing seems wasteful, but underestimating needs can create performance problems. Unfortunately, no fixed rules or formulas can guarantee a minimum optimal configuration. Every environment has its own challenges and opportunities, including yours.

When considering the hardware you'll apply to the Nimsoft solution, keep in mind that a hardware configuration that works today may need to grow in the future. Therefore, Nimsoft recommends taking future forecast growth into consideration when planning your hardware requirements. Use the information in this section to begin planning your deployment, but consider that your particular situation may impose greater or lesser demands on the system.

Many professionals believe it is wise to obtain and use hardware of the most current generation. By starting with hardware of the latest architecture, one can anticipate the longest useful life.

Consult your Nimsoft Sales Engineer if you have any doubts or concerns about your hardware needs.

Distribution of Nimsoft Components

The Nimsoft solution comprises three primary components:

- NM server, which contains (and is sometimes referred to as) the Primary Hub
- Nimsoft Information Store (NIS) database, previously called the SLM database
- Unified Management Portal (UMP)

Each primary component plays a critical role in the overall Nimsoft solution. When installing for a small environment, you may choose to install everything on a single machine. However, it is usually advisable to distribute these components across multiple virtual or physical servers. This gives each component sufficient computing power and memory to perform optimally.

Note: The optional UMP DMZ proxy server component must be installed on an additional system.

In addition, you may want to install two Hubs on the same domain, and use the High-Availability probe to provide fail-over capability. This provides two levels of assurance in the event the Primary Hub fails:

- Your Nimsoft solution will continue to operate seamlessly
- Your user and security data—such as Nimsoft user definitions, ACLs, and so on—will remain intact and fully functional.

Capacity Planning

While every situation is unique in its own way, the following size categories can give you a starting point to assess your hardware requirements.

One hub, fewer than 100 robots

In a modest deployment—for example, a proof-of-concept for a small business in which there is a single hub and a few dozen robots—Nimsoft recommends you use no fewer than two servers or virtual machines:

- Use one for the NMS (Primary Hub) and Unified Management Portal.
- Use the other for the database server that hosts the NIS database.

For good performance, each server should have at least one dual-core processor (XEON-class 2.4 GHz or better) and no less than 8GB of memory.

Up to five hubs, fewer than 250 robots

In a medium-scale deployment—for example, a small government agency or business in which there are several hubs and a few hundred robots—Nimsoft recommends you use no fewer than three servers or virtual machines:

- Use one for the NMS (Primary Hub) and one for the Unified Management Portal.
- Use another for the database server that hosts the NIS database.

For good performance, each server should have the equivalent of one or two quad-core processors (XEON-class 2.4 GHz or better), each with no less than 12GB of memory.

Up to twenty hubs, fewer than 500 robots

In a large-scale deployment, Nimsoft recommends no fewer than three physical servers or virtual machines:

- Use one generously configured virtual machine or physical server for the NMS (Primary Hub) system. The NM server system should have dual quad-core processors (XEON-class 2.4 GHz or better), and contain 12GB or more of memory.
- Use one generously configured virtual machine or a physical server for the Unified Management Portal.
- Use one physical server for the NIS database server. The NIS database should be run on dual- or quad-core processors (XEON-class 3.0 GHz or better), with 12GB to 18GB of physical memory.

Up to fifty hubs, fewer than 1000 robots

In a major deployment, Nimsoft recommends no fewer than three physical servers:

- Use one for the NMS (Primary Hub). The NM server system should have dual quad-core processors (XEON-class 2.4 GHz or better), and contain 16GB or more of memory.
- Use one for the Unified Management Portal.
- Use one for the NIS database server. The NIS database should be run on quad- or eight-core processors (XEON-class 3.0 GHz or better), with 18GB to 24GB of physical memory.

Over fifty hubs, over 1000 robots

A deployment of this scale should be specified and planned using the resource levels given above as a starting point, along with the assistance of Nimsoft professional services or a Nimsoft certified partner.

Determining Database Performance Requirements

Relational database server performance is heavily affected by disk I/O performance and server bus bandwidth. Crowded VM hosts, clusters, or heavily shared storage in VM environments are not recommended for hosting the Nimsoft NIS database.

Nimsoft recommends starting with at least 1TB of storage for the NIS database; RAID 10 is suggested for speed and reliability. Also consider spreading the database files across multiple disks to improve I/O performance. Choose drive subsystems with low latency and seek times, high spindle speeds and high interconnect bandwidth.

Further, data redundancy/synchronization model needs to be considered on an on-going basis, taking into account the growth of the database. Selecting the right database storage solution is beyond the scope of this document--we recommend you discuss this with your storage vendor/VAR/consultant.

Microsoft Windows and MS-SQL Server

Your system must meet these criteria. Check the Nimsoft Compatibility Support Matrix to confirm which versions are supported.

NM server host system options

- Windows Server 2003
- Windows Server 2008

  Note: For ***non-production uses*** (such as proof-of-concept) testing, NM server can be hosted on Windows 7, Windows Vista or Windows XP.

Database options

- SQL Server 2008
- SQL Server 2008 R2

Windows System Prerequisites

Microsoft Windows User Account Control

Supported Microsoft Windows platforms newer than Windows XP and Windows 2003 implement User Account Control (UAC) to prevent unauthorized modifications to the computer.

If UAC is turned on, administrative privileges are needed to install NMS. On Windows Vista, they are also needed to run the NM server.

Note: Nimsoft recommends using Windows Vista only for test or evaluation.

Note: Although Nimsoft does not recommend it, you can turn UAC off if you prefer. See the Windows documentation for details.

Java Virtual Machine (JVM)

The installer requires Java Virtual Machine (JVM) 1.6 or later. It is generally acceptable to simply install the latest JVM, but be sure to check the *NMS Release Notes and Upgrade Guide* for the latest updates on supported JVM versions.

To ensure you have a supported Java Virtual Machine, execute:

```
java -version
```

If the command fails:

- If you believe your system has a supported version, make sure that the JVM is part of the system PATH environment variable.
- If there is no directory on the system for Java, go to http://www.java.com (not affiliated with Nimsoft) and download a Java distribution. Install it according to the directions on that site.

  Ensure that the JVM is included in the PATH environment variable by executing:

  ```
  java -version
  ```

Important! Be sure you get the right package (32-bit or 64-bit) for your operating system. For example, you *must* use a 64-bit JVM if you have a 64-bit operating system; a 32-bit JVM will not suffice.

Java on VMware Virtual Machines

When installing on a VMware ESX Server, please review VMware's *Enterprise Java Applications on VMware - Best Practices Guide*. Go to http://www.vmware.com/resources/techresources/1087 (not affiliated with Nimsoft).

Firewalls and Virus Scanners

Before installation:

- Shut down any anti-virus software (required).
- Shut down the firewall (optional). While not always necessary, this maximizes your chance of a successful installation. If you keep your firewall running, you must at least:
  - Ensure the port between the NMS system and the database system is open.
  - Specify a starting port during NMS installation (the recommended default is port 48000).
  - Ensure that an adequate range of ports are open (for example, ports 48000 through 48020). At minimum, the first three ports assigned (controller, spooler, and hub) must be open. The port used for **distsrv** is dynamically assigned.

Important: Turn the firewall and anti-virus software when installation is complete.

Database Prerequisites

Important: Nimsoft strongly encourages you to begin with a fresh installation of your database software on an otherwise clean system. NM server has a track record of easy and successful installation in such an environment. A pre-existing database can be used, but experience shows you may encounter subtle configuration conflicts that are hard to diagnose and make the experience unnecessarily difficult.

Microsoft SQL Server Software Installation

Nimsoft recommends only the full licensed product version with database authentication or Windows authentication for production environments.

Check the Nimsoft Compatibility Support Matrix for supported versions.

Note: Use the free Express version only for evaluation or demonstration purposes.

To obtain a copy of Microsoft SQL Server, go to www.microsoft.com/sqlserver/ (not affiliated with Nimsoft). Make sure the version is compatible with your hardware (32-bit or 64-bit).

Follow the installation instructions available with the download.

Configuring Microsoft SQL Server

The simplest option:

- Accept the default instance name when you install Microsoft SQL Server
- Use the default port (1433) when you install NMS

Other options have different requirements. If you:

- Use a non-default instance name for the Microsoft SQL Server, you must use the default port (1433) when installing NMS.
- Want to use a port *other* than 1433 for NMS, you *must* use the default MS SQL Server instance name.

During NM server installation you will select one of these authentication options:

- Using SQL Server with SQL Server login
- Using SQL Server with windows authentication

You may need to make database modifications in advance, as described in the following sections.

SQL Server with SQL Server Login

No modifications are needed. You must provide the SQL Server user name and password during installation.

SQL Server with Windows NT Authentication

Windows Authentication has these requirements.

- Before you install NM server, you must:
  - Add a domain administrator with permission to *Log on as a Service*. This is required on both the NMS system and on the database server system. For instructions, go to:

    http://technet.microsoft.com/en-us/library/dd277404.aspx
  - Configure SQL Server to use Windows Authentication For instructions, go to:

    http://msdn.microsoft.com/en-us/library/aa337562.aspx

  Note: The user installing NM server must have the same administrative rights as those used to install the MS-SQL Server, and supply those credentials during the installation. Specifically, the data_engine probe must have identical administrative rights on both the local computer and the MS-SQL Server computer.
- After installation, you must change the login for the Nimsoft Robot Watcher service to run as a user with the same administrative rights as are used to access the MS-SQL Server.
- **Important:** Ensure that you enter the following as the name for the system where you will install UMP:

  ```
  <domain>\<UMP_system_name>$
  ```

SQL Server Express

Note: SQL Server Express can be used for demonstration and proof-of-concept installations. It is not supported for production use because of limitations it imposes on security, storage capacity, and performance.

To use SQL Server Express, you must:

- Specify the following options to the SQL Server Express setup program:
  SAPWD=<*password*> SECURITYMODE=SQL DISABLENETWORKPROTOCOLS=0
- Use this format when specifying the server name:
  <*server_name*>\SQLEXPRESS
- Use the default port (1433) when you install NMS because SQL Server Express installs a named instance (SQLExpress) unless a default instance is specified.

Microsoft Windows and MySQL Server

Your system must meet these criteria. Check the Nimsoft Compatibility Support Matrix to confirm which versions are supported.

NMS host system options

- Windows Server 2003
- Windows Server 2008

  Note: For ***non-production uses*** (such as proof-of-concept) testing, NMS can be hosted on Windows 7, Windows Vista or Windows XP.

Database options

- MySQL Server 5.5 (recommended due to improved performance and scalability)
- MySQL Server 5.1 (supported but will be discontinued in a future release)

Windows System Prerequisites

Microsoft Windows User Account Control

Supported Microsoft Windows platforms newer than Windows 2003 implement User Account Control (UAC) to prevent unauthorized modifications to the computer.

If UAC is turned on, administrative privileges are needed to install NMS. On Windows Vista, they are also needed to run NMS.

Note: Nimsoft recommends using Windows Vista only for test or evaluation.

Note: Although Nimsoft does not recommend it, you can turn UAC off if you prefer. See the Windows documentation for details.

Java Virtual Machine (JVM)

The installer requires Java Virtual Machine (JVM) 1.6 or later. It is generally acceptable to simply install the latest JVM, but be sure to check the *NMS Release Notes and Upgrade Guide* for the latest updates on supported JVM versions.

To ensure you have a supported Java Virtual Machine, execute:

```
java -version
```

If the command fails:

- If you believe your system has a supported version, make sure that the JVM is part of the system PATH environment variable.
- If there is no directory on the system for Java, go to http://www.java.com (not affiliated with Nimsoft) and download a Java distribution. Install it according to the directions on that site.

  Ensure that the JVM is included in the PATH environment variable by executing:

  ```
  java -version
  ```

  Important! Be sure you get the right package (32-bit or 64-bit) for your operating system. For example, you *must* use a 64-bit JVM if you have a 64-bit operating system; a 32-bit JVM will not suffice.

Java on VMware Virtual Machines

When installing on a VMware ESX Server, please review VMware's *Enterprise Java Applications on VMware - Best Practices Guide*. Go to http://www.vmware.com/resources/techresources/1087 (not affiliated with Nimsoft).

Firewalls and Virus Scanners

Before installation:

- Shut down any anti-virus software (required).
- Shut down the firewall (optional). While not always necessary, this maximizes your chance of a successful installation. If you keep your firewall running, you must at least:
  - Ensure the port between the NMS system and the database system is open.
  - Specify a starting port during NMS installation (the recommended default is port 48000).
  - Ensure that an adequate range of ports are open (for example, ports 48000 through 48020). At minimum, the first three ports assigned (controller, spooler, and hub) must be open. The port used for **distsrv** is dynamically assigned.

Important: Turn the firewall and anti-virus software when installation is complete.

Database Prerequisites

Important: Nimsoft strongly encourages you to begin with a fresh installation of your database software on an otherwise clean system. NMS has a track record of easy and successful installation in such an environment. A pre-existing database can be used, but experience shows that you may encounter subtle configuration conflicts that are hard to diagnose and make the experience unnecessarily difficult.

Installing the MySQL Software

You can obtain a copy of Microsoft SQL Server from www.microsoft.com/sqlserver/ (not affiliated with Nimsoft). Make sure the version is supported and compatible with your hardware. You can use either the free Community Edition or licensed software.

For installation instructions, go to http://dev.mysql.com/doc/ (not affiliated with Nimsoft).

Required MySQL Configuration

Certain capabilities are set via MySQL variables.

Important: You must restart the database after making changes.

To check and set the required MySQL variable settings:

1. Log in as the MySQL administrator.
2. On the MySQL server, execute:

```
show variables like 'local_infile';
show variables like 'lower_case_table_names';
```

3. See if you have these variables and values.
   - local_infile: **ON**
   - lower_case_table_names: **1**
   - binlog_format: **mixed**
4. If the variables do not exist or the values are not correct, add these lines to the MySQL server configuration file or correct their values.

```
[mysqld]
 local_infile = 1
 lower_case_table_names = 1
 binlog_format = mixed
```

MySQL in Large Environments

If you are preparing for a large-scale or major deployment (as defined in **Capacity Planning** on page 16) you must set additional database parameters to allow for the greater demands of such an environment. Nimsoft recommends you begin with the values shown below, and then fine-tune settings depending on your circumstances.

To manually set database parameters for a large deployment:

As the MySQL administrator, add these lines to the MySQL server configuration file:

```
[mysqld]
 max_heap_table_size = 134217728
 query_cache_limit = 4194304
 query_cache_size = 268435456
 sort_buffer_size = 25165824
 join_buffer_size = 67108864
 max_tmp_tables = 64
```

Creating the Database and User

There are three ways to create the database and user.

- Installer creates the database; user is **root**
- Installer creates the database; user is an existing account
- Administrator creates the database and user *before* NMS installation

Installer Creates Database; User is root

This method creates the MySQL database and gives access to the **root** user. To do this, you must:

- Grant the root user account remote access before installation.

MySQL user accounts (including root) by default cannot access the MySQL server remotely. To allow this access, execute directly on the MySQL database server:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY ‘<root password>’ WITH GRANT OPTION;
GRANT TRIGGER ON nimsoftnis.* TO 'root'@'%' WITH GRANT OPTION;
GRANT SUPER ON *.* TO 'root'@'%';
FLUSH PRIVILEGES;
```

Installer Creates Database; User is an Existing Account

The installer can create the database with an existing user provided you use root to set up the database during installation. To do this, you must:

- Grant the root user account remote access before installation.
- Specify the existing user account in the **Nimsoft SLM Database User Account** field during installation. The root account will create the database and apply the appropriate permissions to the existing user.

MySQL user accounts (including root) by default cannot access the MySQL server remotely. To allow this access, execute directly on the MySQL database server:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY '<root password>' WITH GRANT OPTION;
GRANT TRIGGER ON nimsoftnis.* TO 'root'@'%' WITH GRANT OPTION;
GRANT SUPER ON *.* TO 'root'@'%';
FLUSH PRIVILEGES;
```

Administrator Creates Database and User *Before* NMS Installation

The advantage of this approach is that you do not have to allow Nimsoft Server access to a MySQL account with administrator privileges. If you decide to create a Nimsoft-specific MySQL user account, you should also create the database.

To manually create the NIS database and user and grant the required privileges, follow these steps.

1. Login as the MySQL administrator.
2. Create the database. Execute:

```
CREATE DATABASE IF NOT EXISTS DB_name DEFAULT CHARACTER SET =utf8 DEFAULT COLLATE =utf8_unicode_ci;
```

   where *DB_name* is the desired database name.

3. Create the user and assign required privileges. Execute:

```
CREATE USER 'nmsuser'@'%' IDENTIFIED BY 'nmsuserpass';
GRANT ALL PRIVILEGES ON DB_name.* TO 'nmsuser'@'%';
GRANT TRIGGER ON DB_name.* TO 'nmsuser'@'%';
GRANT SUPER ON *.* TO 'nmsuser'@'%';
FLUSH PRIVILEGES;
```

   Where *nmuser* is the desired Nimsoft user name, *nmuserpass* is the desired password, and *DB_name* is the name of the database you created.

   Note: The single-quotation marks (') are required.

When you install NMS:

- Select **Use existing database** for the Nimsoft Server information.
- Provide the actual database name, user and password you created above.

Microsoft Windows and Oracle

Your system must meet these criteria. Check the Nimsoft Compatibility Support Matrix to confirm which versions are supported.

NMS host system options

- Windows Server 2003
- Windows Server 2008

  Note: For ***non-production uses*** (such as proof-of-concept) testing, NMS can be hosted on Windows 7, Windows Vista or Windows XP.

Database options

- Oracle 11g R1
- Oracle 11g R2

Windows System Prerequisites

Microsoft Windows User Account Control

Supported Microsoft Windows platforms newer than Windows XP and Windows 2003 implement User Account Control (UAC) to prevent unauthorized modifications to the computer.

If UAC is turned on, administrative privileges are needed to install NMS. On Windows Vista, they are also needed to run NMS.

Note: Nimsoft recommends using Windows Vista only for test or evaluation.

Note: Although Nimsoft does not recommend it, you can turn UAC off if you prefer. See the Windows documentation for details.

Java Virtual Machine (JVM)

The installer requires Java Virtual Machine (JVM) 1.6 or later. It is generally acceptable to simply install the latest JVM, but be sure to check the *NMS Release Notes and Upgrade Guide* for the latest updates on supported JVM versions.

To ensure you have a supported Java Virtual Machine, execute:

```
java -version
```

If the command fails:

- If you believe your system has a supported version, make sure that the JVM is part of the system PATH environment variable.
- If there is no directory on the system for Java, go to http://www.java.com (not affiliated with Nimsoft) and download a Java distribution. Install it according to the directions on that site.

  Ensure that the JVM is included in the PATH environment variable by executing:

  ```
  java -version
  ```

Important! Be sure you get the right package (32-bit or 64-bit) for your operating system. For example, you *must* use a 64-bit JVM if you have a 64-bit operating system; a 32-bit JVM will not suffice.

Java on VMware Virtual Machines

When installing on a VMware ESX Server, please review VMware's *Enterprise Java Applications on VMware - Best Practices Guide*. Go to http://www.vmware.com/resources/techresources/1087 (not affiliated with Nimsoft).

Firewalls and Virus Scanners

Before installation:

- Shut down any anti-virus software (required).
- Shut down the firewall (optional). While not always necessary, this maximizes your chance of a successful installation. If you keep your firewall running, you must at least:
  - Ensure the port between the NMS system and the database system is open.
  - Specify a starting port during NMS installation (the recommended default is port 48000).
  - Ensure that an adequate range of ports are open (for example, ports 48000 through 48020). At minimum, the first three ports assigned (controller, spooler, and hub) must be open. The port used for **distsrv** is dynamically assigned.

Important: Turn the firewall and anti-virus software when installation is complete.

Database Prerequisites

Important: Nimsoft strongly encourages you to begin with a fresh installation of your database software on an otherwise clean system. NMS has a track record of easy and successful installation in such an environment. A pre-existing database can be used, but experience shows that you may encounter subtle configuration conflicts that are hard to diagnose and make the experience unnecessarily difficult.

Oracle Environment

The Oracle Instant Client must be installed.

1. Go to the Oracle Instant Client download page:

   http://www.oracle.com/technetwork/database/features/instant-client/index-097480.html

2. Click the appropriate operating system and hardware.
3. Download and install the **Instant Client Package – Basic**.
4. Add the unzipped Instant Client directory to your path.
5. Restart the system.

Oracle Configuration

The Oracle administrator must set certain configuration parameters before installing NM server.

1. As the Oracle database administrator, enter the following commands:

```
ALTER SYSTEM SET NLS_COMP=LINGUISTIC SCOPE=SPFILE;
ALTER SYSTEM SET NLS_SORT=BINARY_AI  SCOPE=SPFILE;
ALTER SYSTEM SET PROCESSES = 300 SCOPE=SPFILE;
ALTER SYSTEM SET SESSIONS = 335 SCOPE=SPFILE; -- 1.1 * PROCESSES + 5
ALTER SYSTEM SET OPEN_CURSORS=1000 SCOPE=BOTH;
```

2. Restart the database.

Creating the Tablespace and User

You can either:

- Create the database tablespace and user before running the installer (recommended).

  Advantage: You do not have to allow NMS to access an Oracle account.

- Allow the NM server installer to create the Oracle tablespace.

  Risk: You must allow NMS to access an Oracle account with administrator privileges (such as SYS), which can be a security risk.

To create the database tablespace before installation

1. Log in as the Oracle administrator.
2. To create the tablespace, execute (all on one line):

```
create tablespace <nimsoftslm> datafile '<nimsoftslm>.dbf' size
1000m autoextend on maxsize unlimited;
```

   where *< nimsoftslm >* is a tablespace name of your choice.

3. To create the user and assign required privileges, execute:

```
create user <nmuser> IDENTIFIED BY Password1 DEFAULT TABLESPACE nimsoftslm;
grant all privileges to <nmuser>;
grant select on sys.v_$database to <nmuser>;
grant select on sys.v_$session to <nmuser>;
grant select on sys.v_$parameter to <nmuser>;
grant select on sys.sm$ts_used to <nmuser>;
grant select on sys.dba_data_files to <nmuser>;
grant select on sys.dba_tables to <nmuser>;
grant select on sys.dba_free_space to <nmuser>;
```

   where *<nmsuser>* is a user name of your choice.

4. Restart the database to create the user and assign required privileges.

   Note: Make a note of the user name and tablespace name, as you will need to know them during NM server installation.

Linux and MySQL Server

Your system must meet these criteria. Check the Nimsoft Compatibility Support Matrix to confirm which versions are supported.

NMS host system options

- Red Hat Enterprise Linux (RHEL) version 6
- Red Hat Enterprise Linux (RHEL) version 5
- SUSE Linux Enterprise Server (SLES) version 11
- SUSE Linux Enterprise Server (SLES) version 10

Note: The system must be running on x86 or AMD64 hardware.

Database options

- MySQL Server 5.5 (recommended due to improved performance and scalability)
- MySQL Server 5.1 (supported but will be discontinued in a future release)

System Prerequisites

Linux System Swap Space

The system must be configured with:

- 4 GB of swap space (minimum), or
- 6 GB or more of swap space (recommended for optimal performance and reliability).

This requirement applies to both the NM server system and the Unified Management Portal (UMP) server system

Java Virtual Machine (JVM)

The installer requires Java Virtual Machine (JVM) 1.6 or later. It is generally acceptable to simply install the latest JVM, but be sure to check the *NMS Release Notes and Upgrade Guide* for the latest updates on supported JVM versions.

To ensure you have a supported Java Virtual Machine, execute:

```
java -version
```

If the command fails:

- If you believe your system has a supported version, make sure that the JVM is part of the system PATH environment variable.
- If there is no directory on the system for Java, go to http://www.java.com (not affiliated with Nimsoft) and download a Java distribution. Install it according to the directions on that site.

  Ensure that the JVM is included in the PATH environment variable by executing:

  ```
  java -version
  ```

  Important! Be sure you get the right package (32-bit or 64-bit) for your operating system. For example, you *must* use a 64-bit JVM if you have a 64-bit operating system; a 32-bit JVM will not suffice.

Java on VMware Virtual Machines

When installing on a VMware ESX Server, please review VMware's *Enterprise Java Applications on VMware - Best Practices Guide*. Go to http://www.vmware.com/resources/techresources/1087 (not affiliated with Nimsoft).

The Standard C++ Compatibility Library

The standard C++ library must be present.

If necessary, download the distribution that applies to your architecture from:

- Your Linux distribution official support site
- http://www.rpmseek.com/rpm-pl/compat-libstdc%5C%5C-33.html?hl=com&cx=0:: (not affiliated with Nimsoft).

Install the package according to the instructions available with the download.

Firewalls and Virus Scanners

Before installation:

- Shut down any anti-virus software (required).
- Shut down the firewall (optional). While not always necessary, this maximizes your chance of a successful installation. If you keep your firewall running, you must at least:
  - Ensure the port between the NMS system and the database system is open.
  - Specify a starting port during NMS installation (the recommended default is port 48000).
  - Ensure that an adequate range of ports are open (for example, ports 48000 through 48020). At minimum, the first three ports assigned (controller, spooler, and hub) must be open. The port used for **distsrv** is dynamically assigned.

Important: Turn the firewall and anti-virus software when installation is complete.

Security-Enhanced Linux

Security-Enhanced Linux (SELinux) is a Linux feature that supports access control security policies. While shutting down SELinux before installing NM server is is not always necessary, it will maximize your chance for a successful installation.

If SELinux status is enabled, a **Current mode** of **permissive** is acceptable. Disabling SELinux entirely is an even safer approach.

If you must run NM server in SELinux **Enforcing** mode, add the Nimsoft shared libraries to a safe list, which lets the shared libraries. After you install NMS, execute:

```
chcon -f -t textrel_shlib_t /<NM_install>/hub/libldapssl.so.0
chcon -f -t textrel_shlib_t /<NM_install>/hub/libldapsdk.so.0
chcon -f -t textrel_shlib_t /<NM_installn>/hub/libldapx.so.0
```

where *NM_install* is the directory where NMS is installed.

Important: After installation, NMS will not function correctly in SELinux **Enforcing** mode until you add the Nimsoft shared libraries to the safe list.

About Localization

If the system is set to a non-English language (for example, Norwegian), you will get the following error message during installation:
The database does not exist or could not be created.

To prevent this, execute:

```
export LC_ALL=your_locale
```

where **your_locale** is the appropriate locale string (for example, *norwegian*).

Database Prerequisites

Important: Nimsoft strongly encourages you to begin with a fresh installation of your database software on an otherwise clean system. NMS has a track record of easy and successful installation in such an environment. A pre-existing database can be used, but experience shows that you may encounter subtle configuration conflicts that are hard to diagnose and make the experience unnecessarily difficult.

Installing the MySQL Software

You can obtain a copy of Microsoft SQL Server from www.microsoft.com/sqlserver/ (not affiliated with Nimsoft). Make sure the version is supported and compatible with your hardware. You can use either the free Community Edition or licensed software.

For installation instructions, go to http://dev.mysql.com/doc/ (not affiliated with Nimsoft).

Required MySQL Configuration

Certain capabilities are set via MySQL variables.

Important: You must restart the database after making changes.

To check and set the required MySQL variable settings:

1. Log in as the MySQL administrator.
2. On the MySQL server, execute:

```
show variables like 'local_infile';
show variables like 'lower_case_table_names';
```

3. See if you have these variables and values.
   - local_infile: **ON**
   - lower_case_table_names: **1**
   - binlog_format: **mixed**
4. If the variables do not exist or the values are not correct, add these lines to the MySQL server configuration file or correct their values.

```
[mysqld]
 local_infile = 1
 lower_case_table_names = 1
 binlog_format = mixed
```

MySQL in Large Environments

If you are preparing for a large-scale or major deployment (as defined in **Capacity Planning** on page 16) you must set additional database parameters to allow for the greater demands of such an environment. Nimsoft recommends you begin with the values shown below, and then fine-tune settings depending on your circumstances.

To manually set database parameters for a large deployment:

As the MySQL administrator, add these lines to the MySQL server configuration file:

```
[mysqld]
 max_heap_table_size = 134217728
 query_cache_limit = 4194304
 query_cache_size = 268435456
 sort_buffer_size = 25165824
 join_buffer_size = 67108864
 max_tmp_tables = 64
```

Creating the Database and User

There are three ways to create the database and user.

- Installer creates the database; user is **root**
- Installer creates the database; user is an existing account
- Administrator creates the database and user *before* NMS installation

Installer Creates Database; User is root

This method creates the MySQL database and gives access to the **root** user. To do this, you must:

- Grant the root user account remote access before installation.

MySQL user accounts (including root) by default cannot access the MySQL server remotely. To allow this access, execute directly on the MySQL database server:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY ‘<root password>’ WITH GRANT OPTION;
GRANT TRIGGER ON nimsoftnis.* TO 'root'@'%' WITH GRANT OPTION;
GRANT SUPER ON *.* TO 'root'@'%';
FLUSH PRIVILEGES;
```

Installer Creates Database; User is an Existing Account

The installer can create the database with an existing user provided you use root to set up the database during installation. To do this, you must:

- Grant the root user account remote access before installation.
- Specify the existing user account in the **Nimsoft SLM Database User Account** field during installation. The root account will create the database and apply the appropriate permissions to the existing user.

MySQL user accounts (including root) by default cannot access the MySQL server remotely. To allow this access, execute directly on the MySQL database server:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY ‘<root password>’ WITH GRANT OPTION;
GRANT TRIGGER ON nimsoftnis.* TO 'root'@'%' WITH GRANT OPTION;
GRANT SUPER ON *.* TO 'root'@'%';
FLUSH PRIVILEGES;
```

Administrator Creates Database and User *Before* NMS Installation

The advantage of this approach is that you do not have to allow Nimsoft Server access to a MySQL account with administrator privileges. If you decide to create a Nimsoft-specific MySQL user account, you should also create the database.

To manually create the NIS database and user and grant the required privileges, follow these steps.

1. Login as the MySQL administrator.
2. Create the database. Execute:

```
CREATE DATABASE IF NOT EXISTS DB_name DEFAULT CHARACTER SET =utf8 DEFAULT COLLATE =utf8_unicode_ci;
```

   where *DB_name* is the desired database name.

3. Create the user and assign required privileges. Execute:

```
CREATE USER 'nmsuser'@'%' IDENTIFIED BY 'nmsuserpass';
GRANT ALL PRIVILEGES ON DB_name.* TO 'nmsuser'@'%';
GRANT TRIGGER ON DB_name.* TO 'nmsuser'@'%';
GRANT SUPER ON *.* TO 'nmsuser'@'%';
FLUSH PRIVILEGES;
```

   Where *nmuser* is the desired Nimsoft user name, *nmuserpass* is the desired password, and *DB_name* is the name of the database you created.

   Note: The single-quotation marks (') are required.

When you install NMS:

- Select **Use existing database** for the Nimsoft Server information.
- Provide the actual database name, user and password you created above.

Linux and Oracle

Your system must meet these criteria. Check the Nimsoft Compatibility Support Matrix to confirm which versions are supported.

NMS host system options

- Red Hat Enterprise Linux (RHEL) version 6
- Red Hat Enterprise Linux (RHEL) version 5
- SUSE Linux Enterprise Server (SLES) version 11
- SUSE Linux Enterprise Server (SLES) version 10

Note: The system must be running on x86 or AMD64 hardware.

Database options

- Oracle 11g R1
- Oracle 11g R2

System Prerequisites

Linux System Swap Space

The system must be configured with:

- 4 GB of swap space (minimum), or
- 6 GB or more of swap space (recommended for optimal performance and reliability).

This requirement applies to both the NMS system and the Unified Management Portal (UMP) server system

Java Virtual Machine (JVM)

The installer requires Java Virtual Machine (JVM) 1.6 or later. It is generally acceptable to simply install the latest JVM, but be sure to check the *NMS Release Notes and Upgrade Guide* for the latest updates on supported JVM versions.

To ensure you have a supported Java Virtual Machine, execute:

```
java -version
```

If the command fails:

- If you believe your system has a supported version, make sure that the JVM is part of the system PATH environment variable.
- If there is no directory on the system for Java, go to http://www.java.com (not affiliated with Nimsoft) and download a Java distribution. Install it according to the directions on that site.

  Ensure that the JVM is included in the PATH environment variable by executing:

  ```
  java -version
  ```

  Important! Be sure you get the right package (32-bit or 64-bit) for your operating system. For example, you *must* use a 64-bit JVM if you have a 64-bit operating system; a 32-bit JVM will not suffice.

Java on VMware Virtual Machines

When installing on a VMware ESX Server, please review VMware's *Enterprise Java Applications on VMware - Best Practices Guide*. Go to http://www.vmware.com/resources/techresources/1087 (not affiliated with Nimsoft).

The Standard C++ Compatibility Library

The standard C++ library must be present.

If necessary, download the distribution that applies to your architecture from:

- Your Linux distribution official support site
- http://www.rpmseek.com/rpm-pl/compat-libstdc%5C%5C-33.html?hl=com&cx=0:: (not affiliated with Nimsoft).

Install the package according to the instructions available with the download.

Firewalls and Virus Scanners

Before installation:

- Shut down any anti-virus software (required).
- Shut down the firewall (optional). While not always necessary, this maximizes your chance of a successful installation. If you keep your firewall running, you must at least:
  - Ensure the port between the NMS system and the database system is open.
  - Specify a starting port during NMS installation (the recommended default is port 48000).
  - Ensure that an adequate range of ports are open (for example, ports 48000 through 48020). At minimum, the first three ports assigned (controller, spooler, and hub) must be open. The port used for **distsrv** is dynamically assigned.

Important: Turn the firewall and anti-virus software when installation is complete.

Security-Enhanced Linux

Security-Enhanced Linux (SELinux) is a Linux feature that supports access control security policies. While shutting down SELinux before installing NMS is not always necessary, it will maximize your chance for a successful installation.

If SELinux status is enabled, a **Current mode** of **permissive** is acceptable. Disabling SELinux entirely is an even safer approach.

If you must run NMS in SELinux **Enforcing** mode, add the Nimsoft shared libraries to a safe list, which lets the shared libraries. After you install NMS, execute:

```
chcon -f -t textrel_shlib_t /<NM_install>/hub/libldapssl.so.0
chcon -f -t textrel_shlib_t /<NM_install>/hub/libldapsdk.so.0
chcon -f -t textrel_shlib_t /<NM_installn>/hub/libldapx.so.0
```

where *NM_install* is the directory where NMS is installed.

Important: After installation, NMS will not function correctly in SELinux **Enforcing** mode until you add the Nimsoft shared libraries to the safe list.

About Localization

If the system is set to a non-English language (for example, Norwegian), you will get the following error message during installation:
The database does not exist or could not be created.

To prevent this, execute:

```
export LC_ALL=your_locale
```

where **your_locale** is the appropriate locale string (for example, *norwegian*).

Language Environment Variable

The language environment of the system where you intend to install NMS must match the language environment of the system where the Oracle database resides.

To test and match the language environment of the Oracle database and NMS host:

1. As the database administrator, run the following command on the database:

   ```
   SELECT userenv('language') from dual
   ```

   The result will be a string representing the language environment known to the database. For example, it might look something like this:

   ```
   AMERICAN_AMERICA.WE8MSWIN1252
   ```

2. Check the environment variables for the system that will host NMS. There must be an **NLS_LANG** environment variable with a value that matches the result of the previous step. For example:

   ```
   NLS_LANG=AMERICAN_AMERICA.WE8MSWIN1252;
   ```

   If there is no **NLS_LANG** environment variable, or if the value is not the same as the result of the SELECT command in the previous step, create an environment variable named **NLS_LANG** (if necessary) and set it to match the output of the SELECT command from the previous step.

Database Prerequisites

Important: Nimsoft strongly encourages you to begin with a fresh installation of your database software on an otherwise clean system. NMS has a track record of easy and successful installation in such an environment. A pre-existing database can be used, but experience shows that you may encounter subtle configuration conflicts that are hard to diagnose and make the experience unnecessarily difficult.

Required Oracle Environment

The Oracle Instant Client must be installed. Follow these steps.

1. Visit the Instant Client download page at http://www.oracle.com/technetwork/database/features/instant-client/index-097480.html.
2. Click the link for the operating system and hardware of your system.
3. Download the zip file for the Instant Client Package – Basic.
4. Install the Instant Client according to the directions on the web site. Be sure to add the unzipped Instant Client directory to your path.
5. Restart the system.

Required Oracle Configuration

The Oracle administrator must set certain configuration parameters before installing NMS.

To set the required Oracle configuration parameters:

1. As the Oracle database administrator, enter the following commands:

```
ALTER SYSTEM SET NLS_COMP=LINGUISTIC SCOPE=SPFILE;
ALTER SYSTEM SET NLS_SORT=BINARY_AI  SCOPE=SPFILE;
ALTER SYSTEM SET PROCESSES = 300 SCOPE=SPFILE;
ALTER SYSTEM SET SESSIONS = 335 SCOPE=SPFILE; -- 1.1 * PROCESSES
+ 5
ALTER SYSTEM SET OPEN_CURSORS=1000 SCOPE=BOTH;
```

2. Restart the database.

Creating the Tablespace and User

You can either:

- Create the database tablespace and user before running the installer (recommended).

  Advantage: You do not have to allow NMS to access an Oracle account.

- Allow the NMS installer to create the Oracle tablespace.

  Risk: You must allow NMS to access an Oracle account with administrator privileges (such as SYS), which can be a security risk.

To create the database tablespace before installation:

1. Log in as the Oracle administrator.
2. To create the tablespace, execute (all on one line):

   ```
   create tablespace <nimsoftslm> datafile '<nimsoftslm>.dbf' size
   1000m autoextend on maxsize unlimited;
   ```

   where *< nimsoftslm >* is a tablespace name of your choice.

3. To create the user and assign required privileges, execute:

   ```
   create user <nmuser> IDENTIFIED BY Password1 DEFAULT TABLESPACE nimsoftslm;
   grant all privileges to <nmuser>;
   grant select on sys.v_$database to <nmuser>;
   grant select on sys.v_$session to <nmuser>;
   grant select on sys.v_$parameter to <nmuser>;
   grant select on sys.sm$ts_used to <nmuser>;
   grant select on sys.dba_data_files to <nmuser>;
   grant select on sys.dba_tables to <nmuser>;
   grant select on sys.dba_free_space to <nmuser>;
   ```

   where *<nmsuser>* is a user name of your choice.

4. Restart the database to create the user and assign required privileges.

   Note: Make a note of the user name and tablespace name, as you will need to know them during NMS installation.

Linking Shared Oracle Libraries

Shared Oracle libraries must be linked. Follow these steps.

1. Create the following file:

   ```
   /etc/ld.so.conf.d/oracle.conf
   ```

2. In the file, enter the path to the Instant Client directory. For example:

   ```
   /root/instantclient_11_1
   ```

3. Save the file.

4. Navigate to the Instant Client directory (/root/instantclient_11_1 in the example).

5. Execute: ldconfig

6. Execute: ldd libociei.so

7. Verify that there are links for all the libraries and there are no **not found** messages. The output should look similar to this:

   ```
   linux-vdso.so.1 => (0x00007fff5b0e2000)
   libclntsh.so.11.1 => /root/instantclient_11_1/libclntsh.so.11.1
   (0x00007f36030b3000)
   libdl.so.2 => /lib64/libdl.so.2 (0x00007f3602eae000)
   libm.so.6 => /lib64/libm.so.6 (0x00007f3602c57000)
   libpthread.so.0 => /lib64/libpthread.so.0 (0x00007f3602a3a000)
   libnsl.so.1 => /lib64/libnsl.so.1 (0x00007f3602821000)
   libc.so.6 => /lib64/libc.so.6 (0x00007f36024c1000)
   libnnz11.so => /root/instantclient_11_1/libnnz11.so
   (0x00007f3602064000)
   libaio.so.1 => /lib64/libaio.so.1 (0x00007f3601e61000)
   /lib64/ld-linux-x86-64.so.2 (0x00007f360a0a0000)
   ```

Solaris and MySQL Server

Your system must meet these criteria. Check the Nimsoft Compatibility Support Matrix to confirm which versions are supported.

NMS host system

- Solaris 10

Note: The system must be running on SPARC or x86 hardware.

Database options

- MySQL Server 5.5 (recommended due to improved performance and scalability)
- MySQL Server 5.1 (supported but will be discontinued in a future release)

System Prerequisites

Solaris System Swap Space

The system must be configured with a minimum of 4 GB of swap space during installation. Nimsoft highly recommends 6 GB or more for optimal performance and reliability. This requirement applies to both the Nimsoft Monitor server and the UMP server.

To ensure sufficient swap space, review the man page for the **swap** command.

Java Virtual Machine (JVM)

The installer requires Java Virtual Machine (JVM) 1.6 or later. It is generally acceptable to simply install the latest JVM, but be sure to check the *NMS Release Notes and Upgrade Guide* for the latest updates on supported JVM versions.

To ensure you have a supported Java Virtual Machine, execute:

```
java -version
```

If the command fails:

- If you believe your system has a supported version, make sure that the JVM is part of the system PATH environment variable.
- If there is no directory on the system for Java, go to http://www.java.com (not affiliated with Nimsoft) and download a Java distribution. Install it according to the directions on that site.

  Ensure that the JVM is included in the PATH environment variable by executing:

  ```
  java -version
  ```

  Important! Be sure you get the right package (32-bit or 64-bit) for your operating system. For example, you *must* use a 64-bit JVM if you have a 64-bit operating system; a 32-bit JVM will not suffice.

Java on VMware Virtual Machines

When installing on a VMware ESX Server, please review VMware's *Enterprise Java Applications on VMware - Best Practices Guide*. Go to http://www.vmware.com/resources/techresources/1087 (not affiliated with Nimsoft).

Firewalls and Virus Scanners

Before installation:

- Shut down any anti-virus software (required).
- Shut down the firewall (optional). While not always necessary, this maximizes your chance of a successful installation. If you keep your firewall running, you must at least:
  - Ensure the port between the NMS system and the database system is open.
  - Specify a starting port during NMS installation (the recommended default is port 48000).
  - Ensure that an adequate range of ports are open (for example, ports 48000 through 48020). At minimum, the first three ports assigned (controller, spooler, and hub) must be open. The port used for **distsrv** is dynamically assigned.

Important: Turn the firewall and anti-virus software when installation is complete.

About Localization

If the system is set to a non-English language (for example, Norwegian), you will get the following error message during installation:
The database does not exist or could not be created.

To prevent this, execute:

```
export LC_ALL=your_locale
```

where **your_locale** is the appropriate locale string (for example, *norwegian*).

Database Prerequisites

Important: Nimsoft strongly encourages you to begin with a fresh installation of your database software on an otherwise clean system. NMS has a track record of easy and successful installation in such an environment. A pre-existing database can be used, but experience shows that you may encounter subtle configuration conflicts that are hard to diagnose and make the experience unnecessarily difficult.

Installing the MySQL Software

You can obtain a copy of Microsoft SQL Server from www.microsoft.com/sqlserver/ (not affiliated with Nimsoft). Make sure the version is supported and compatible with your hardware. You can use either the free Community Edition or licensed software.

For installation instructions, go to http://dev.mysql.com/doc/ (not affiliated with Nimsoft).

Required MySQL Configuration

Certain capabilities are set via MySQL variables.

Important: You must restart the database after making changes.

To check and set the required MySQL variable settings:

1. Log in as the MySQL administrator.
2. On the MySQL server, execute:

   ```
   show variables like 'local_infile';
   show variables like 'lower_case_table_names';
   ```

3. See if you have these variables and values.
   - local_infile: **ON**
   - lower_case_table_names: **1**
   - binlog_format: **mixed**
4. If the variables do not exist or the values are not correct, add these lines to the MySQL server configuration file or correct their values.

   ```
   [mysqld]
    local_infile = 1
    lower_case_table_names = 1
    binlog_format = mixed
   ```

MySQL in Large Environments

If you are preparing for a large-scale or major deployment (as defined in **Capacity Planning** on page 16) you must set additional database parameters to allow for the greater demands of such an environment. Nimsoft recommends you begin with the values shown below, and then fine-tune settings depending on your circumstances.

To manually set database parameters for a large deployment:

As the MySQL administrator, add these lines to the MySQL server configuration file:

```
[mysqld]
 max_heap_table_size = 134217728
 query_cache_limit = 4194304
 query_cache_size = 268435456
 sort_buffer_size = 25165824
 join_buffer_size = 67108864
 max_tmp_tables = 64
```

Creating the Database and User

There are three ways to create the database and user.

- Installer creates the database; user is **root**
- Installer creates the database; user is an existing account
- Administrator creates the database and user *before* NMS installation

Installer Creates Database; User is root

This method creates the MySQL database and gives access to the **root** user. To do this, you must:

- Grant the root user account remote access before installation.

MySQL user accounts (including root) by default cannot access the MySQL server remotely. To allow this access, execute directly on the MySQL database server:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY '<root password>' WITH GRANT OPTION;
GRANT TRIGGER ON nimsoftnis.* TO 'root'@'%' WITH GRANT OPTION;
GRANT SUPER ON *.* TO 'root'@'%';
FLUSH PRIVILEGES;
```

Installer Creates Database; User is an Existing Account

The installer can create the database with an existing user provided you use root to set up the database during installation. To do this, you must:

- Grant the root user account remote access before installation.
- Specify the existing user account in the **Nimsoft SLM Database User Account** field during installation. The root account will create the database and apply the appropriate permissions to the existing user.

MySQL user accounts (including root) by default cannot access the MySQL server remotely. To allow this access, execute directly on the MySQL database server:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY '<root password>' WITH GRANT OPTION;
GRANT TRIGGER ON nimsoftnis.* TO 'root'@'%' WITH GRANT OPTION;
GRANT SUPER ON *.* TO 'root'@'%';
FLUSH PRIVILEGES;
```

Administrator Creates Database and User *Before* NMS Installation

The advantage of this approach is that you do not have to allow Nimsoft Server access to a MySQL account with administrator privileges. If you decide to create a Nimsoft-specific MySQL user account, you should also create the database.

To manually create the NIS database and user and grant the required privileges, follow these steps.

1. Login as the MySQL administrator.
2. Create the database. Execute:

```
CREATE DATABASE IF NOT EXISTS DB_name DEFAULT CHARACTER SET =utf8 DEFAULT COLLATE =utf8_unicode_ci;
```

   where *DB_name* is the desired database name.

3. Create the user and assign required privileges. Execute:

```
CREATE USER 'nmsuser'@'%' IDENTIFIED BY 'nmsuserpass';
GRANT ALL PRIVILEGES ON DB_name.* TO 'nmsuser'@'%';
GRANT TRIGGER ON DB_name.* TO 'nmsuser'@'%';
GRANT SUPER ON *.* TO 'nmsuser'@'%';
FLUSH PRIVILEGES;
```

   Where *nmuser* is the desired Nimsoft user name, *nmuserpass* is the desired password, and *DB_name* is the name of the database you created.

   Note: The single-quotation marks (') are required.

When you install NMS:

- Select **Use existing database** for the Nimsoft Server information.
- Provide the actual database name, user and password you created above.

Solaris and Oracle

Your system must meet these criteria.

NMS host system

- Solaris 10

Note: The system must be running on SPARC or x86 hardware.

Database options

- Oracle 11g R1
- Oracle 11g R2

System Prerequisites

Solaris System Swap Space

The system must be configured with a minimum of 4 GB of swap space during installation. Nimsoft highly recommends 6 GB or more for optimal performance and reliability. This requirement applies to both the Nimsoft Monitor server and the UMP server.

To ensure sufficient swap space, review the man page for the **swap** command.

Java Virtual Machine (JVM)

The installer requires Java Virtual Machine (JVM) 1.6 or later. It is generally acceptable to simply install the latest JVM, but be sure to check the *NMS Release Notes and Upgrade Guide* for the latest updates on supported JVM versions.

To ensure you have a supported Java Virtual Machine, execute:

```
java -version
```

If the command fails:

- If you believe your system has a supported version, make sure that the JVM is part of the system PATH environment variable.
- If there is no directory on the system for Java, go to http://www.java.com (not affiliated with Nimsoft) and download a Java distribution. Install it according to the directions on that site.

  Ensure that the JVM is included in the PATH environment variable by executing:

  ```
  java -version
  ```

  Important! Be sure you get the right package (32-bit or 64-bit) for your operating system. For example, you *must* use a 64-bit JVM if you have a 64-bit operating system; a 32-bit JVM will not suffice.

Java on VMware Virtual Machines

When installing on a VMware ESX Server, please review VMware's *Enterprise Java Applications on VMware - Best Practices Guide*. Go to http://www.vmware.com/resources/techresources/1087 (not affiliated with Nimsoft).

Firewalls and Virus Scanners

Before installation:

- Shut down any anti-virus software (required).
- Shut down the firewall (optional). While not always necessary, this maximizes your chance of a successful installation. If you keep your firewall running, you must at least:
  - Ensure the port between the NMS system and the database system is open.
  - Specify a starting port during NMS installation (the recommended default is port 48000).
  - Ensure that an adequate range of ports are open (for example, ports 48000 through 48020). At minimum, the first three ports assigned (controller, spooler, and hub) must be open. The port used for **distsrv** is dynamically assigned.

Important: Turn the firewall and anti-virus software when installation is complete.

About Localization

If the system is set to a non-English language (for example, Norwegian), you will get the following error message during installation:
The database does not exist or could not be created.

To prevent this, execute:

```
export LC_ALL=your_locale
```

where **your_locale** is the appropriate locale string (for example, *norwegian*).

Language Environment Variable

The language environment of the system where you intend to install NMS must match the language environment of the system where the Oracle database resides.

To test and match the language environment of the Oracle database and NMS host:

1. As the database administrator, run the following command on the database:

   ```
   SELECT userenv('language') from dual
   ```

   The result will be a string representing the language environment known to the database. For example, it might look something like this:

   ```
   AMERICAN_AMERICA.WE8MSWIN1252
   ```

2. Check the environment variables for the system that will host NMS. There must be an **NLS_LANG** environment variable with a value that matches the result of the previous step. For example:

   ```
   NLS_LANG=AMERICAN_AMERICA.WE8MSWIN1252;
   ```

   If there is no **NLS_LANG** environment variable, or if the value is not the same as the result of the SELECT command in the previous step, create an environment variable named **NLS_LANG** (if necessary) and set it to match the output of the SELECT command from the previous step.

Database Prerequisites

This section covers database information that applies before you install NMS. When the database meets the prerequisites in this section, you avoid several potential installation difficulties.

Important: Nimsoft strongly encourages you to begin with a fresh installation of your database software on an otherwise clean system. NMS has a track record of easy and successful installation in such an environment. A pre-existing database can be used, but experience shows that you may encounter subtle configuration conflicts that are hard to diagnose and make the experience unnecessarily difficult.

Required Oracle Environment

To perform later tasks, the Oracle Instant Client must be installed.

1. Visit the Instant Client download page at http://www.oracle.com/technetwork/database/features/instant-client/index-097480.html.

2. Click the link for the operating system and hardware of your system.

3. Download the zip file for the Instant Client Package – Basic.

4. Install the Instant Client according to the directions on the web site. Be sure to add the unzipped Instant Client directory to your path.

5. Restart the system.

Required Oracle Configuration

The Oracle administrator must set certain configuration parameters before installing NMS.

To set the required Oracle configuration parameters:

1. As the Oracle database administrator, enter the following commands:

   ```
   ALTER SYSTEM SET NLS_COMP=LINGUISTIC SCOPE=SPFILE;
   ALTER SYSTEM SET NLS_SORT=BINARY_AI  SCOPE=SPFILE;
   ALTER SYSTEM SET PROCESSES = 300 SCOPE=SPFILE;
   ALTER SYSTEM SET SESSIONS = 335 SCOPE=SPFILE; -- 1.1 * PROCESSES + 5
   ALTER SYSTEM SET OPEN_CURSORS=1000 SCOPE=BOTH;
   ```

2. Restart the database.

Creating the Tablespace and User

You can either:

- Create the database tablespace and user before running the installer (recommended).

  Advantage: You do not have to allow NMS to access an Oracle account.

- Allow the NMS installer to create the Oracle tablespace.

  Risk: You must allow NMS to access an Oracle account with administrator privileges (such as SYS), which can be a security risk.

To create the database tablespace before installation:

1. Log in as the Oracle administrator.
2. To create the tablespace, execute (all on one line):

   ```
   create tablespace <nimsoftslm> datafile '<nimsoftslm>.dbf' size
   1000m autoextend on maxsize unlimited;
   ```

   where < *nimsoftslm* > is a tablespace name of your choice.

3. To create the user and assign required privileges, execute:

   ```
   create user <nmuser> IDENTIFIED BY Password1 DEFAULT TABLESPACE nimsoftslm;
   grant all privileges to <nmuser>;
   grant select on sys.v_$database to <nmuser>;
   grant select on sys.v_$session to <nmuser>;
   grant select on sys.v_$parameter to <nmuser>;
   grant select on sys.sm$ts_used to <nmuser>;
   grant select on sys.dba_data_files to <nmuser>;
   grant select on sys.dba_tables to <nmuser>;
   grant select on sys.dba_free_space to <nmuser>;
   ```

   where *<nmsuser>* is a user name of your choice.

4. Restart the database to create the user and assign required privileges.

   Note: Make a note of the user name and tablespace name, as you will need to know them during NMS installation.

Chapter 3: NMS Installation

This section is intended for a first-time installation of the NMS software.

To update an existing installation, download the *NM Server Release Notes and Upgrade Guide* at http://support.nimsoft.com/ and follow the instructions.

This section contains the following topics:

Overview

NMS installation is done with an InstallAnywhere installer, which unifies installation under Windows, Linux, and Solaris. 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)

Installation Requirements

All three methods require that you:

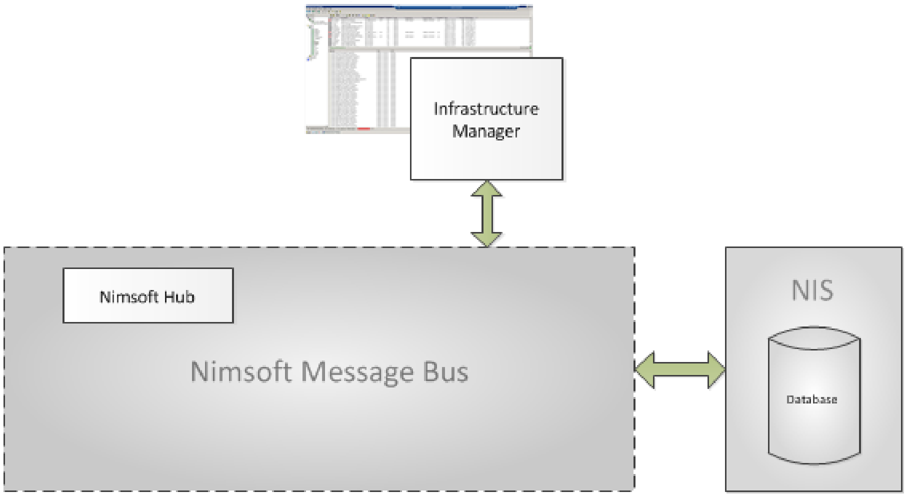
- Ensure all pre-installation requirements are met.
- Have administrator login information and IP addresses for your NMS system and database system.
- Download the installation package.
- Choose whether to have the installer create the Nimsoft database (called the Nimsoft Information Store, or NIS; also referred to as the SLM database).
- Have necessary information about your existing database (if already created), such as the database name and administrator login information. If you let the installer set up the database, you will specify this information during installation.
- Specify Primary Hub configuration information.

Installed Components

After installation, the following components reside on the NMS system:

- Nimsoft Primary Hub
- Nimsoft Message bus
- Server robot and Service probes
- Infrastructure Manager
- Server web page, which:
  - Will be accessed by users on client systems who will download and install Nimsoft infrastructure and management consoles
  - References packages used to automatically deploy and install Nimsoft infrastructure on many client systems

The Nimsoft Information Store (NIS) database, also referred to as the SLM database, resides on the database server.



Note: IM is installed on Windows systems with GUI installation mode. After NMS installation, it can be installed on any Windows system. **Refer to Installing a Management Console** (see page 69).

Note: If you are installing on a Microsoft high-availability platform, refer to Installing Nimsoft in an active/passive Microsoft Cluster" (see page 80) for additional details.

Installing NMS on Windows with the InstallAnywhere GUI

This procedure is intended for a first-time installation. If you want to:

- **Upgrade**, you must first disable package forwarding and clear the distsrv job queue (required) and remove customized probes in your probe archive (recommended). See the *NMS Release Notes and Upgrade Guide* for details.
- **Reinstall**, click **Cancel**, uninstall the prior version (see **Uninstalling NMS** on page 64), and restart the installation process. Note that your server configuration (domain and hub

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).

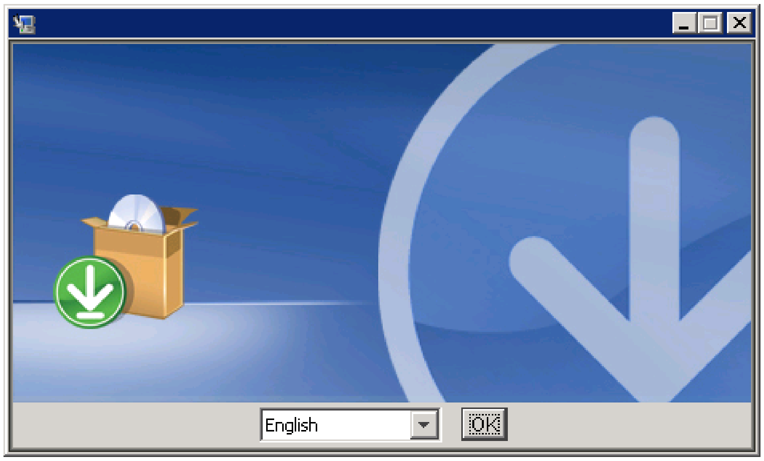
   Note: Turn the anti-virus scanners on again immediately after installation.

2. Log in to the Nimsoft Customer Support Center site.

   If you don't have a username and password, click **Home > Nimsoft Support** to request access.

3. Download the most recent NMS Install Package for Windows.

4. Double-click **installNMS**. The Install Package files are unpacked (this could take a few minutes), and the **Introduction** dialog displays.



5. Select a language and click **OK**.

   Note: If you select Spanish or Brazilian Portuguese, you must first configure cmd.exe (or the command shell you use) to use the appropriate codepage for your intended locale, and to display in a TrueType font, rather than a raster font. Otherwise, the installer messages will not display properly.

6. Make sure you have quit all other programs before continuing and follow the recommended precautions. Click **Next**.

   Note: If the installer detects a previous installation, the software version and a warning message are shown. If you want to:

   - **Upgrade**, you must first disable package forwarding and clear the distsrv job queue (required) and remove customized probes in your probe archive (recommended). See the *NMS Release Notes and Upgrade Guide* for details.
   - **Reinstall**, click **Cancel**, uninstall the prior version, and restart the install process. Note that your server configuration (domain and hub names, IP addresses, user accounts /passwords, etc.) is *not* retained.

7. Accept the terms of the license agreement to continue.
8. You are informed that the installer will launch the software after installation. Click **Next**.
9. Enter the path (or use the default path) to the folder where you want to install NMS, then click **Next**.
10. Select either:

    - **Create database**. The installer builds the required tables on the database server and creates the Nimsoft Information Store (NIS).
    - **Use existing database**. Nimsoft strongly encourages you to begin with a fresh installation of your database software on an otherwise clean system. Using a pre-existing database can result in subtle configuration conflicts that are difficult to diagnose.

11. Select the type of database (MySQL, Oracle, or SQL Server).
12. Perform the appropriate action for your database type:

    - **MySQL**— Go to the next step
    - **Oracle**—Note that the Oracle InstantClient is required
    - **SQL Server**—Choose a database authentication type (Windows or SQL Server)

13. Specify the database server parameters.

    The parameters available depend on the database type and whether it is new or existing. All fields are case sensitive.

    For details, refer to:

    - **MySQL Database Parameters** (page 58)
    - SQL Server **Database** Parameters (page 58)
    - **Oracle** Database **Parameters** (page 59)

14. The installer verifies the parameters. If there are:

    - No errors, a verification screen appears.
    - Errors, the cause (as nearly as the installer can determine) is shown. If you entered incorrect data, go **Back** and make corrections, or **Cancel** the installation, address the causes, and restart the installation.

15. Specify your NMS hub configuration information.

    For details, refer to **Hub Configuration Values** (see page 59).

16. Specify a network mask or IP address range that you want NMS to discover, and a range of IP addresses to exclude if necessary.

    Note: If no entries are made, discovery is skipped.

17. Select the methods you want NMS to use to obtain information, then enter the authentication credentials under each selected method.

    - **WMI—**domain, user and password
    - **SNMP**—community string, this is often *public* (the default)
    - **ssh**— User name and password for a user with administrative privileges on your UNIX®-based computers

    Note: You can add additional credentials later with the Remote Administration utility or NIS Manager.

18. Select the **Service Catalogs**. Devices discovered on the network are grouped into these catalogs by pre-defined filters.

    - Windows Servers
    - UNIX®-based Servers
    - Network Printers
    - Network Devices
    - Auto Configure Managed Systems only: This option selects a pre-defined configuration profile that is used for all computer systems manually set to *Managed* state in Remote Administrator or NIS Manager.If *not* selected, the pre-defined profile is used for all computer systems, independent of the state set in Remote Administrator or NIS Manager.

    Note: Use Remote Administrator or NIS Manager to make catalog changes later or modify the filters, which can filter on a number of parameters, such as IP-range or OS.

19. Review the pre-installation summary. If the information is not correct, click **Previous** to return to previous screens and make the corrections.

20. Click **Install** to begin the file extraction. A progress bar shows process status.

21. When extraction is complete, the **Ready for post configuration** screen displays. Click **Continue**. Post configuration can take several minutes.

22. The **Install Complete** window prompts you to restart the system to complete the installation. Click **Next**.

    Note: A warning that one or more probes did not activate before the installer finished executing does not necessarily represent an issue. Some probes might not finish their start up sequence before the installer displays its final screen.

23. Click **Done** to exit.

    Important: If you turned off any anti-virus scanners, turn them back on now.

Installation is complete. Go to **Chapter 4: Nimsoft Client Installation** (see page 65) to deploy and install Nimsoft infrastructure on client systems.

Installing NMS on Linux or Solaris with Console Mode

This procedure is intended for a first-time installation. If you want to:

- **Upgrade**, you must first disable package forwarding and clear the distsrv job queue (required) and remove customized probes in your probe archive (recommended). See the *NMS Release Notes and Upgrade Guide* for details.
- **Reinstall**, click **Cancel**, uninstall the prior version (see **Uninstalling NMS** on page 64), and restart the installation process. Note that your server configuration (domain and hub names, IP addresses, user accounts /passwords, etc.) is *not* retained.

Follow these steps.

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

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

2. Log in to the Nimsoft Customer Support Center site.
3. Download the most recent NMS install package for Linux or Solaris (the package is over 1 GB, so this could take several minutes).
4. Execute `chmod 755` on the install file to make it executable.
5. Run the installer. From a command line, execute:

   - **Linux**—installNMS_linux.bin -i console
   - **Solaris**—installNMS_solaris.bin -i console

   The installer unpacks the files (this could take several minutes) then displays the Introduction.

6. Specify a language.
7. Read the license agreement (optional).
8. Enter the path to the directory where you want NMS to be installed, or use the default path (**/opt/nimsoft**).
9. Specify whether you want to use an existing database or create a new one.
10. Specify the database type.
11. Specify the database server parameters.

    The parameters available depend on the database type and whether it is new or existing. All fields are case sensitive.

For details, refer to **GUI and Console Mode** (page 58).

12. The installer verifies the parameters for your database.

    a. If there are errors, the cause—as nearly as the installer can determine—is presented in the next dialog. Cancel the installation, address the reason for the errors, and restart the installation.

    b. If there are no errors, you get a verification screen.

13. Specify your NMS hub configuration information.

    For details, refer to **Hub** Configuration **Values** (see page 59).

14. Enter the authentication credentials for each method you want NMS to use to obtain information. Skip any that do not apply in your case.

    - **SNMP**—community string, this is often *public* (the default)
    - **WMI—**domain, user name and password
    - **ssh**—user name and password for a user with administrative privileges on your UNIX®-based computers

15. Enter the Service Catalogs to be created in the database. Devices discovered on the network are grouped into these catalogs by pre-defined filters.

    Note: Use Remote Administrator (or the NIS Manager) to make catalog changes later or modify the filters, which can filter on a number of parameters, such as IP-range, OS, etc.

    - Windows Servers
    - UNIX®-based Servers
    - Network Printers
    - Network Devices
    - Auto Configure Managed Systems only

      This option selects a pre-defined configuration profile that is used for all computer systems manually set to *Managed* state in Remote Administrator or the NIS Manager.

      If this option is *not* selected, the pre-defined configuration profile is used for all computer systems, independent of the state set in Remote Administrator (or the NIS Manager).

16. Review the pre-installation summary. If you need to make changes, go back to prior steps.

17. The installer unpacks the files and completes the installation. A progress bar shows the installation status.

    This process can take several minutes or more. To see the progress of the installation in detail, execute:

    ```
    tail -f /tmp/ia/iaoutput.txt
    ```

18. NMS launches. If it does not, execute:

    ```
    cd /etc/init.d
    nimbus start
    ```

Important: If you turned off any anti-virus scanners, turn them back on now.

Installation is complete. Go to **Chapter 4: Nimsoft Client Installation** (see page 65) to deploy and install Nimsoft infrastructure on client systems.

Installing NMS on Windows, Linux or Solaris with Silent Mode

Important: This procedure is intended for a first-time installation. To reinstall, you must first uninstall the existing software. Refer to **Uninstalling** (page 64) for details.

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

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

2. Log in to the Nimsoft Customer Support Center site.

3. Download the:

   - Most recent NMS install package for your operating system (the package is over 1 GB, so this could take several minutes)
   - Silent install template zip package

4. On Linux or Solaris, execute `chmod 755` on the install file to make it executable.

5. Prepare your response file:

   a. Extract the silent install templates.

   b. Locate the **installer.*database_type*.*OS*.properties** file that corresponds to your system setup, and save the file as **installer.properties** in the same directory as the installer.

   c. Open **installer.properties** and enter or change the parameter values. All lines that do not begin with a **#** symbol must have a value.

      For details, refer to Silent Install Parameter Values (see page 60).

   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).

6. Run the installer.

   - **Windows**—double-click **installNMS**
   - **Linux or Solaris**—execute either:

     ```
     installNMS_linux.bin -i silent
     installNMS_solaris.bin -i silent
     ```

7. 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
   ```

8. NMS launches. If for some reason it does not, enter these commands:

   - **Windows**—execute:

     ```
     net start NimbusWatcher Service
     ```

   - **Linux or Solaris**—execute either:

     ```
     cd /etc/init.d
     nimbus start
     ```

9. If you turned off any anti-virus scanners, turn them back on now.

Installation is complete. Go to **Chapter 4: Nimsoft Client Installation** (see page 65) to deploy and install Nimsoft infrastructure on client systems.

Server and Database Installation Parameters

GUI and Console Mode Parameter Values

MySQL Database Parameters

Parameter	Value
Database Server	Database server IP address
Database Name	Desired name (new) or actual name (existing)
Database Port	Database server port (typically 3306)
Database Administrator **Administrator Password**	Either: ▪ Use the MySQL administrative account (root). If you are creating a new database, enter the desired password for the root account to be created. ▪ Use an account other than root by checking **Nimsoft SLM Database User Account**. Enter the username and password for an existing account (new or existing database), or enter the desired name and password for an account to be set up (new database).

SQL Server Database Parameters

Parameter	Value
Database Server	▪ Database server hostname or IP address ▪ hostname\instance_name if you have a named instance on a standard port (i.e. 1433) ▪ hostname if you have a named instance on a **non**-standard port
Database Name	Desired name (new) or actual name (existing)
Database Port	Database server port (typically 1433)
Database User	Database administrative account (root)
Database Password	Password for database administrator account or desired password if the account is to be created

Oracle Database Parameters

Parameter	Value
Database Server	Database server IP address
Service Name	Desired database name (new) or actual name (existing)
Database Port	Database server port (typically 1521)
SYS Password	Password for the server system administrator account
Nimsoft DB User	Desired name for the Nimsoft database administrator account, which will be created by the installer
Nimsoft DB Password	Desired password for the Nimsoft database administrator
Tablespace Name	Desired name (new) or actual name (existing)
Tablespace Location	Desired location or leave blank to use the default (new)
Database Size	Desired size (new)
Auto Extend Size	Desired size or leave blank to use the default
Maximum Size	Desired size or leave blank to use the default

Hub Configuration Values

Parameter	Value
Hub Domain	Desired name for this NMS domain (default is the name of the server with **dom** appended).
Hub Name	Desired name for this hub (default is the name of the server with **hub** appended).
Password	Desired password (at least six characters) for your Nimsoft administrator. The name of this user is always administrator; the name and the password are required to log in to NMS after installation.
First Probe Port (optional)	Use the default (48000) and let the system assign ports as needed unless you have a reason to specify an initial port for Nimsoft probes.
License	The license key exactly as it appears on your Nimsoft License Document. (If you do not have a license, the installer creates a temporary trial license that will work for 30 days).
Select IP for Hub	The installer displays all network interfaces attached to the computer. Select the IP address you want to use for NMS traffic. **Note**: Unless you have a specific reason to do so, do not choose a Link Local address, which is an address that starts with 169.254 (IPv4) or fe80: (IPv6). A warning displays if you do. If you want to proceed using a Link Local address, click the Allow Link Local Address box.

Silent Install Parameter Values

For silent install, the following parameters must be defined in the installer.properties file. Note that some parameters:

- Are not required for certain platforms and/or operating systems. If a parameter is not included in **the installer.*DB_type_OS*.properties** file, it is not required.
- Require actual values if your database or required user accounts are already created.
- Require you to specify values if the database and/or accounts are to be created.

In the accepted values columns:

- **Bold** text represents actual accepted values that can be entered verbatim.
- Regular text represents values that exist and are specific to your setup, such as a server IP address .
- *Italic* text represents values you define during installation, such as the Nimsoft domain name.

Database Configuration Parameters

Parameter	Definition	Accepted Values
USER_INSTALL_DIR	Target folder for installed files	▪ **C\:\\Program Files\\Nimsoft** (Windows default) ▪ **/opt/nimsoft** (Linux/Solaris default) ▪ Existing directory ▪ *Directory to be created by installer*
NIMDBCREATE	Create database?	▪ **true** (default) ▪ **false**
NIMDBTYPE	Database Type	▪ **mysql**, **oracle** or **mssql** (defaults)
MSSQLAUTHTYPE	Microsoft SQL Authentication Type	▪ **sql** (default) ▪ **trusted**

Parameter	Definition	Accepted Values
DB_SERVER	Database server hostname or IP address	▪ Hostname or IP address On SQL server: ▪ hostname\instance_name if you have a named instance on a standard port (i.e. 1433) ▪ hostname if you have a named instance on a **non**-standard port
DB_PORT	Database port	▪ **3306** (MySQL default) ▪ **1521** (Oracle default) ▪ **1433** (MSSQ L default) ▪ User-specified port
NIMDBNAME	Database name	▪ **NimsoftSLM** (default) ▪ *Desired database name* (new database) ▪ Actual database name (existing database)
DB_ADMIN_USER	Nimsoft database administrator username	▪ **Sys** (required user for Oracle) ▪ DB admin username (MySQL and SQL server)
DB_ADMIN_PASSWORD	Database administrator password	▪ SYS password (Oracle) ▪ Actual DB admin password (MySQL and SQL server)
NIMDB_USER *Oracle: required* *MySQL: optional*	Nimsoft database user account	▪ **Nimsoft** (default for new DB; required on Oracle) ▪ **root** (optional for MySQL)
NIMDB_PASS *Oracle: required* *MySQL: optional*	Nimsoft database account password	▪ **SID** (Oracle)
DROP_COLUMNS (MySQL and Oracle)	Drop the *inserttime* column from the database schema	▪ **1** (drop columns, default) ▪ **2** (keep but do not create in new table) ▪ **3** (keep and create in new table)

Hub Configuration Parameters

Parameter	Definition	▪ Accepted Values
NMSHUB	Hostname or IP address for the Primary hub	▪ Hostname or IP address
NMSDOMAIN	NMS domain name	▪ Actual domain name (if it exists) ▪ *User-specified domain name* (if being created) ▪ <no value> (default domain name is the server name with **dom** appended)
NMSNETWORKIP	NMS Network Interface IP	▪ IP address of Primary Hub NIC
NMS_PROBE_PORT	NMS first probe port	▪ **48000** (default) ▪ Any available port ▪ <no value> (probe ports will be auto assigned)
IPV6_ENABLED=0	Enable IPV6	▪ **0** (false, default) ▪ **1** (true)
NMSLICENSE	Nimsoft License string	▪ License number
NMS_PASSWORD	Password created for NMS Administrator account	▪ User-specified
DISCOVERY_NET_1	Addresses to be included in discovery	▪ *Range of addresses* (can be a scope or range, ex: 18.4.135.0/24)
DISCOVERY_NET_2	Addresses to be excluded from discovery	▪ *Range of addresses* (can be a scope or range, ex: 18.4.135.0/24)
SRVCAT_WINSRV **SRVCAT_UNIXSRV** **SRVCAT_NETPRN** **SRVCAT_NETDEV**	Configure for Windows servers, UNIX servers, network printers or network devices	▪ true ▪ **false** (default) ▪
SRVCAT_AUTOMNG	Auto Configure Managed Systems only	▪ **true** (default) ▪ false

Parameter	Definition	▪ Accepted Values
SNMP authentication string parameters; leave blank if none		
SNMP_AUTH	SNMP community string; typically **public**	▪ String ▪ <blank>
WMI_AUTH_1	WMI Authentication Credentials (leave blank if none)	▪ windows domain
WMI_AUTH_2	WMI Authentication Credentials (leave blank if none)	▪ wmi domain user
WMI_PASS	WMI Authentication Credentials (leave blank if none)	▪ wmi password
Secure Shell (SSH) authentication string parameters; leave blank if none		
SSH_AUTH	SSH authentication credentials	▪ ssh user
SSH_PASS	SSH password	▪ ssh password

Uninstalling NMS

These are the only recommended methods to uninstall NMS.

Windows

1. Go to the Control Panel.
2. Choose **Programs and Features** (**Add/Remove Programs** on older versions of Windows).
3. Select each NMS component.
4. Click **Uninstall/Change**, then follow the system prompts.

Linux and Solaris

1. Run the uninstaller using this format:
2. Go to:
   <*NMS_install_dir*>/NM_Server_installation

   NMS_install_dir is the directory where NMS was installed (default is **/opt/nimsoft**).
3. Run the uninstaller:

   ```
   uninstall -i console
   ```

Important: The Nimsoft-provided uninstaller will succeed regardless of how NMS was installed, whether by the interface or by command line. No other uninstall approach is advised.

Chapter 4: Nimsoft Client Installation

This section explains how to install Nimsoft management tools and infrastructure components on client systems in your managed environment. It contains the following topics:

- **Overview** (page 65)
- **Windows Client Installation** (page 69)
- **Linux or Solaris Client Installation** (page 73)
- **Installing a Robot on an AS400 Computer** (page78)

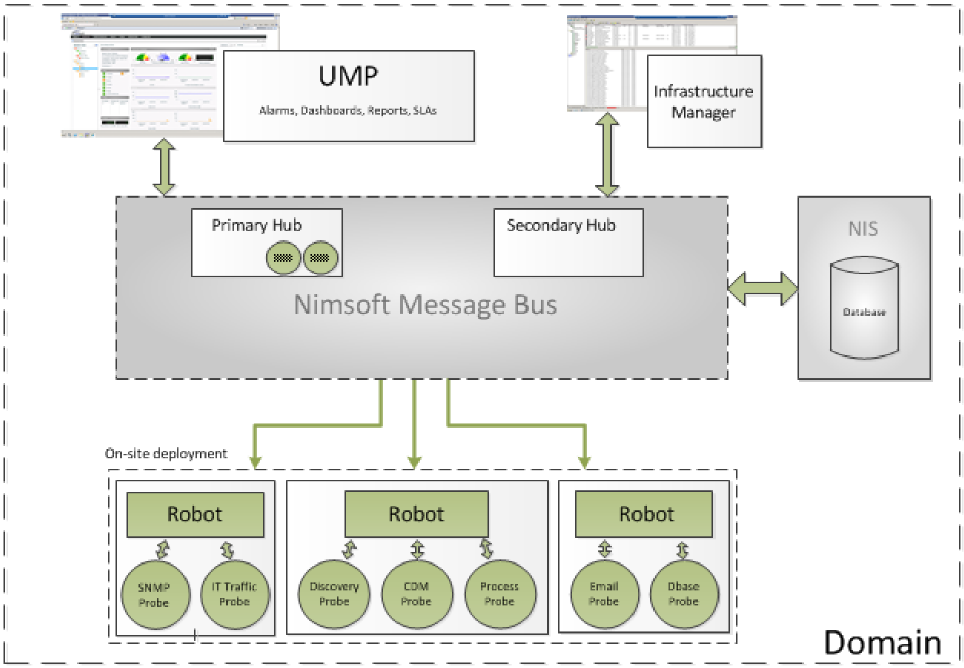
Overview

All software required by client systems resides on the NMS system. Various installation packages available on the NMS web page allow you to install the components of your choice.

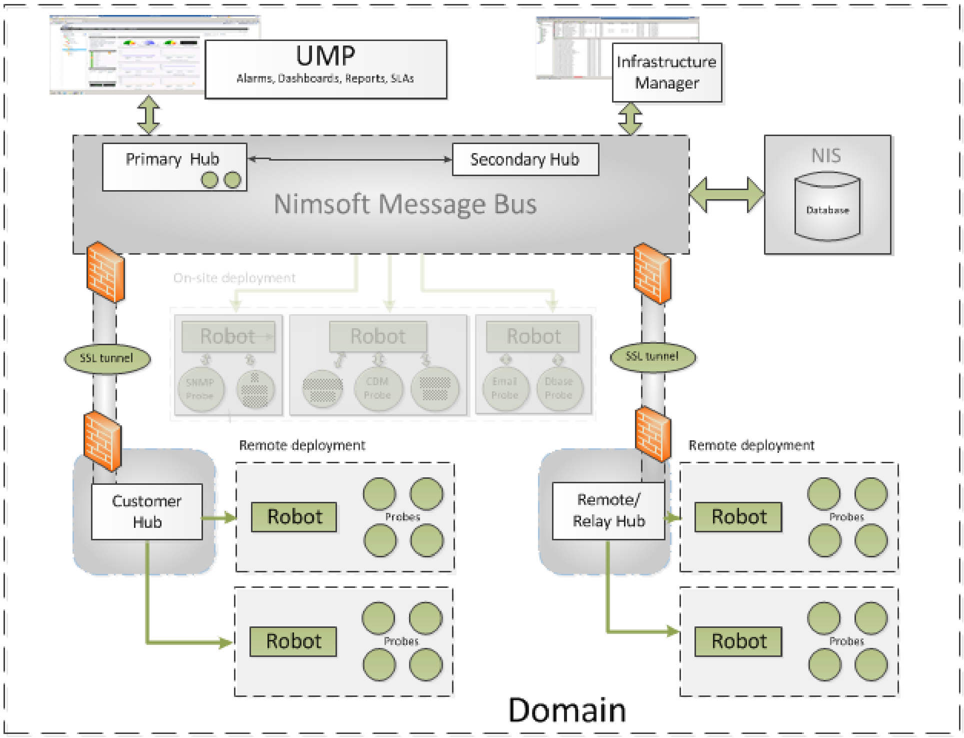
Client systems can be set up with either a *pull* or *push* deployment model.

- **Pull** – Administrators and users download the install packages from the NMS web page to the client system, then execute the install packages on the client systems. This model is explained in this chapter.
- **Push** – An administrator pushes the software from the NMS system to the individual clients and executes the installation remotely. For details, refer to **Appendix A: Bulk Robot Deployment with the Automated Deployment Engine (ADE)** on page 80.

The following illustration shows a robot and a variety of probes deployed from the NMS system to each of three computers within a managed Nimsoft domain.



If you are installing one or more hubs, robots, and probes) on remote sites, you may need to set up tunnels to enable secure communication. The DMZ wizard helps you set up tunnels between hubs.



Management Consoles

Management consoles let you manage your Nimsoft infrastructure and control and view the collected data. Four consoles are available.

The consoles can be installed on Windows systems.

- Unified Management Portal (UMP)

  UMP offers the most features. Functionality for older consoles (such as Enterprise Console) has been and will continue to be incorporated in UMP. For UMP Installation, see the *UMP Installation Guide* available from Nimsoft support.

- Infrastructure Manager (IM)

  This interface lets you configure the Nimsoft Infrastructure and view monitoring information for systems, applications and networks.

  Installation dependencies: IM can be installed and run stand-alone on any Windows-based computer that has network access to the Nimsoft hub.

- **Service Level Manager (SLM)**

  The Service Level Manager enables administrators to quickly define Service Level Agreements (SLAs) between the client and the service provider and to generate QoS reports.

  Installation dependencies: Service Level Manager can be installed and run stand-alone on any Windows-based computer that has network access to the Nimsoft hub.

Infrastructure Components

Nimsoft infrastructure refers to the hubs, robots, and probes that gather QoS and alarm information from your IT environment and direct this information to management consoles and the Alarm Console.

The following infrastructure installation packages are available:

- **Windows Robot, Hub, Distribution Server, Alarm Server**

  This package consists of all the infrastructure components you need to install and configure a Windows-based computer. The package also contains the DMZ wizard component, which sets up a tunnel between the firewall and the DMZ server.

- **Windows Robot**

  The Nimsoft robot controls and manages probes and provides a simple database service to spool and forward probe messages and alarms. The robot must be installed on all Windows systems where you want to distribute probes.

- **Nimsoft Infrastructure (nimldr) for all platforms**

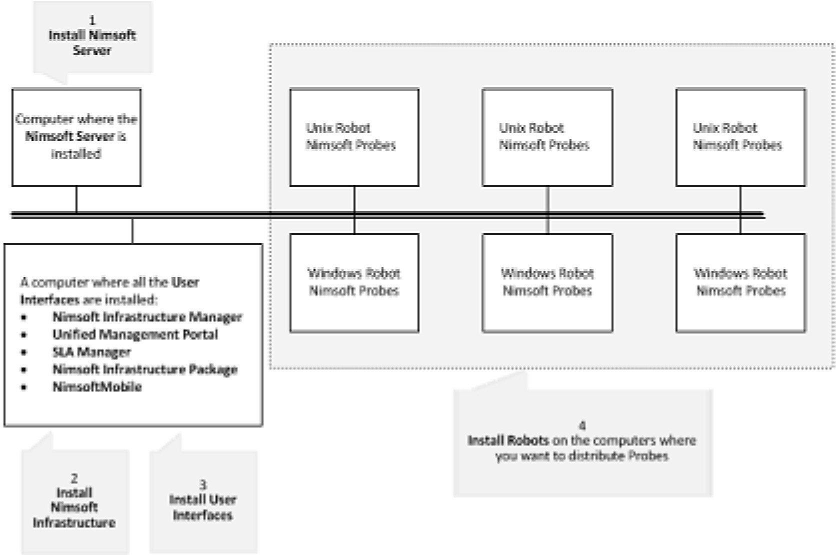
  The **nimldr** package contains the robot software for Linux and Solaris systems. The robot controls and manages probes and provides a simple database service to spool and forward probe messages and alarms. The robot must be installed on all Linux or Solaris systems where you want to distribute probes.

- **Web Service (wasp)**

  This service must be installed on any robot running the wasp probe . For more details about the wasp_web_service, refer to the **Archives** tab of Nimsoft Support Site (http://support.nimsoft.com/). This service replaces the legacy web service.

Typical Infrastructure Deployment

Steps 2 through 4 in the following illustration show a typical infrastructure component deployment**:**


1
Install Nimsoft Server
Computer where the Nimsoft Server is installed
Unix Robot
Nimsoft Probes
Unix Robot
Nimsoft Probes
Unix Robot
Nimsoft Probes
Windows Robot
Nimsoft Probes
Windows Robot
Nimsoft Probes
Windows Robot
Nimsoft Probes
A computer where all the User Interfaces are installed:
Nimsoft Infrastructure Manager
Unified Management Portal
SLA Manager
Nimsoft Infrastructure Package
NimsoftMobile
4
Install Robots on the computers where you want to distribute Probes
2
Install Nimsoft Infrastructure
3
Install User Interfaces

Note: In some cases, before you can distribute probes to local or remote computers, you may need to download the probe packages themselves from the Nimsoft Archive on the support site (www.nimsoft.com/support) to your computer. Some probes require additional licensing; see http://www.nimsoft.com/support/licence-updates for details.

Windows Client Installation

Installing a Management Console

1. On the client computer where you want to install a console, browse to your NMS web page (http://<*servername_or_server_IP_address*>:8008).

   Note: You must specify port 8008.

2. In the left pane, click **Client Installation**.
3. In the **User Interfaces** table, click a console installer, then select **Run**.
4. Follow the prompts to complete the installation. Note that:
   - If you are installing IM, you must select which components to install: Infrastructure Manager and/or Alarm SubConsole. Normally both should be installed.
   - If you choose to install the Microsoft SOAP Toolkit, the toolkit setup wizard launches.
5. Verify that the installation was successful by launching the console:
   - **Start > Programs > Nimsoft Monitoring > Infrastructure Manager**
   - **Start > Programs > Nimsoft Monitoring > Service Level Manager**

Installing a Windows Robot

When you install a robot you can choose **Normal** or **Cloud** installation.

Cloud installation lets administrators install a Nimsoft robot onto a master image of a virtual machine (VM) for provisioning purposes. This lets the administrator monitor new VMs as they are deployed.

Note: Cloud installation leaves the installed robot in a latent state. The robot starts after a configurable number of host restarts.

1. On the client computer where you want to install a robot, browse to your NMS web page:

   ```
   http://<server_name_or_IP_address>:8008
   ```

   Note: You must specify port 8008.

2. In the left pane, click **Client Installation**.
3. In the **Infrastructure** table, click **Windows Robot**, then select **Run**.
4. Follow the prompts to complete the installation. Note that:
   - For **Normal** installation, you must specify the domain you want the robot to be part of. Check a domain (if more than one is available) or select **Choose to connect to the network interface through IP address** to attach the robot to a specific hub.

- For **Cloud** installation, a hub on a cloud instance is assumed. If a hub external to the cloud is used, the robot must be configured with **robotip_alias** = <*external IP of cloud instance*> after the cloud instance is created.
- If the computer has multiple network interface cards (NICs), the **Local IP address** dialog appears. Select the network interface the robot will use to send and receive information.
- In the **Options** dialog:
  - Leave the **First probe port** field blank (recommended) to let the system will use default port numbers, or specify the first port to be used to start probes.
  - Select **Passive mode** if you want to set the hub as passive.

Installing Windows Robot, Hub and Distribution Server

This install package offers three types of installation: **automatic**, **custom** and **DMZ**.

Note: If Nimsoft software if found on the system, the installer allows you to either:

- **Remove** all components then restart the installation (recommended)
- Select **Upgrade/Reinstall** to overwrite existing components

Automatic Installation

Automatic installation searches for a hub. If a hub is:

- not found, then the robot, hub, and Distribution Server (distsrv) are installed
- found, only the robot only software is installed

Follow these steps.

1. On the client computer, browse to your NMS web page:

   `http://<server_name_or_IP_address>:8008`
2. In the left pane, click **Client Installation**.
3. In the Infrastructure table, click **Windows Robot, Hub, Distribution server, Alarm Server**, then select **Run**.
4. Follow the prompts to complete the installation. Note that:
   - Setup Type is Automatic.
   - If no hub is found, you must specify an existing domain name.
   - If you are setting up a hub, you must specify the desired hub name.

Custom Installation

Custom installation allows you to decide which Nimsoft components to install:

- Robot
- Hub (Nimsoft recommends you install at least two hubs on the same domain and network to ensure you have a backup of the user and security data stored on the Primary Hub)
- Distribution Server (distsrv)
- Probe Runtime libraries (needed to create your own probes)
- DMZ Wizard

Follow these steps.

1. On the client computer, browse to your NMS web page:

   `http://<server_name_or_IP_address>:8008`

2. In the left pane, click **Client Installation**.
3. In the Infrastructure table, click **Windows Robot, Hub, Distribution server, Alarm Server**, then select **Run**.
4. Follow the prompts to complete the installation. The information required depends on your system and the components selected.
   - If no hub is found, you must choose an existing domain. All available domains are shown.
   - If you are setting up a hub:
     - You must specify the desired hub name and enter the hub license number.
     - You will set up a hub user account (called the **Initial User**) for the hub. Specify a user name or use the default (administrator), and choose a password.
   - Unless you have a reason to specify the first probe port, leave the field blank to let the system assign ports automatically.
   - If you choose to install the DMZ wizard, refer to DMZ Installation (see page72) for details on required information.

DMZ Installation

DMZ installation:

- Lets you set up a secure communication tunnel between hubs separated by a firewall, DMZ or both.
- Consists of two parts: creating and configuring a tunnel *server*, then creating and configuring a tunnel *client*.
- Requires that you determine which hub will be the tunnel server and install this hub first, then set up the tunnel client.

This section explains how to set up tunnels during installation. To configure an existing hub for tunnels, use the Infrastructure Manager Hub Configuration utility.

1. On the client computer, browse to your NMS web page:

   `http://<server_name_or_IP_address>:8008`

   Note: You must specify port 8008.
2. In the left pane, click **Client Installation**.
3. In the Infrastructure table, click **Windows Robot, Hub, Distribution server, Alarm Server**, then select **Run**.
4. Follow the prompts to complete the installation. Note that:
   - When prompted to log in, use the Nimsoft hub administrator account you set up during this installation.
   - You must specify an *existing* domain name.
   - You must specify the *desired* hub name. The hub must have a public IP address if you want to access it from the Internet.
   - For a **DMZ tunnel server**:
     - You will set up a hub user account (called the **Initial User**) for the hub. Specify a user name or use the default (administrator), and choose a password.
     - When prompted to log in, enter the hub user name and password.
     - In the **Setting up Tunnel Server** dialog, you create an authentication password. This password is required when you set up the tunnel client.
     - In the **Generating Client Certificate** dialog, enter the IP address of the client for which you want to generate the certificate.
     - Copy the certificate to removable media. You will need it when you set up the client.
   - For a DMZ tunnel client:
     - Enter the IP of the tunnel server, the server port, and the password created during tunnel server setup.
     - **Browse** for the certificate file. When the file is found, the certificate text displays.

Linux or Solaris Client Installation

All Linux or Solaris client installations use the Nimsoft Loader utility (**nimldr**). Utility options let you set up:

- **Robots**, which includes the robot and basic service probes.
- **Hubs**, which includes a hub, robots, service probes and the Distribution Server (**distsrv**).

  Nimsoft recommends you install at least two Nimsoft hubs on the same domain and network to ensure you have a backup of the user and security data in the event the primary hubs fails.
- **Tunnel server hubs** and **tunnel client hubs**, which allow secure communication in environments with firewalls or a DMZ.
  - To learn more about Nimsoft SSL tunnels and required ports, refer to **Working with Firewalls and DMZs** (see page 11)
  - Required Ports for SSL Tunnels (see page 12)

Note: If NM server is already installed and running on the system:

- Turn off all NMS processes:

  ```
  /opt/Nimsoft/bin/niminit stop
  ```
- Remove the robot:

  ```
  /opt/Nimsoft/bin/inst_init.sh remove
  ```

Installing Infrastructure with the Nimsoft Loader (nimldr)

Follow these steps.

1. On the client computer, browse to your NMS web page:

   ```
   http://<server_name_or_IP_address>:8008
   ```

   Note: You must specify port 8008.
2. In the left pane, click **Client Installation**.
3. In the Infrastructure table, click **UNIX installation utility (nimldr) for all platforms**, then **Save** the file.

   Note: If the client system doesn't have a browser, download the installer to a Windows computer and copy it to the client. Make sure the file is named nimldr.tar.Z.
4. Uncompress **nimldr.tar.Z**.
5. Extract the tar file :

   ```
   # tar xf nimldr.tar
   ```

   This creates a directory with sub-directories that contain nimldr installers for various Linux and Solaris platforms.
6. Enter the appropriate sub-directory for your platform (for example, **LINUX_23_64**).

7. If the client is on the:
   - Same network segment as the NM server, execute:

     ```
     # ./nimldr
     ```

   - Different network segment ,execute:

     ```
     # ./nimldr -I <NM_server_IP_address>
     ```

8. The install program guides you through the installation by asking a series of questions, which are detailed in Questions and Answers for the nimldr Installer (see page 74).

   Installation progress is logged in the **nimldr.log** file located where nimldr stores temporary files (**typically opt/nimsoft/tmp**). To view it, execute:

   ```
   tail -f /opt/nimsoft/tmp/nimldr.log
   ```

Questions and Answers for the nimldr Installer

The following table lists the questions asked by the installer. Note that:

- Default answers are in brackets. Press **Enter** to use the default, or type in the requested information.
- Not all questions are asked; some questions are asked or not depending on your answers to previous questions.
- Answers in *italics* represent values that do not exist but will be created by the installer.
- If express installation is specified, default values are used automatically.
- Additional questions for tunnel server and tunnel client setup follow this table.

Question	Answer
Where should nimldr store temporary files?	▪ opt/nimsoft/tmp (default) ▪ Directory of your choice
Is this a Cloud installation?	▪ Yes (cloud install) ▪ No (all other installs)
Do we have the installation file locally?	▪ Yes ▪ No
Where do we have the installation file(s)?	▪ Path to installation file(s)
Is there a host running a Nimsoft hub we can query for the installation file?	▪ Yes ▪ No
What is the IP address of the host running a Nimsoft hub?	▪ Hub IP address
What is the Nimsoft Domain called?	▪ Domain name (if it exists) ▪ *Desired name* (if it is being created) ▪ ***** (asterisk) to search for domains

Question	Answer
What is the Nimsoft hub called?	▪ Hub name (if it exists) ▪ *Desired name* (if it is being created) ▪ ***** to search for hubs
What is the installation file called?	▪ install_*platform*
Which of these archives would you like to connect to?	▪ Specify archive
Enter Nimsoft username and password.	▪ Name/password of the Nimsoft account set up during NMS installation ▪ administrator (typically)
Where do we have the installation files?	▪ Install file directory (if local)
What are we installing?	▪ **1** (robot only) ▪ **2** (robot and hub, tunnel server, or tunnel client)
Would you like to install the Distribution Server (distsrv)?	▪ Yes ▪ No ***distsrv** is the Nimsoft probe archive*
Where should the Nimsoft software be installed?	▪ /opt/nimsoft (default)
Automatically unregister robot from hub on termination?	▪ Yes ▪ No (default)
Should this robot run in passive mode?	▪ Yes (default, hub requests data from robot) ▪ No (robot sends data to hub)
What is this Nimsoft Domain called?	▪ Existing domain set up during NMS installation
Which Nimsoft hub should this robot connect to?	▪ Hub name
What is this Nimsoft hub called?	▪ Hub name
What is that Nimsoft hub's IP address?	▪ IP address
Are you setting up a tunnel between this hub and another hub?	▪ Yes ▪ No
Would you like to initialize the security settings on this hub?	▪ Yes (default) ▪ No
Please specify the administrator user password.	▪ Password for Nimsoft account set up during NMS installation
Are you setting up a Nimsoft tunnel between this hub and another hub?	▪ Yes ▪ No

Tunnel Server Installation Questions

Question	Answer
Enter Nimsoft username and password.	▪ Username and password for Nimsoft administrator account set up during NMS installation
Is this hub going to be a tunnel server?	▪ Yes
The following values are used to create the tunnel client certificate, which the tunnel client needs to connect to the tunnel server.	
What is the name of your organization?	▪ Company name
What is the name of the organizational unit?	▪ Organizational unit
What is the administrator email address?	▪ Nimsoft administrator account address
What password should we use for the Server certificate?	▪ Password you specify for tunnel client certificate ▪ **Note**: you need this password when you set up the tunnel client
What is the IP address of the tunnel client?	▪ IP address of the system on which you will install the tunnel client
What file should the certificate be written to?	▪ /opt/nimsoft/client.txt (default) ▪ Path and *filename* for client certificate
What is the IP address of the tunnel server hub?	▪ Tunnel server hub IP address

Tunnel Client Installation Questions

Question	Answer
Is this hub going to be a tunnel server?	▪ No
Is this hub going to be a tunnel client?	▪ Yes
What is the IP address of the tunnel server hub?	▪ Tunnel server hub IP address
What port is the server listening on?	▪ Port number assigned during NMS installation; typically 48000 (default)
What password was used to generate this certificate?	▪ Password defined when tunnel client certificate was created during tunnel server setup
What file is the client certificate in?	▪ Path and filename for client certificate that was copied from the tunnel server to the tunnel client

Flags for nimldr Installer

The following flags can be used to modify how the installer runs or to specify specific information.

Usage	Flag	Description
All installations	-d	Debug level , 0 (default)-5
	-l	Installation logfile
	-t	Location for temporary files during installation; default is /opt/nimsoft/tmp
	-D	NimBUS domain name
	-H	NimBUS hub name
	-N	Override robot name
	-p	NimBUS installation path; default is /opt/nimsoft
	-f	Override package file name; default installation file is detected by the program **Note**: Case sensitive, omit .zip extension
	-u	Install as current user, not as root (NOT recommended)
	-o	First probe port
	-R	IP address for this robot (useful for systems with multiple network cards)
	-a	set the automatic unregister flag; default is **no**
	-s	Set the robot to passive mode
	-v	prints version of ./nimldr
	-h	prints this help text
Installation file is on local system	-F	Directory containing installation file (if installation file is on local system)
Installation file is on a NimBUS Distribution Server	-I	IP address of NimBUS hub running a Distribution Server (note that this overrides the -H flag)
	-V	Package version (gets the specified version of the package, not the latest one)
Installation modes	-r	Install robot only (default)
	-i	Install Infrastructure (robot, hub and distsrv)
	-E	Express installation (uses defaults or supplied flags; requires that install file is on local system)
	-X	Silent express installation (fails instead of going to interactive mode; requires that install file is on local system)
Cloud installation	-C	Cumber of restarts until robot should become active
	-M	DNS name of the system running the hub

Installing a Robot on an AS400 Computer

Follow these steps.

1. Download the install files:

   a. On the AS400 client system or any other Nimsoft client, browse to your NMS web page:

   ```
   http://<server_name_or_IP_address>:8008
   ```

   b. In the left pane, click **Client Installation**.

   c. In the **Infrastructure** table, click:

   ■ **iSeries Robot Program Files** and **Save** the file (**nimBUS.savf**).
   This file contains the program files.

   ■ **iSeries Robot File Structure**, then **Save** the file (**nimsoft.savf**).This file contains the file structure and configuration files.

   d. If you are using a client that is not the target AS400, copy the files to the AS400.

2. On the AS400, create the NIMBUS user:

   ```
   CRTUSRPRF USRPRF(NIMBUS) PASSWORD()
   USRCLS(*SECOFR) TEXT('Nimbus User for Nimsoft Management')
   ```

3. Create temporary files for the save files:

   ```
   CRTSAVF <LIBRARY>/NIMBUS TEXT('Savf of Nimsoft LIB')
   CRTSAVF <LIBRARY>/NIMSOFT TEXT('Savf of Nimbus_Software')
   ```

4. Execute:

   ```
   LCD <workstation folder containing savefiles>
   CD <LIBRARY on AS400 containing temporary save files>
   BIN
   PUT NIMBUS.savf
   PUT NIMSOFT.savf
   Quit
   ```

5. Install the robot.

   a. Restore /qsys.lib/Nimbus.lib. Execute:

   ```
   RSTLIB SAVLIB(NIMBUS) DEV(*SAVF) SAVF(<<LIBRARY>>/NIMBUS)
   ```

   b. Restore /Nimbus_Software/NimBUS file-tree. Execute:

   ```
   QSYS/CRTDIR DIR('/Nimbus_Software')
   QSYS/CRTDIR DIR('/Nimbus_Software/NimBUS/')
   QSYS/RST DEV('/QSYS.lib/<<LIBRARY>>.lib/NIMSOFT.file')
   OBJ(('/Nimbus_Software/NimBUS/*'))
   ```

6. Edit the **/Nimbus_Software/NimBUS/robot.cfg** configuration parameters with appropriate values as shown below. The file follows this format:

   ```
   EDTF STMF('/Nimbus_Software/NimBUS/robot/robot.cfg')
   <controller>
       domain = Nimsoft
       hub = Development
       hubrobotname = src1
       hubip = 10.0.0.10
       robotname = server3
       robotip = 10.0.0.11
   </controller>
   <remote>
       contip = 10.0.0.11
   </remote>
   ```

Parameter	Value
domain	Nimsoft domain name
hub	Name of the hub to which the robot will connect
hubrobotname	Name of the robot to install
hubip	Hub IP address
robotname	Intended name for the robot on the target system
robotip	Target system IP address
contip	Target system IP address

7. To start the robot, execute:

   ```
   STRSBS NIMBUS/NIMBUS
   ```

Notes:

- To stop the robot, execute:

  ```
  ENDSBS NIMBUS
  ```

- If you want to shut down the /tcpip system each night for backup, you should also stop Nimsoft and start it again after tcpip has been restarted.

  Stopping and starting Nimsoft can be done in **jobscde** as described in the example below (which has stop time 01.00.00 and start time 07.00.00 every day):

  ```
  ADDJOBSCDE JOB(ENDNIMSOFT) CMD(ENDSBS SBS(NIMBUS) DELAY(120))
  FRQ(*WEEKLY) SCDDATE(*NONE) SCDDAY(*ALL) SCDTIME('01.00.00')
  USER(NIMBUS) TEXT('End Nimsoft')
  ADDJOBSCDE JOB(STRNIMSOFT) CMD(STRSBS SBSD(NIMBUS/NIMBUS))
  FRQ(*WEEKLY) SCDDATE(*NONE) SCDDAY(*ALL) SCDTIME('07.00.00')
  USER(NIMBUS) TEXT('Str Nimsoft')
  ```

- If you want to change the schedules, use **WRKJOBSCDE**.

Appendix A: Bulk Robot Deployment with the Automated Deployment Engine (ADE)

Introduction

Nimsoft Monitor administrators who want to deploy Robots in bulk to multiple remote computers and virtual machines have the following options:

- Use the Automated Deployment Engine (ADE) with its graphical user interface. See **Using ADE in GUI Mode** (page 82) for details.
- Use the Automated Deployment Engine with its command-line interface (XML-based deployment). See **Using the ADE Command Line Interface** (page 86) for details.
- Use the robot_msi_rpm robot installer packages with a third-party deployment tool of choice. See **Deploying Robots with a Third-Party Mechanism** (page 88) for more information.

Nimsoft ADE provides a *push* alternative to the standard *pull* robot distribution method:

- **Push**—With ADE, robot software from the *source* system (the NMS system or a hub) is deployed silently and simultaneously to multiple target systems.
- **Pull**—With standard client installation, a user on a client system accesses the NMS system and downloads the software to the client system. This is explained in **Chapter 4: Nimsoft Client Installation** on page 65.

The Nimsoft ADE probe is installed and activated by default when NM Server is installed or upgraded to the latest version.

Prerequisites for ADE

Before using ADE, ensure that:

- Your source system's NMS Archive has the required archive package robot_msi_rpm.zip, which includes both MSI and RPM robot installers. Nimsoft recommends you run ADE from the primary hub, which by default, will have this archive package installed and available.
- Your target systems are supported. ADE is supported on Windows and Linux. For details, see the Nimsoft Compatibility Support Matrix, which is updated regularly.

- You have the required software components on the source and target systems:

Windows	Linux
▪ .NET 2.0 runtime library (or higher) is required for the ADE GUI and MSI robot installer packages ▪ WMI and DCOM are configured and running, as are the services WMI requires: – COM+ Event System – COM+ System Application – Remote Procedure Call (RPC) – Remote Procedure Call (RPC) Locator – Remote Registry – Server – Windows Management Instrumentation ▪ Microsoft Visual Studio C++ 2008 redistributable runtime library (or SP1); download **vcredist_x86.exe** (32-bit) or **vcredist_x64.exe** (64-bit) from www.microsoft.com ▪ Nimsoft Robot installed on the machine on which the ADE GUI will run	▪ **/bin/sh** (symlink to bash; /bin/bash must be installed, note that any shell can be run) ▪ **glibc**

- All appropriate firewall ports are configured to allow remote WMI and DCOM connections, as well as Windows shares (refer to Microsoft documentation for details).
- Source system and target systems are in the same Windows domain, unless target systems are in the default Windows domain **workgroup** (see Note below).

  Note: Redhat Linux provides a native authentication tool that allows a Linux system to join a Windows domain.

  Note: You can deploy to systems in the default Windows domain, **workgroup**, from any Linux or Windows system provided the hostname is specified in this format: **[workgroup]\[hostname]**.

- You have appropriate privileges.

  Windows:

  - If you are using Windows Native Deployment, you must have local administrative privileges on the target systems.
  - The user listed in the host-profiles.xml for target Windows systems must have remote access and remote execution privileges. It is recommended that this user be an administrator.

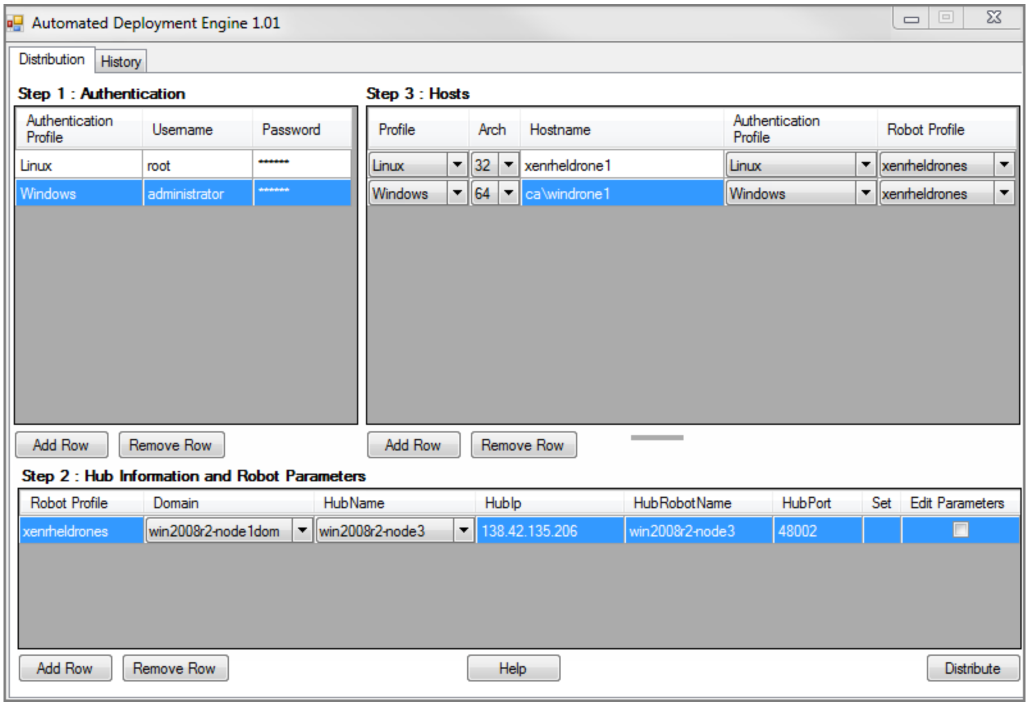
  Linux: root

Using ADE in GUI Mode

Overview

The Automated Deployment Engine (ADE) **GUI** lets you set up and specify parameters for a distribution request. ADE executes the distribution request according to the source and target information you specify in three tables:

- **Authentication**, which lets you specify login information for targets
- **Hub Information and Robot Parameters**, which lets you specify robot parameters
- **Hosts**, which lets you specify the targets to which the robots will be deployed



Step 1 : Authentication

Authentication Profile	Username	Password
Linux	root	*******
Windows	administrator	*******

Step 3 : Hosts

Profile	Arch	Hostname	Authentication Profile	Robot Profile
Linux	32	xenrheldrone1	Linux	xenrheldrones
Windows	64	ca\windrone1	Windows	xenrheldrones

Step 2 : Hub Information and Robot Parameters

Robot Profile	Domain	HubName	HubIp	HubRobotName	HubPort	Set	Edit Parameters
xenrheldrones	win2008r2-node1dom	win2008r2-node3	138.42.135.206	win2008r2-node3	48002		□

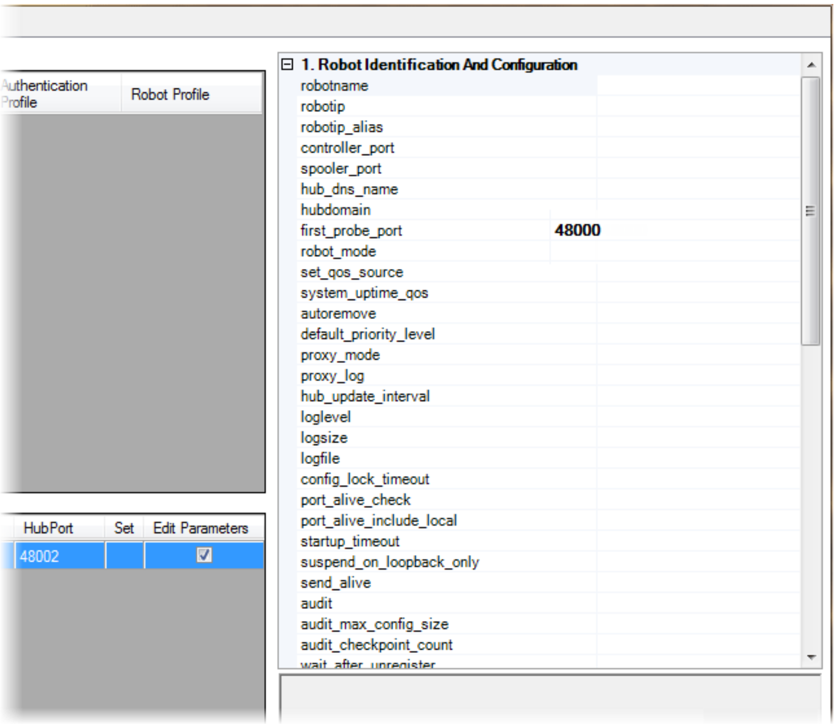
Deployment Steps

Important: The GUI does not save the information you enter to a persistent file. If the GUI closes for any reason before your distribution request is finished, the information you entered is lost.

1. Open the ADE probe GUI (double-click the **automated deployment engine** probe in Infrastructure Manger) and enter the desired deployment information.

   - **Authentication**—Create a profile for an admin account for the target systems. A profile can be assigned to one or more target systems that have a username and password in common. See **Authentication Parameters** (page 84) for details.
   - **Hub Information and Robot**—Specify details about the robot and its hub. See **Hub Information and Robot Parameters** (page 84) for details.

     Click in the check box for **Edit Parameters** to activate a grid that lets you view and set additional parameters. Select a parameter in the grid to see its description and default value.



uthentication Profile	Robot Profile

HubPort	Set	Edit Parameters
48002		☑

⊟ 1. Robot Identification And Configuration

robotname	
robotip	
robotip_alias	
controller_port	
spooler_port	
hub_dns_name	
hubdomain	
first_probe_port	48000
robot_mode	
set_qos_source	
system_uptime_qos	
autoremove	
default_priority_level	
proxy_mode	
proxy_log	
hub_update_interval	
loglevel	
logsize	
logfile	
config_lock_timeout	
port_alive_check	
port_alive_include_local	
startup_timeout	
suspend_on_loopback_only	
send_alive	
audit	
audit_max_config_size	
audit_checkpoint_count	
wait_after_unregister	

     If a value is not listed to the right of a parameter, the default value for that parameter will be assigned when the remote robot starts.

   - **Hosts**—For each target, specify system details, choose an authentication profile, and choose a robot profile. See **Hosts Parameters** (page 85) for details.

2. Review the values you have entered and enter any missing information. Press **Enter** to instantiate the last value, exit edit mode, and activate the **Distribute** button.
3. Click **Distribute** to start deployment.

   The GUI will automatically switch to the **History** tab and display the real-time distribution status for each host. Each entry contains:

   − **JobID** is a numeric identifier for the distribution

   − **Status** of the current job (QUEUED, IN_PROGRESS, SUCCESS, FAILURE, COMPLETED, ALREADY_IN_PROGRESS, NO_ACTION)

   − **Host** name or IP address of the target system

   − **Description** of the status, including error messages (if applicable)

   Click **Clear** to clear the progress status. If the distribution information is needed again, it is available in the probe log file **ade_history.log**.

Note: ADE installs robots in groups, where group size is a function of the number of CPU cores on the hub where the ADE probe is running.

Note: After installing a robot, ADE waits sixty seconds (default) for the robot to start before reporting its status in the history tab. To change the default length of time, change the value for **verifyDelay** in the ADE probe config file **automated_deployment_engine.cfg**.

Parameter Values

Authentication Parameters

Parameter	Definition	Value
Authentication Profile	Name for this set of account information	▪ Unique ID of your choice
Username	Account username	▪ Any account on the target that has administrative permissions
Password	Account password of the associated username	▪ Password

Hub Information and Robot Parameters

Parameter	Definition	Value
Robot Profile	Name for this set of hub/robot information	▪ Unique ID of your choice
Domain	Nimsoft domain	▪ Select from list of available domains visible to the local ADE
HubName	Name of the hub this robot is associated with	▪ Select from list of available hubs within the selected domain

Parameter	Definition	Value
HubIP	IP address associated with the Hub	▪ Prefilled with the IP address of the Hub
HubRobotName	Name of the robot on the distributing hub	▪ Prefilled with the name of the robot on the distributing hub
HubPort	Port that the hub listens on	▪ Port specified during hub setup ▪ **48002** (default)
Set	Indicates whether or not one or more extended parameters for the robot have been defined or modified from the default	▪ <blank> —Not modified (from default values) ▪ **Y**—extended parameters have been modified (recommendation: review these before distribution)
Edit Parameters	Displays the extended robot property grid, which has optional parameters for: ▪ Robot Identification and Configuration ▪ Alarm Configuration ▪ Failover Configuration ▪ Message Enhancements	▪ Checked (displays grid) ▪ Unchecked (hides grid) **Note:** A description and default value for the selected parameter displays below the grid.

Hosts Parameters

Parameter	Definition	Value
Profile	Operating system on target system	▪ Windows ▪ Linux
Arch	Architecture of target operating system	▪ 32-bit ▪ 64-bit
Hostname	Target system name	▪ Hostname or IP address
Authentication Profile	Login information	▪ Select from list of profiles defined in the Authentication table (see Note below)
Robot Profile	Robot/hub information	▪ Select from list of profiles defined in the Hub Information and Robot Parameters table (see Note below).
Note: The GUI displays a warning if an attempt is made to change the name of either an authentication or robot profile while it is associated with a host.		

Using the ADE Command Line Interface

Command line mode lets you specify parameters in an XML file (**host-profiles.xml**). ADE then uses this file to direct robot deployment.

The command line interface:

- Supports Public key authentication for SSH. The XML field that defines the path to the public key is on the hub machine at:

  ```
  <rsakeyfile>/path/to/public_key_file</rsakeyfile>
  ```

- Allows use of ADE on Linux systems where no windowing environment is required.

Follow these steps.

1. Create a **host-profiles.xml** file to specify the hosts on which to install robots and the information for the hub with which the robot will connect. The format for host-profiles.xml is described in the example and table below.

   Note: Windows Hostname must be in the form *domain\hostname* when entered in the host-profiles.xml file. If a host is specified in an invalid format, deployment to that host is skipped to prevent issues with deployment to that host.

2. Copy the host-profiles.xml file into the ADE probe directory. By default this is:

   - Windows:
     <***nimsoft_home_directory*>\probes\service\automated_deployment_engine**
   - Linux:
     <*nimsoft_home_directory*>/probes/service/automated_deployment_engine

   Note: The <nimsoft home directory> is, by default:

   - Windows – **C:\Program Files\Nimsoft**
   - Linux – **/opt/nimsoft**

3. Deployment begins automatically--the ADE probe service/daemon scans the probe directory every thirty seconds and starts the deployment whenever a **host-profiles.xml** file is detected.

4. Following deployment (regardless of success or failure), the **host-profiles.xml** file is renamed **host-profiles-*YYYY-MM-DD_HH-mm-ss*** to reflect the date and time of deployment.

   This ensures that in the event the ADE probe restarts, deployment does not automatically restart. If you want to restart distribution, the ADE service/daemon will deploy using the same file if you (a) manually rename the file back to **host-profiles.xml**, and (b) change its size by a nominal amount (edit the file and add an additional line.) Deployment will restart with the next scan of the probe directory by the ADE service/daemon.

Deployment status is stored in **ade_history.log** in the ADE probe directory. View the status with **tail** (Linux and Solaris) or a similar utility in Windows. For example:

```
tail -f ade_history.log
```

You can also tail **automated_deployment_engine.log** for additional detail.

Example host-profiles.xml File

```
<!-- profile | hostname:port | username | password | domain | hubip | hubname |
hubrobotname | hubport  -->
<!-- default port is 22  -->
  <hosts>
    <host>
                <profile>Linux</profile>
                <arch>64</arch>
                <hostname>172.19.8.81</hostname>
                <username>root</username>
                <password>password</password>
                <domain>mcanji-W2K8-2dom</domain>
                <hubip>172.19.8.8</hubip>
                <hubname>mcanji-W2K8-2hub</hubname>
                <hubrobotname>mcanji-w2k8-2</hubrobotname>
                <hubport>48002</hubport>
    </host>
    <host>
                <profile>Windows</profile>
                <arch>32</arch>
                <hostname>workgroup\172.19.8.34</hostname>
                <username>Administrator</username>
                <password>password</password>
                <domain>mcanji-W2K8-2dom</domain>
                <hubip>172.19.8.8</hubip>
                <hubname>mcanji-W2K8-2hub</hubname>
                <hubrobotname>mcanji-w2k8-2</hubrobotname>
                <hubport>48002</hubport>
    </host>
  </hosts>
```

Parameter Values for host-profiles.xml

Parameter	Definition	Value
profile	Operating system on target system	▪ Windows ▪ Linux
arch	Architecture of target operating system	▪ 32 ▪ 64
hostname	Target system name	▪ Hostname or IP address
username	Admin account on target system	▪ Any account on the target that has administrative permissions
password	Admin account password	▪ Password string
domain	Nimsoft domain	▪ Nimsoft domain name (respect case)
hubip	IP address of the hub to which this robot will belong	▪ IP address
hubname	Name of the hub to which this robot will belong	▪ Hub name
hubrobotname	Name of the robot to be deployed	▪ Name of the robot on the distributing hub (respect case)
hubport	Port that the hub listens on	▪ 48002 (default) ▪ Port specified during hub setup

Deploying Robots with a Third-Party Mechanism

Overview

Many IT environments already have a mass software deployment mechanism in place. Some examples are Puppet and Yum (Linux), Altiris (Windows), or Microsoft System Center Configuration Manager (Windows). Almost any third-party distribution mechanism can be used as long as it can:

- Copy an **msi** or **rpm** robot installer to remote systems
- Copy an answer file (in the format specified below)
- Execute the installer

There are a total of four **robot_msi_rpm** installers:

- Two Windows installers: one 32-bit and one 64-bit Microsoft Installer (MSI) package
- Two Linux (SUSE and RedHat) installers: one 32-bit and one 64-bit RPM (RedHat Package Manager) package

Note: The msi and rpm installers are designed to execute silently and require an answer file. For manual installation of a robot without need for an answer file, see **Chapter 4: Nimsoft Client Installation** on page 65.

Deployment Steps

1. On the computer that will distribute robots (the *source* system), download the desired **robot_msi_rpm** package from either the:

   - Client Installation page on the NMS web page (http://<*nm_server*>:8008)
   - NMS file system:
     - **Windows**: C:\Program Files (x86)\Nimsoft\install\setup
     - **Linux**: /opt/nimsoft/install/setup

2. Prepare the answer file named **nms-robot-vars.cfg**. The file follows this syntax and format:

```
domain = <name of the domain that the robot belongs to>
hub = <primary hub name>
hubip = <primary hub IP address>
hubrobotname = <robot name of the primary hub>
hubport = <port number of the primary hub; default is 48002>
(optional fields)
```

   Note that:

   - All text within brackets must be replaced with actual values.
   - Optional parameters with no answer are valid. However, it is better to omit a parameter from the answer file rather than include it with an empty setting.

   The following table provides examples of the required values and three options.

Parameter	Definition	Example value
domain	Nimsoft Domain	HOST_ABC_DOM
hub	Nimsoft name of the hub to which the robot will be assigned	HOST_ABC_HUB
hubip	Hostname or IP address of the hub to which this robot will belong	10.0.0.10
hubrobotname	Name of the robot to be deployed	HOST_ABC_HUB
hubport	Port that the hub listens on	48002
Robotip *optional*	Hostname or IP address of the target system	10.0.0.10
Robotname *optional*	Desired name for robot on target (default is the hub IP)	HOST_ABC
first_probe_port *optional*	Port on source system to be used by the first probe	48000

   Note: For a full description of all robot configuration parameters, refer to the online help in the Controller probe GUI.

3. Copy the answer file to a directory on the target system.

   - **Windows** : same directory as the package
   - **Linux**: `/opt` (even if installing the robot to a non-standard directory)

4. Execute the appropriate command:

   - **Windows**

     ```
     msiexec /i <MSI _package> /qn
     ```

     To specify the target directory, execute:

     ```
     Msiexec /I <MSI_package> /qn TARGETDIR="path"
     ```

     You also can omit **qn** (silent mode) to display a simple GUI (interactive mode) where you can specify the target directory.

   - **Linux**

     ```
     rpm -ivh <RPM_package>
     ```

     To specify the target directory, execute:

     ```
     rpm -ivh nimsoft-robot.<arch>.rpm --prefix=<directory >
     ```

     where:

     `<arch>` is the architecture of the target system (**x86** or **x86_64**)

     `<directory>` is the path/name of the target directory

     The **rpm** flags function as follows:

     -i Installs the software package

     -v Displays a simple status line to show what is being installed (*verbose* mode)

     -h Displays fifty hash marks (**#**) to show the status as the install proceeds; when all fifty have displayed, the install is complete

   Tip: To view detailed status and progress as the deployment progresses, execute **tail ade_history.log** in the probe directory (Linux only; in Windows, use a utility similar to tail).

5. Installation is successful if there are no errors related to failing scripts and if the software is installed in the specified directory.

   After execution, the robots will (by default):

   - Auto-start on Windows systems
   - *Not* auto-start on Linux systems

     To start a robot on Linux, execute:

     ```
     /etc/init.d/nimbus start
     ```

     To view status of the robot, execute either:

     ```
     view controller.log
     tail controller.log
     ```

Removing the Package

To remove the package, execute the appropriate command.

- Windows

  ```
  msiexec /x <MSI _package> /qn
  ```

- Linux

  ```
  rpm -e <RPM_package minus the .rpm extension>
  ```

Appendix B: Installing NMS in an Active/Passive Microsoft Cluster

This section contains the following topics:

Overview

Running NMS within an active/passive MS Server 2008 R2 Failover Cluster minimizes the risk of having a single point of failure due to hardware problems or maintenance. All monitoring continues to operate as if nothing had happened, even if the cluster nodes change state.

To set up NMS to run on a cluster, you must:

1. **Install NMS on the Cluster** (page 93)
2. **Configure the Nimsoft Robot Watcher Service** (page 94)
3. **Test Failover Operation** (page 96)

Note: This procedure assumes your cluster is configured. Cluster configuration is covered in detail in Microsoft documentation and a variety of Microsoft developer and third-party internet resources. Some suggested sources for more information:

- http://technet.microsoft.com
- http://blogs.msdn.com
- Search internet video sites for Windows Server 2008 R2 Failover Clustering

Prerequisites

Required

- Virtual IP address you will assign to the virtual Nimsoft service
- Administrative access to an active/passive two-node failover cluster
- Shared disk/iSCSI target (typically SAN, NAS or RAID array) configured
- All resources are available to both cluster nodes

Recommended

- Do *not* install any Nimsoft consoles (primarily Infrastructure Manager) on the cluster nodes. Install these on a separate workstation.

Note: For database high availability, MS SQL Server is often configured to run in a MS Server 2008 cluster. When using a MS SQL Server database (with NMS running either on a single host or in a cluster), the HA database service appears to NMS the same as a non-cluster implementation. No special database connection or configuration is required.

Install NMS on the Cluster

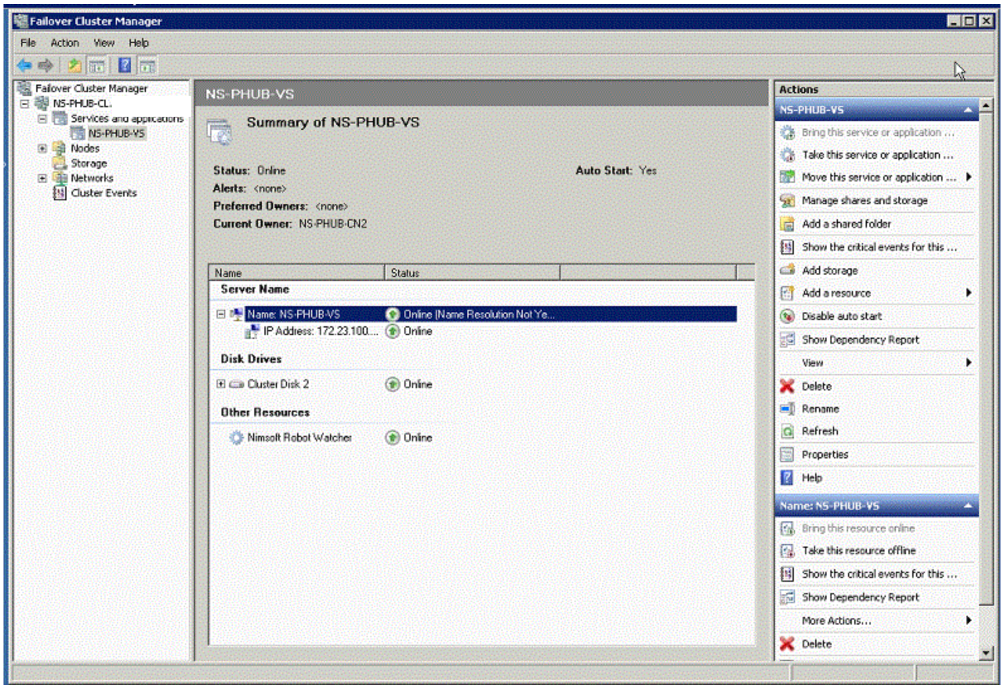
1. Install NMS on the active node in the cluster. Use one of the Windows installation procedures in **Chapter 3: NMS Installation** (page 50), **with one exception**:
   - When you specify the network interface you want to use, enter the virtual IP address you assigned to the virtual Nimsoft service. Do *not* use the virtual IP address of the node or its physical IP address.
2. Verify that the installation was successful by starting Nimsoft and viewing the status of the hub and robot(s) using Infrastructure Manager.
3. Use **Failover Cluster Manager** to fail over the cluster from the active node to the passive node (second system in the cluster).
4. Install NMS on the second system in the cluster (now that it is active) using the procedure you chose for step 1, the virtual IP address assigned to the virtual Nimsoft service for the network interface.

Installing in this manner ensures that all required registry entries and DLLs are installed properly on both nodes of the cluster, and that IP bindings are correct.

Configure the Nimsoft Robot Watcher Service

The Nimsoft Robot Watcher restarts the robot if it stops for any reason. In this context, if the robot stops because a primary node goes down, this service restarts the robot on the failover node.

1. On the active node, launch **Failover Cluster Manager**. The failover cluster is shown. (In the example below, the cluster is NS_PHUB_CL; the NMS service is NS-PHUB-VS.)

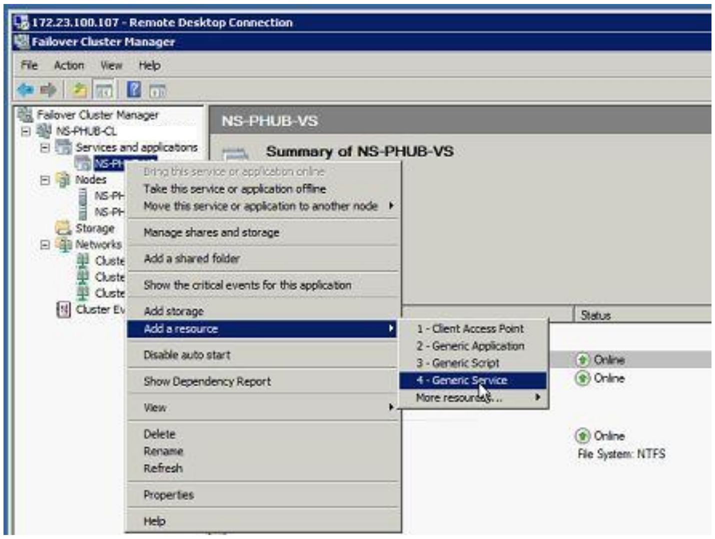


Status: Online
Alerts: <none>
Preferred Owners: <none>
Current Owner: NS-PHUB-CN2
Auto Start: Yes

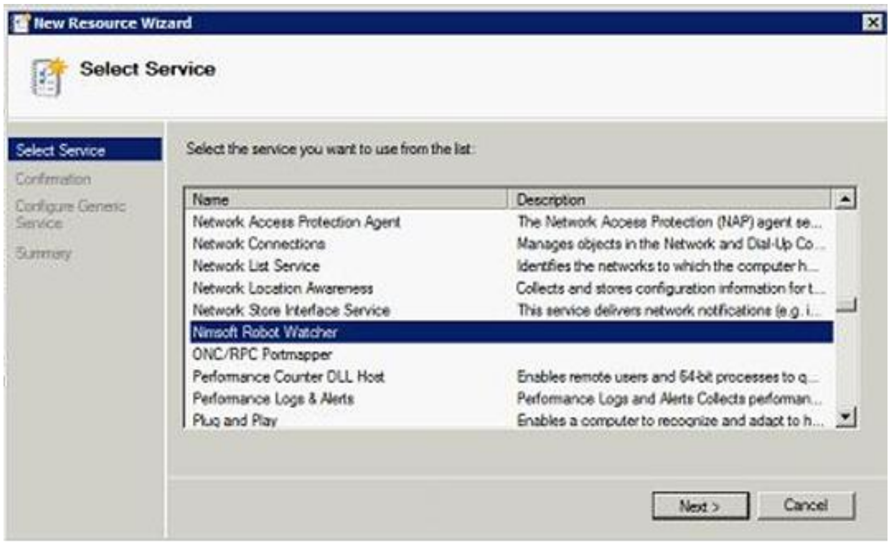
Name	Status
Server Name	
Name: NS-PHUB-VS	Online (Name Resolution Not Ye...
IP Address: 172.23.100....	Online
Disk Drives	
Cluster Disk 2	Online
Other Resources	
Nimsoft Robot Watcher	Online

2. Expand the tree in the left frame. Under **Services and applications**, select the failover cluster object.

3. Right-click on the cluster, then select **Add a resource > Generic Service**.



4. The **New Resource Wizard** launches. Select the **Nimsoft Robot Watcher** service, then click **Next** and **Finish**.



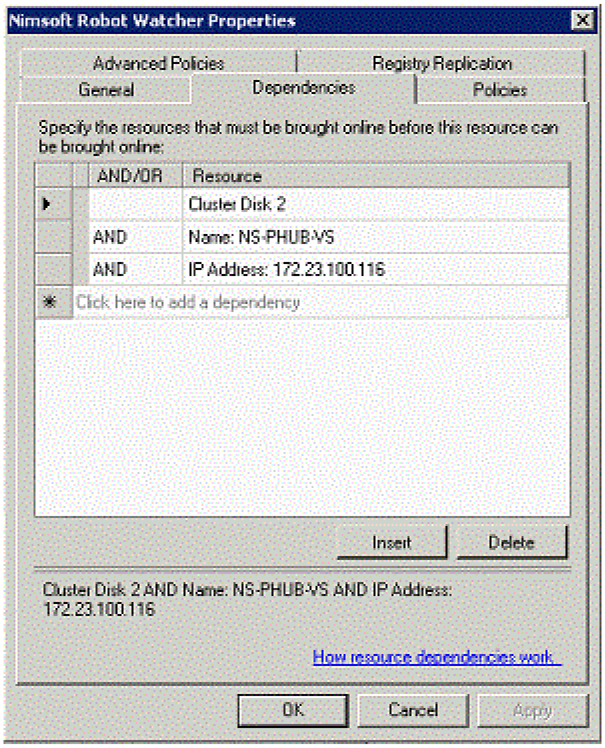
Select the service you want to use from the list:

Name	Description
Network Access Protection Agent	The Network Access Protection (NAP) agent se...
Network Connections	Manages objects in the Network and Dial-Up Co...
Network List Service	Identifies the networks to which the computer h...
Network Location Awareness	Collects and stores configuration information for t...
Network Store Interface Service	This service delivers network notifications (e.g. i...
Nimsoft Robot Watcher	
ONC/RPC Portmapper	
Performance Counter DLL Host	Enables remote users and 64-bit processes to q...
Performance Logs & Alerts	Performance Logs and Alerts Collects performan...
Plug and Play	Enables a computer to recognize and adapt to h...

5. In the cluster **Summary** screen, right-click **Nimsoft Robot Watcher** and select **Properties**.

6. On the **Dependencies** tab, set the dependencies for the Nimsoft Robot Watcher service. Three cluster resources must all be online and available before the Nimsoft Robot Watcher service should start:

- Cluster shared disk
- Virtual Nimsoft resource
- Virtual IP address assigned to the virtual Nimsoft service



Specify the resources that must be brought online before this resource can be brought online:

AND/OR	Resource
	Cluster Disk 2
AND	Name: NS-PHUB-VS
AND	IP Address: 172.23.100.116

Click here to add a dependency

Cluster Disk 2 AND Name: NS-PHUB-VS AND IP Address: 172.23.100.116

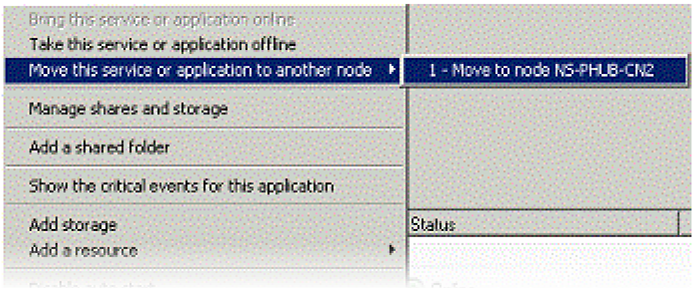
Test Failover Operation

Follow these steps to test the failover and failback operation of Nimsoft within the cluster.

Note: It is good to have Infrastructure Manager (running on a separate workstation) open so you can observe the status of the Nimsoft Hub during the failover test.

1. Launch **Failover Cluster Manager** and expand the tree in the left frame.

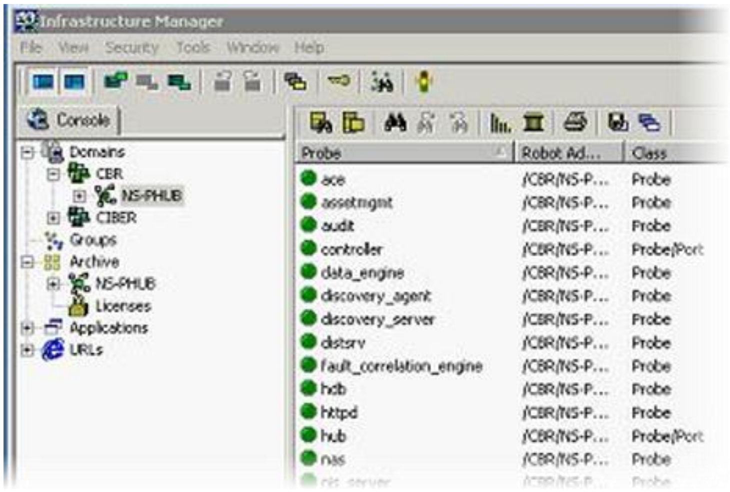
2. Right-click on the virtual Nimsoft hub and select **Move the service or application to another node**.


Bring this service or application online
Take this service or application offline
Move this service or application to another node
1 - Move to node NS-PHUB-CN2
Manage shares and storage
Add a shared folder
Show the critical events for this application
Add storage
Add a resource
Status

3. Select the other node in the cluster and confirm the operation.

4. As the service moves to the passive node, Infrastructure Manager shows that the hub becomes unavailable by displaying it in red. Failover Cluster Manager shows the status of the cluster as the NMS service moves to the failover node.

5. After a short time, check the hub status in Infrastructure Manager. It should be green, indicating that NMS has come up successfully on the failover node.



Probe	Robot Ad...	Class
ace	/CBR/NS-P...	Probe
assetmgmt	/CBR/NS-P...	Probe
audit	/CBR/NS-P...	Probe
controller	/CBR/NS-P...	Probe/Port
data_engine	/CBR/NS-P...	Probe
discovery_agent	/CBR/NS-P...	Probe
discovery_server	/CBR/NS-P...	Probe
distsrv	/CBR/NS-P...	Probe
fault_correlation_engine	/CBR/NS-P...	Probe
hdb	/CBR/NS-P...	Probe
httpd	/CBR/NS-P...	Probe
hub	/CBR/NS-P...	Probe/Port
nas	/CBR/NS-P...	Probe
nis_server	/CBR/NS-P...	Probe

6. Repeat these steps to failback the service to the original node.

Appendix C: MySQL Windows Installation

This section contains the following topics:

Windows Installation

Follow the installation instructions for your platform, available at http://dev.mysql.com/doc/ (not affiliated with Nimsoft).

Supported Windows versions are Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, or Windows Server 2008. Both 32-bit and 64-bit versions are also available where relevant.

MySQL should be installed by a user with administrative privileges to help avoid problems with paths, environment variables or accessing the service control manager. Once the installation is complete, however, MySQL does not need to be run by an administrative user.

Windows-specific Prerequisites and Considerations

Be aware of the following potential issues you may encounter when installing MySQL on Windows.

- If table sizes are expected to exceed 4 GB, then MySQL must be installed on an NTFS or newer file system.
- Virus scanning software can sometimes generate erroneous alerts that incorrectly identify the datafile contents as malicious. This is due to the combination of the MySQL datafile update frequency and the fingerprinting used by some anti-virus packages.

  Recommendation: After installation, prevent any anti-virus software from scanning the main data directory (**datadir**) and any other directory used by MySQL for temporary datafile creation.
- Windows XP and later include a firewall that specifically blocks ports. If you intend to use MySQL through a network port, ensure the relevant ports are open before installation.

Installation Steps

1. Run the installer package.
2. Acknowledge any security warnings.
3. Select install type:
   - **Complete** is recommended.
   - Choose **Custom** if you want to specify datafile locations, such as on a separate, high-performance disk. Specify the paths where required. This can also be done after installation by rerunning the installer and selecting **Modify** on the basis that there is no data installed, as existing datafiles are not copied).
4. In the **Ready to install** dialogue, select **Continue**. Ignore information about MySQL Enterprise.
5. When installation is complete, the installer allows you to **Register MySQL as a Service**. This is recommended, as it allows control of MySQL from Windows Service Manager and ensures the database starts automatically if required.

If desired, you can configure the MySQL instance. For example, you can create the root password, add additional users, specify configuration details such as datafile location.

There are no specific post-installation steps to carry out, as the paths, directories, system tables and service manager registration are all set up by the installer.

Standard Post-installation Configuration

1. To enable mysql startup at boot time, and simplify the server control, copy the server startup scripts to the relevant location. From the **mysql** directory, execute:

   ```
   cp support-files/mysql.server
   /etc/init.d/mysqld
   ```

   This allows the server to be started using:

   ```
   /etc/init.d/mysqld [start|stop|restart|status]
   ```

2. Create the empty file **/etc/my.cnf** (or modify one of the standard configurations as specified in **Basic Tuning Configuration Changes** on page 99.
3. Insert the following into **my.cnf** in the **mysqld** section:

   ```
   [mysqld]
   innodb_file_per_table
   slow_query_log_file=[path/to/chosen/location/for/slowlog.log]
   datadir=[path/to/datafile/location]
   ```

Basic Tuning Configuration Changes

Available tuning parameters depend on the hardware, memory, number of expected connections and throughput/queries per second. As more of this information is available and known, the configuration and tuning parameters can be modified to ensure optimal performance for the NIS database. However, without this information you are still able to establish a good initial setup with the following parameters and configuration settings.

Follow these steps to adjust the parameters as appropriate for your hardware performance.

1. Choose a configuration file appropriate for your system.

   A number of pre-populated **my.cnf** or **my.ini** configuration files are bundled with MySQL. These are named **my-small**, **my-medium**, **my-large**, and **my-huge**.

   The configuration files contain indicators of the size of system for which they might be appropriate.

2. Estimate the **max_connections** parameters based on the total RAM available with the following calculation:

   (total RAM — global buffers)/ total size of thread buffers

   a. From the MySQL command line, execute:

   ```
   show variables
   ```

   b. Calculate *global_buffers* by adding the values of:

   ```
   key_buffer_size
   innodb_buffer_pool_size
   innodb_log_buffer_size
   innodb_additional_mem_pool
   net_buffer_length
   ```

   c. Calculate *thread buffers* by adding the values of:

   ```
   sort_buffer_size
   myisam_sort_buffer_size
   read_buffer_size
   join_buffer_size
   read_rnd_buffer_size
   ```

   d. Estimate of the *open_files_limit*. Add the number of *max_connections* with the *table_cache*, then double the number.

3. Because this installation is InnoDB specific, we suggest the following parameters as a starting point. Note that:

    - Changes you make to these parameters in **my.cnf** are made available when the server is restarted.
    - Some parameters are dynamic and can be changed via the MySQL client for immediate benefit.

Parameter	Recommendation
innodb_buffer_pool_size	Typically 70% to 80% of available RAM.
innodb_log_file_size	256 MB is an adequate size (your value depends on recovery speed requirements).
innodb_log_buffer_size	4 MB is a standard setting and is effective for most installations unless large amounts of binary data are in use.
innodb_flush_log_at_trx_commit	This can make a significant difference in performance. At the risk of losing the last second or two of data in the event of a crash, set this to **2**.
innodb_thread_concurrency	**8** (the default) is a good starting point.
innodb_flush_method	Set this to **O_DIRECT** to avoid double buffering, reduce swap usage and improve performance. (Note that without a battery-backed-up RAID cache write, IO may suffer.)
innodb_file_per_table	Set this to take full advantage of disk data allocation in partitioning. It does not affect performance directly, but makes data management and disk/OS housekeeping more manageable.

For a complete list of the server option parameters and their status as **dynamic** or **configuration only**, go to:

http://dev.mysql.com/doc/refman/5.5/en/server-system-variables.html

More accurate tuning can be performed once throughput, load and data-size are known.

Deployment Statistics and Estimations

Deployments can be considered small, medium or large as follows.

Deployment	Insert rate	Average row length	Approximate data growth rate
Small	1000 rows/second	170 bytes	9.7 MB per minute 12 GB per day
Medium	5000 rows/second	170 bytes	48 MB per minute 68 GB per day
Large	20,000 rows/second	170 bytes	194 MB per minute 273 GB per day

Specific disk configurations are not required to accommodate this data, as MySQL does not use the same logging configurations as other RDBMSs.

Schema and Data Management

The table schema is as follows:

```
CREATE TABLE `test`.`RN_QOS_DATA_xxxx` (
  `table_id` int(11) NOT NULL,
  `sampletime` timestamp NOT NULL,
  `samplevalue` bigint(20) DEFAULT NULL,
  `samplestdev` bigint(20) NOT NULL,
  `samplerate` bigint(20) NOT NULL,
  `samplemax` bigint(20) NOT NULL,
  `compressed` tinyint(4) DEFAULT '0',
  `tz_offset` bigint(20) NOT NULL,
  `inserttime` timestamp NOT NULL,
  PRIMARY KEY (`sampletime`,`table_id`)
) ENGINE=InnoDB;
```

Appendix D: Installation Modifications to Windows Systems

This appendix describes the system modifications made by Nimsoft installation.

NMS or Nimsoft Infrastructure Modifications

If you select a VB runtime when installing NMS or Nimsoft Infrastructure, the following components are installed.

Component	Install status
atl.dll (Windows system directory)	Updated if the existing version is old. This should not be the case on Window XP or Windows 2000 with an updated service pack.
asycfilt.dll stdole2.tlb	Updated if the existing version is old. This should not be the case on Window XP or Windows 2000 with an updated service pack.
asycfilt.dll stdole2.tlb	Updated if nonexistent, or the existing version is old.

Robot Modifications

Valid on Windows Server 2003/2008.

The following components are installed.

Component	Install status
.../Nimsoft	Nimsoft product directory. The default is **C:\Program Files\Nimsoft Monitoring**.
msvcrt.dll (Microsoft C library; installed in Windows system directory)	Updated if the existing version is old. This should not be the case on Window XP or Windows 2000 with an updated service pack.

New Registry sections	These store variables used internally by Nimsoft.
	`HKEY_LOCAL_MACHINE\Software\Nimsoft Software`
	`HKEY_LOCAL_MACHINE\Software\Nimsoft Software AS`
	`HKEY_LOCAL_MACHINE\Software\Nimsoft Corporation`

Start > Programs > Nimsoft Monitoring	Menu choice to start the Service Controller.
Services	The *Nimsoft Watcher* service can be managed with the service controller. To remove the service, execute: `…\Nimsoft\bin\Nimsoft -remove`