CA Nimsoft Monitor Server

Installation Guide

Release 7.6

ca
technologies

CA Nimsoft Monitor Copyright Notice

This online help system (the "System") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This System may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This System is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties. This System may not be disclosed by you or used for any purpose other than as may be permitted in a separate agreement between you and CA governing your use of the CA software to which the System relates (the "CA Software"). Such agreement is not modified in any way by the terms of this notice.

Notwithstanding the foregoing, if you are a licensed user of the CA Software you may make one copy of the System for internal use by you and your employees, provided that all CA copyright notices and legends are affixed to the reproduced copy.

The right to make a copy of the System is limited to the period during which the license for the CA Software remains in full force and effect. Should the license terminate for any reason, it shall be your responsibility to certify in writing to CA that all copies and partial copies of the System have been destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS SYSTEM "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS SYSTEM, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The manufacturer of this System is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Legal information on third-party and public domain software used in the Nimsoft Monitor solution is documented in *Nimsoft Monitor Third-Party Licenses and Terms of Use (*http://docs.nimsoft.com/prodhelp/en_US/Library/Legal.html*).*

Contact CA

Contact CA Support

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

- Online and telephone contact information for technical assistance and customer services

- Information about user communities and forums

- Product and documentation downloads

- CA Support policies and guidelines

- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

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

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

Document Revision History

Version	Date	Changes
7.6	June 2014	Revised for CA Nimsoft Monitor 7.6
7.5	March 2014	Revised for CA Nimsoft Monitor 7.5
7.1	Dec 2013	Revised for CA Nimsoft Monitor 7.1
7.0	Sept 2013	Revised for CA Nimsoft Monitor v7.0--changes in ADE and documentation fixes
6.5	3/31/2013	Updated for v6.5 NMS: new Admin Console, IP discovery runs after installation has completed, adoption of new RPM package in ADE 1.21, minor revisions to illustrations
6.2	12/14/2012	Updated and revised for automated_deployment_engine probe v1.20
6.1	9/10/2012	Minor revisions and documentation fixes for NMS Server 6.1
6.0	6/29/2012	Revised for release 6.0 of NMS and Automated Deployment Engine (ADE) probe v1.0
3.3	3/12/2012	Documentation fixes; added remote access and authentication install information for MySQL.
3.2	2/22/2012	Documentation fixes and hardware capacity planning figures revised
3.1	1/4/2012	Documentation fixes and "AAI robot installer packages" relabeled as "robot_msi_rpm installer packages"
3.0	12/16/2011	Minor revisions and documentation fixes for NMS Server 5.61
2.0	10/24/2011	New title: Nimsoft Monitor Server Installation Guide. Contains only content and procedures for new installations of NMS v5.6. Updated for InstallAnywhere Windows installer. Added section on Advanced Agent Installer (AAI). Migrated content from previous use guide to new document: NMS Configuration Guide
1.0	6/30/2010	Initial version NMS Installation and User Guide.

Contents

Chapter 1: Introduction

This guide is for systems administrators who are installing CA Nimsoft Monitor Server. It contains the following sections:

- **Introduction** provides an overview of the installation phases.

- Preparing the Servers (page 13) explains how to set up the servers that will host CA Nimsoft Monitor server, hte database, and the Unified Management Portal (UMP) software.

- Installing the Primary Hub (page 27) explains how to run the CA Nimsoft Monitor server installer, which sets up your primary hub, installs Admin Console, installs Infrastructure Manager (on Windows servers), and provides the software you need to install robots and hubs.

- Installing Robots and Secondary Hubs (page 45) explains how to deploy secondary hubs, which are used to connect remote systems and can be and robot software onto the systems you want to monitor. This section also explains how to run the robot installer to set up robots one at a time.

- Deploying Robots in Bulk explains how to use the Automated Deployment Engine (ADE) or a third-party tool to deploy robots throughout your infrastructure.

- Installing and Accessing Management Consoles (page 73) explains how to access the web-based Admin Console and how to install Infrastructure Manager on a system other than the primary hub.

- Modifications to Windows Systems (page 75) describes the system modifications made during installation.

Notes: *Unified Management Portal (*UMP) and *Unified Reporter* (UR) have their own installation guides. If you are upgrading, see the *CA Nimsoft Monitor Release Notes and Upgrade Guide.*

These documents are available either from the documentation library or the **Downloads** tab at support.nimsoft.com.

Installation Overview

The CA Nimsoft Monitor solution is made up of a number of distributed, loosely-coupled software modules. The process of installing these modules to build out a full deployment can be divided into three phases:

1. **Preparing the servers.** Proper configuration of the operating systems and database helps ensure a successful installation.

2. **Installing CA Nimsoft Monitor Server.** This process installs the foundation, which consists of the:

   ■ Primary hub, which includes a robot and service probes

   ■ Message bus, which enables communication between the hub, its robots and probes and between the hub and the database

   ■ CA Nimsoft Monitor web page, which provides convenient links to infrastructure client installers and to Admin Console, a web-based infrastructure management application

   ■ Nimsoft Information Store (NIS) database, formerly referred to as the SLM database

   ■ CA Nimsoft Monitor Administrator account on the primary hub server and database server

   ■ Software required to deploy secondary hubs, robots and probes throughout your infrastructure
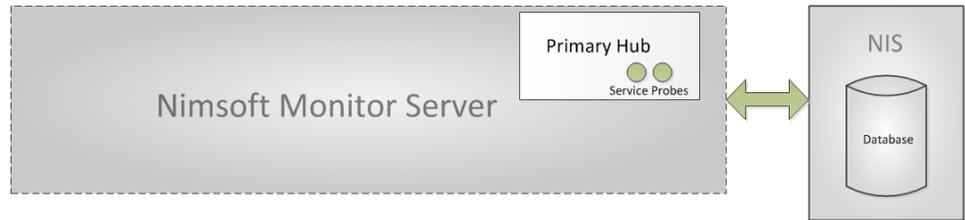
3. **Installing secondary hubs (optional) and robots.** These elements create the CA Nimsoft Monitor infrastructure that will manage the monitoring probes, collect their data, and route it to the primary hub.

   You can install the 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 might require you to create secure tunnels between hubs.

See the following for diagrams that illustrate a local deployment and a deployment that is both local and remote.

Local Deployment

Local and Remote Deployment
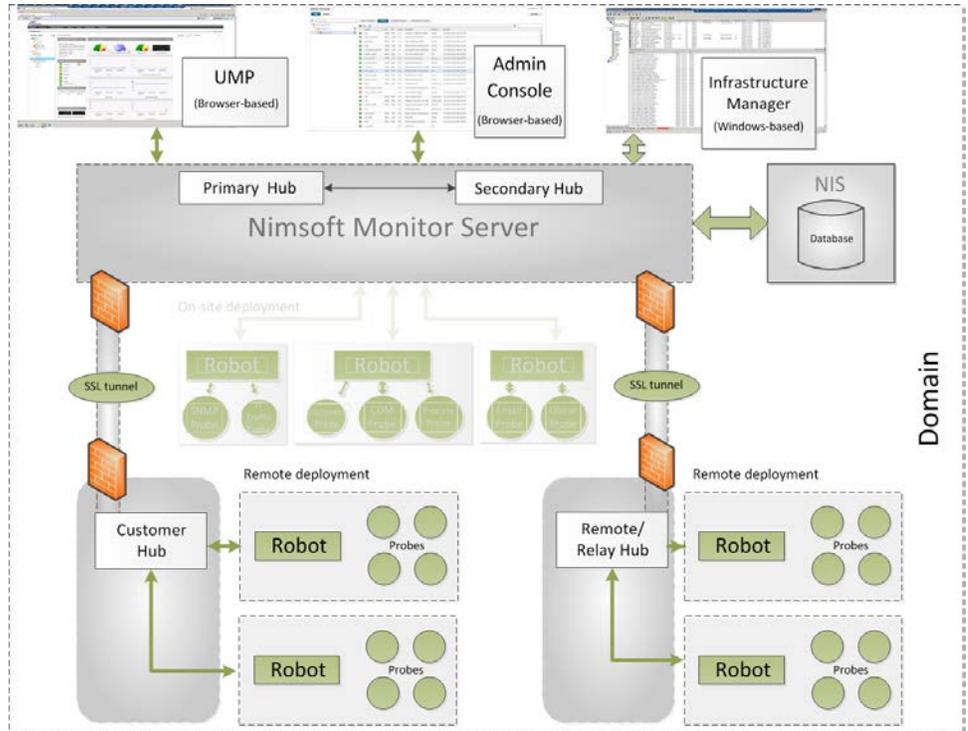
Working with Firewalls and DMZs

Most companies have one or more firewalls in their network, both internally between different networks and externally against the Internet or a network DMZ.

Because network administrators are often reluctant to open a firewall for the number of IP addresses and ports that management applications require, it can be difficult to monitor the whole network from a central location.

The solution is to set up a secure shell (SSH) tunnel between two hubs that are separated by a firewall. The tunnel:

- Sets up a VPN (Virtual Private Network) connection between the hubs.

- Enables all requests and messages to be routed over the tunnel and dispatched on the other side. This routing is transparent to all the users within the CA Nimsoft Monitor domain.

Note: A hub in a DMZ must have a public IP address if you want to access it from the Internet.

Security

Security between hubs 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. You will configure the tunnel server hub to be a CA (Certificate Authority), which will then give you the ability to create client certificates.

- **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 levels provide greater security but are more resource intensive for the systems at both ends of the tunnel.

Tunnel Setup Overview

You can set up tunnels:

- **During installation**. The hub installation processes let you set up DMZ tunnel servers and clients. For details refer to:

    - Installing a Windows Robot, Hub and Distribution Server (page 48)

    - Installing Infrastructure on Linux or Solaris Clients (page 51)

- **On existing hubs after installation** by configuring the hubs. This can be done in either *Admin Console*, the CA Nimsoft Monitor web-based management console, or *Infrastructure Manager*, the CA Nimsoft Monitor Windows-based console.

Note: Because the tunnel server uses a fair amount of computing power, the system with the lower load should be the tunnel server. If you plan to have a central hub with several remote hubs attached to it, it is better for the remote hubs to be the tunnel servers so that each remote hub only adds a small amount of overhead to the central hub.

Required Ports for SSL Tunnels

The following ports are required.

- **48000** (controller)

- **48002** (hub)

- A configured tunnel server port (default is **48003**, this also can be set to **443**). This 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.

- **8443** and **8080** (service_host) to allow web access to AdminConsole and the CA Nimsoft Monitor web page.

Chapter 2: Preparing the Servers

For best performance, the physical or virtual servers that host your primary components must have sufficient processing power and memory. To set up your servers, you will:

1. **Determine the size of your deployment.**

2. **Select sufficient hardware.**

3. **Install system and database software.**

   Note: Your servers do NOT need to run the same operating system.

Separate topics explain how to set up the following servers to meet the needs of your deployment:

- **NMS server**, which hosts your primary hub

- **NIS server** (Nimsoft Information Store), which hosts your database

- **UMP server**, which hosts the Unified Management Portal

For evaluations, you can install all three components on a single system. For production environments, we recommend you distribute them across multiple virtual or physical servers to give them sufficient computing power and memory to perform optimally.

Use the Server Setup Checklist (page 24) to keep track of information and requirements as you go through the process of setting up your servers.

Determine Your Deployment Size

Your hardware needs are determined by the size of your deployment, which is based on the number of hubs and robots you expect to install.

	Hubs	Robots
Small	1	100
Medium	5	250
Large	20	500
Major	50	1000

Plan to deploy more than 50 hubs and 1000 robots? Use the specifications for a major deployment as a starting point, and consult with professional services or a certified partner for guidance.

When choosing your size, keep in mind that:

- A hardware configuration that works today may need to grow in the future. Consider forecast growth when choosing your hardware.

- Use the numbers provided here to begin planning your deployment, but consider that your particular situation may impose greater or lesser demands on the system.

Consult your sales representative if you have questions about your hardware needs.

Set up the Server to Host Primary Hub

Your NMS server must meet the following requirements. For supported software versions, see the Nimsoft Monitor Compatibility Matrix at http://support.nimsoft.com/downloads/doc/NMSCompatibility_SupportMatrix_current.pdf.

Deployment	Processor 64-bit XEON-class, 2.0 GHz or better	Memory	Software
Small	One dual-core	4 to 8 GB	■ Supported version of Windows, Linux or Solaris
Medium	One or two quad-core	12 GB	■ Supported 64-bit Java Runtime Environment ■ JRE is in system PATH
Large	Two quad-core	12 GB	■ Disk compression is NOT enabled ■ *Linux and Solaris:* minimum 4 GB swap space (6 GB recommended)
Major	Two quad- or eight-core	16 to 24 GB	■ *Linux:* standard C++ library

Plan to use SQL Server? Ensure that a domain administrator has permission to **log on as a service**. See *Configuring User Rights* at technet.microsoft.com/en-us/library/dd277404.aspx for instructions.

Plan to use Oracle? You must install Oracle Instant Client on the NMS server.

Using Linux? The system's /etc/hosts file must map 127.0.0.1 to localhost, and its own IP address to its hostname.

Installing on VMware ESX Server? Review *Enterprise Java Applications on VMware — Best Practices Guide* at www.vmware.com/resources/techresources/1087.

Oracle Instant Client Installation

1. Go to www.oracle.com and select **Downloads** > **Instant Client**.

2. Select the 64-bit Instant Client for your operating system.

3. Download the version of **Instant Client Package – Basic** that corresponds to your Oracle database version.

4. Unzip the package into a single directory (for example, *instantclient*).

5. Set the *library loading path* environment variable to that directory.

   Note: LD_LIBRARY_PATH is the appropriate environment variable on many UNIX platforms. Use PATH on Windows.

6. Restart the server.

Set up the NIS server to host the database

Your NIS server must meet the following requirements. For supported software versions, see the Nimsoft Monitor Compatibility Matrix at
http://support.nimsoft.com/downloads/doc/NMSCompatibility_SupportMatrix_current.pdf.

Deployment	Processor 64-bit XEON-class, 2.0 GHz or better	Memory	Storage recommendations	Software
Small	One dual-core	8 GB	■ 1 TB minimum for NIS database ■ RAID 10 (for speed and reliability) ■ Spread DB files across multiple disks to improve I/O ■ Choose drive subsystems with low latency/seek times, high spindle speeds, high interconnect bandwidth ■ Continually consider data redundancy, synchronization, and database growth	■ Supported version of Windows, Linux or Solaris ■ Supported version of SQL Server (*Windows only*), MySQL or Oracle, installed and configured (see instructions below) ■ Disk compression is NOT enabled ■ *Linux:* standard C++ library
Medium	One or two quad-core	12 GB		
Large	Two quad-core	12 to 18 GB		
Major	Two quad- or eight-core	18 to 24 GB		

Begin with a clean system and a fresh database installation. Using a pre-existing database can cause subtle configuration conflicts that are hard to diagnose.

- SQL Server installation and configuration (page 17)

- MySQL installation and configuration (page 18)

- Oracle installation and configuration (page 22)

Using Linux? The system's /etc/hosts file must map 127.0.0.1 to localhost, and its own IP address to its hostname.

Installing on VMware ESX Server? Review *Enterprise Java Applications on VMware — Best Practices Guide* at www.vmware.com/resources/techresources/1087.

Note: 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 NIS database. Selecting the right database storage solution is beyond the scope of this document. Consult your storage vendor if you need further assistance.

SQL Server Installation and Configuration

To set up your database software:

1. Go to www.microsoft.com/sqlserver and download 64-bit SQL Server. (Use the free Express version only for evaluations or demonstrations; see notes below.)

2. Install the software, noting that the instance name you choose now affects your database port selection during NMS installation. If you use:

   ■ **the default instance name**, the database port can be:

      – 1433, the default port (simplest method)

      – any open port of your choice

   ■ **any other instance name**, you must use port 1433

3. If necessary, set up Windows authentication. During NMS installation, you will choose an authentication option. If you plan to choose:

   ■ **SQL Server with SQL Server login**, no modifications are needed.

   ■ **SQL Server with Windows authentication**, you must ensure that:

      – A domain administrator has permission to **log on as a service** on both the NMS server and the NIS server. See *Configuring User Rights* at technet.microsoft.com/en-us/library/dd277404.aspx.

      – SQL Server is configured to use Windows authentication. See *Create a Login* at msdn.microsoft.com/en-us/library/aa337562.aspx.

4. Ensure that a domain administrator has permission to **log on as a service**. See *Configuring User Rights* at technet.microsoft.com/en-us/library/dd277404.aspx for instructions.

5. Ensure that **TCP/IP client protocol** is enabled for SQL Server (you can do this in the SQL Server Configuration Manager).

6. If you plan to use UMP with a non-English language, set the database collation to that language before installing NMS.

   Note: If you install NMS before setting the database collation, you must un-install NMS, change the database collation, and then re-install NMS.

Your NIS server is ready.

MySQL Installation and Configuration

MySQL reference manuals are available at dev.mysql.com/doc. Refer to the *Server Option and Variable Reference* in the appropriate manual for a list of server and status variables and command line options.

1. Go to http://dev.mysql.com/downloads and download a supported version of MySQL Enterprise, Cluster or Community Server.

2. Install the software. Note the following:

    ■ Run the installer as an administrator to help avoid problems with paths, environment variables or accessing the service control manager.

    ■ When you select the 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.

3. Log into MySQL server as the administrator.

4. Set the following variables in the MySQL server configuration file.

    ■ local_infile: **ON**
    ■ lower_case_table_names: **1**
    ■ binlog_format: **mixed**
    ■ log_bin: **ON**

5. *Large or major deployments only:* Add these lines to the MySQL server configuration file. Use the values shown here, then fine-tune them as needed.

    ```
    [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
    ```

6. Decide how you will create your database:

    ■ **During NMS installation.** The NMS installer can create the database. In this case, root must have remote access to the MySQL service.

    ■ **Manually, before <NMS installation.** The advantage is you do not have to allow NMS to access a MySQL account with administrator privileges.

7. If you want the installer to create the database, grant remote access to root. Execute:

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

    where *<root_password>* is the MySQL administrator password.

8. If you want to create the database manually:

   a. Log in as the MySQL administrator.

   b. Create the database. Execute:

      ```
      CREATE DATABASE IF NOT EXISTS <nimsoft_db_name> DEFAULT CHARACTER SET
      =utf8 DEFAULT COLLATE =utf8_unicode_ci;
      ```

      where *<nimsoft_db_name>* is the desired database name.

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

      ```
      CREATE USER 'nimsoft_db_owner'@'%' IDENTIFIED BY
      'nimsoft_db_owner_password';
      GRANT ALL PRIVILEGES ON <nimsoft_db_name>.* TO
      'nimsoft_db_owner'@'%';
      GRANT TRIGGER ON <nimsoft_db_name>.* TO 'nimsoft_db_owner'@'%';
      GRANT SUPER ON *.* TO 'nimsoft_db_owner'@'%';
      FLUSH PRIVILEGES;
      ```

      where *<nimsoft_db_owner>* is the desired user name for the owner,
      *<nimsoft_db_owner_password>*is the desired password, and
      <nimsoft_db_name> is the database you just created.

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

9. When prompted, select **Register MySQL as a Service** (recommended). This lets you control MySQL from Windows Service Manager and ensures the database starts automatically if required.

Your NIS server is ready. Refer to the MySQL server documentation at dev.mysql.com/doc www.dev.mysql.com/doc for information on post-installation configuration.

Basic Tuning Configuration Changes

Available tuning parameters depend on the hardware, memory, number of expected connections and throughput/queries per second.

You can establish a good initial setup with the following parameters and configuration settings. As more of this information is available and known, you can modify the settings to ensure optimal database performance.

Follow these steps:

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 **my.cnf** parameters take effect 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.

Go to http://dev.mysql.com/doc/refman/5.5/en/server-system-variables.html for a complete list of the server option parameters and their status as **dynamic** or **configuration only**,

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

Oracle Installation and Configuration

1. Install the software:

    a. Go to www.oracle.com http://www.oracle.com and select **Downloads** > **Oracle Database**.

    b. Download the 64-bit packages appropriate for your operating system and unzip the files into the same directory.

    c. Install the software as instructed at docs.oracle.com/cd/E16655_01/nav/portal_11.htm.

2. Set required configuration parameters before installing NMS. As the Oracle database administrator, execute:

    ```
    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;
    ALTER SYSTEM SET NLS_COMP=LINGUISTIC SCOPE=SPFILE;
    ALTER SYSTEM SET NLS_SORT=BINARY_AI SCOPE=SPFILE;
    ```

3. Restart the database service.

4. Decide whether you will create your database manually or with the NMS installer. If you:

    ■   **Create the tablespace manually (recommended)**, you do not have to allow NMS to access an Oracle administrator account.

    ■   **Allow the NMS installer to create the database** (and, if desired, the database owner), root must have remote access to the Oracle service.

5. If you decided to create the database manually:

    a. Log in as the Oracle administrator.

    b. Create the tablespace. Execute:

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

    where <ts_name> is a tablespace name of your choice (typically *nimsoftslm*).

    c. Create the owner and assign required privileges. Execute:

    ```
    create user <db_owner> IDENTIFIED BY <owner_password> DEFAULT TABLESPACE
    <ts_name>;
    grant unlimited tablespace to <db_owner>;
    grant administer database trigger to <db_owner>;
    grant create table to <db_owner>;
    grant create view to <db_owner>;
    grant create sequence to <db_owner>;
    grant create procedure to <db_owner>;
    grant create session to <db_owner>;
    grant create trigger to <db_owner>;
    grant select on sys.v_$session to <db_owner>;
    grant execute on sys.dbms_lob to <db_owner>;
    ```

where *<db_owner>* is the name of the user to be created and *<ts_name>* is the tablespace.

Note: It is common for the owner and tablespace to have the same name.

6. Link the shared Oracle libraries:

   a. Create the file **/etc/ld.so.conf.d/oracle.conf**. In it, specify the path to the Instant Client directory. For example, **/root/instantclient_11_1**.

   b. Navigate to the Instant Client directory and execute:

      ```
      ldconfig
      ```

   c. Execute:

      ```
      ldd libociei.so
      ```

   d. Verify that all the libraries have links and that 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)
      ```

7. Turn off the Oracle recycle bin:

   a. Use a tool such as SQL Developer to connect to the Oracle database.

   b. Execute the following commands:

      ```
      ALTER SYSTEM SET recyclebin = OFF DEFERRED;
      ALTER SESSION SET recyclebin = off;
      ```

   c. Verify that the recycle bin is off. Execute:

      ```
      show parameter recyclebin;
      ```

Your NIS server is ready.

Set up the UMP Server

Your UMP server must meet the following requirements. For supported software versions, see the Nimsoft Monitor Compatibility Matrix at http://support.nimsoft.com/downloads/doc/NMSCompatibility_SupportMatrix_current.pdf.

See the *UMP Installation Guide* for installation instructions.

Deployment	**Processor** 64-bit XEON-class, 2.0 GHz or better	Memory	Software
Small	*Install on the primary hub server.*		■ Supported version of Windows, Linux or Solaris ■ *Linux and Solaris:* minimum 4 GB swap space (6 GB recommended) ■ *Linux:* standard C++ library
Medium	One quad-core	4 to 8 GB	
Large	Two quad-core	8 to 12 GB	
Major	Two quad-core	16 GB	

Using Linux? The system's /etc/hosts file must map 127.0.0.1 to localhost, and its own IP address to its hostname.

Installing on VMware ESX Server? Review *Enterprise Java Applications on VMware — Best Practices Guide* at www.vmware.com/resources/techresources/1087.

Server Setup Checklist

You will need information about your servers when you install NMS. Use this list to keep track of information and check off setup requirements while you prepare your servers.

Deployment size	□ Small □ Medium □ Large □ Major
NMS server setup	NMS server IP: □ Supported OS □ Supported 64-bit Java □ JRE in system path □ Disk compression OFF □ *Linux and Solaris:* 4 to 6 GB swap space □ *Linux:* IP addresses mapped in etc/hosts □ *Linux:* Standard C++ library installed □ *SQL Server:* Domain administrator can log on as a service □ *Oracle*: Oracle Instant client installed
NIS server setup	NIS server IP: Database, instance, or tablespace name (if created): Database user name (if created): □ Supported OS □ Supported database software, installed and configured □ Disk compression OFF □ 1 TB storage □ RAID 10 □ *Linux:* IP addresses mapped in etc/hosts □ *Linux:* Standard C++ library installed
UMP server setup	UMP server IP: □ Supported OS □ Disk compression OFF □ *Linux and Solaris:* 4 to 6 GB swap space □ *Linux:* IP addresses mapped in etc/hosts □ *Linux:* Standard C++ library installed

Chapter 3: Installing the Primary Hub

The NMS installer can be run in three modes:

- **Graphical user interface** (GUI) mode

- **Silent mode**

- **Console mode** (Linux and Solaris only)

If you are installing on a Microsoft high-availability platform, refer to Installing NMS in an Active/Passive Microsoft Cluster (page 36).

Note: This section explains how to install NMS for the first time.

- To upgrade an existing installation, see the *Nimsoft Monitor Server Release Notes and Upgrade Guide* available from **Downloads** at support.nimsoft.com.

- To reinstall, uninstall the prior version as explained in Uninstalling NMS (page 44), and restart the installation process. Note that your server configuration information (domain and hub names, IP addresses, user accounts and passwords) is *not* retained.

Installing in GUI Mode

You can install in GUI mode on Windows, Linux and Solaris platforms.

1. Log on to the NMS server as administrator.

2. Shut down your anti-virus software (required) and firewall (recommended).

3. Log on to Nimsoft Technical Support, click **Downloads**, and go to the current version of NMS Server.

4. Download and launch the appropriate **Installer for NMS**.

5. Follow the prompts to complete the installation. Note the following:

   ■ The installer will prompt you to either create a database or use an existing database. If you select:

      – **Create database**, the installer builds the required tables on the NIS database server.

      – **Use existing database**, you need an empty database instance created in advance specifically for NMS .

   ■ If you are using SQL Server with Windows authentication, make sure a domain administrator has permission to **log on as a service** on both the NMS and the NIS servers, and that SQL Server is configured to use Windows authentication.

   ■ Database server parameters and hub configuration values are case-sensitive. The parameters are defined here:

      – MySQL Database Parameters (page 31)

      – SQL Server Database Parameters (page 32)

      – Oracle Database Parameters (page 32)

      – Hub Configuration Values (page 33)

   ■ Post configuration can take several minutes.

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

6. Turn on your anti-virus and firewall software.

Installation is complete. You are ready to deploy and install secondary hubs and robots on client systems.

Installing in Silent Mode

Follow these steps to install in silent mode.

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. Go to the **Downloads** tab at Nimsoft Technical Support. Under *NMS*, click the link for the current version of *NMS Server*, and download the:

   ■ Most recent *NMS installer package* for your operating system (the package is over 1 GB, so this could take several minutes)

   ■ *Silent Install Templates for NMS* zip package

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

4. Prepare your response file:

   a. Extract the silent install template zip file.

   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. In **installer.properties**, enter or change the parameter values as needed. All lines that do not begin with a **#** symbol must have a value. For details, refer to Silent Install Parameter Values.

   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).

5. Run the installer. From a command line, execute:

   ■ Windows: **installNMS.exe -i silent**

   ■ Linux: **installNMS_linux.bin -i silent**

   ■ Solaris: **installNMS_solaris.bin -i silent**

6. 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
   ```

7. NMS launches. If for some reason it does not, execute:

   ■ Windows: **net start NMS Robot Watcher**

   ■ Linux or Solaris: **/etc/init.d/nimbus start**

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

Installation is complete. Go to Nimsoft Client Installation (page 45) to deploy and install CA Nimsoft Monitor infrastructure on client systems.

Installing in Console Mode (Linux or Solaris)

This procedure can be used on Linux or Solaris systems only.

1. Log on to the NMS server as administrator.

2. Shut down your anti-virus software (required) and firewall (recommended).

3. Log on to Nimsoft Technical Support, click **Downloads**, and go to the current version of NMS Server.

4. Download the appropriate **Installer for NMS**.

5. Execute chmod 755 on the install file to make it executable.

6. From a command line, execute the appropriate command:

   ```
   installNMS_linux.bin -i console
   installNMS_solaris.bin -i console
   ```

   Note: It might take a few minutes for the files to unpack.

7. Follow the prompts to set up your database and specify your hub and robot information. Note the following:

   - You can either create a database now or use an existing database. If you:

     – **Create the database**, the installer builds the required tables on the NIS database server.

     – **Use an existing database**, you need an empty database instance created in advance specifically for NMS.

   - Database server parameters and hub configuration values are case-sensitive. The parameters are defined here:

     – MySQL Database Parameters (page 31)

     – SQL Server Database Parameters (page 32)

     – Oracle Database Parameters (page 32)

     – Hub Configuration Values (page 33)

   - Post configuration can take several minutes.

   - To see the progress of the installation in detail, execute:

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

8. Turn on your anti-virus and firewall software.

Installation is complete. You are ready to deploy and install secondary hubs and robots on client systems.

To start and stop the NMS process, execute:

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

```
$ /etc/init.d/nimbus stop
```

GUI and Console Install Parameters

The GUI and console installation processes prompt you for the parameters required for your operating system and database.

■ MySQL Database Parameters (GUI and console mode) (page 32)

■ SQL Server Database Parameters (GUI and console mode) (page 32)

■ Oracle Database Parameters (GUI and console mode) (page 32)

■ Hub Parameters (GUI and console mode) (page 33)

Silent install parameters are defined in the **installer.DB_OS.properties** file. Parameters for all platforms are listed in this section. Only the parameters included in each file are required for the specified OS.

■ Database Parameters (silent mode) (page 36)

■ Hub Parameters (silent mode) (page 36)

MySQL Parameters (GUI/console)

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 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 Parameters (GUI/console)

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 Parameters (GUI/console)

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 Parameters (GUI/console)

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).
Robot Name	Desired name for the hub robot (default is the name of the server with **robot** 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)	Specify either: ■ No value or the default (**48000**). Port assignments will start at 48000 and increment by 1 until it finds one free, then continue to increment for subsequent assignments. ■ Any available port if you want to specify an initial port for Nimsoft probes. Subsequent assignments will increment from the port you specify.
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 starts with 169.254 (IPv4) or fe80: (IPv6). A warning displays if you do. To proceed using a Link Local address, click the **Allow Link Local Address** box.

Database Parameters (silent)

In the Values column:

- **Bold** text represents actual accepted values that can be entered verbatim.

- *Italic* text represents values you define during installation, such as the Nimsoft domain name.

- Regular text represents values that exist and are specific to your setup, such as a server IP address.

Parameter	Definition	Value
USER_INSTALL_DIR	Target folder for installed files	■ **C:\\Program Files\\Nimsoft** (default for 32-bit Windows) ■ **C:\\Program Files (x86)\\Nimsoft** (default for 64-bit Windows) ■ **/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**
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

Parameter	Definition	Value
USER_INSTALL_DIR	Target folder for installed files	■ **C\:\\Program Files\\Nimsoft** (default for 32-bit Windows) ■ **C\:\\Program Files (x86)\\Nimsoft** (default for 64-bit Windows) ■ **/opt/nimsoft** (Linux/Solaris default) ■ Existing directory ■ *Directory to be created by installer*
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 Parameters (silent)

In the Values column:

- **Bold** text represents actual accepted values that can be entered verbatim.

- *Italic* text represents values you define during installation, such as the Nimsoft domain name.

- Regular text represents values that exist and are specific to your setup, such as a server IP address.

Parameter	Definition	Value
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 – port assignment will start at 48000 and increment 1 until it finds one free, then continue to increment 1 for subsequent assignments
IPV6_ENABLED=0	Enable IPV6	**0** (false, default) **1** (true)
NMSLICENSE	Nimsoft License string	License string provided by Nimsoft Licensing
NMS_PASSWORD	Password created for NMS Administrator account	*User-specified*

Installing in an Active/Passive Microsoft Cluster

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.

Prerequisites

Ensure the following requirements are met before you begin.

Required:

- Administrative access to an active/passive two-node failover cluster

- Shared disk/iSCSI target (typically SAN, NAS or RAID array (in the following procedure this is referred to as S:\, although it could be any drive) *letter.*

- All resources are available to both cluster nodes

- Available IP address for assignment to the virtual NMS service (from network administrator)

Recommended:

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

Note: For database high availability, MS SQL Server is often itself configured to run on an MS Server 2008 cluster. An MS SQL Server database running on a cluster appears to NMS the same as a non-cluster implementation. No special database connection or configuration is required.

Cluster configuration is covered 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**

Installing NMS on the Cluster

In this procedure, the shared disk/iSCSI target (typically a SAN, NAS or RAID array) is referred to as S:\.

Follow these steps:

1. Download the NMS installer to the shared disk (for example S:\).

2. Run the NMS installer on the first system, which is the active node in the cluster (the active node has current control of the S:\ drive). Use one of the Windows installation procedures covered in the section on NMS Installation (page 27), observing these particulars:

   ■ When prompted for an install location, install to a location on the shared drive,such as S:\Nimsoft. Do *not* install to C:\Program Files.

   ■ When prompted to specify the network interface, enter the physical IP address of the system.

   ■ When choosing names for the domain and hub, make note of them, as you will need those at a later point in the procedure.

      Tip: Use a hub name different from the hostname of the node to avoid confusion--both cluster nodes will share this name.

   ■ If the installer warns you that one or more probes did not start, ignore the message.

3. Reboot the first system (active node), which will cause the second system (passive node) to take over and become active.

4. Log into the second system (the new active node) and verify you can access the shared drive (the S:\ drive).

5. Install NMS on this system (now that it is active) using the same install location (in this case S:\Nimsoft) and the same database information. **You must use the same domain and hub names you chose during the first install.** When prompted for an IP address, enter the physical IP address of the second system.

   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 correctly initialized.

6. When installation is complete, reboot the second system and log in to the first system. The first system should regain "active" status due to the reboot of the second, and gain control of the shared drive.

Go on to the next section (page 39) to set up the NMS Robot Watcher Service.

Configuring the Robot Watcher Service

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

Follow these steps:

1. On the active node, launch **Failover Cluster Manager**.

2. Expand the tree in the left frame. Select **Services and applications**, then click on **Configure a Service or Application...** under **Actions** in the right frame.
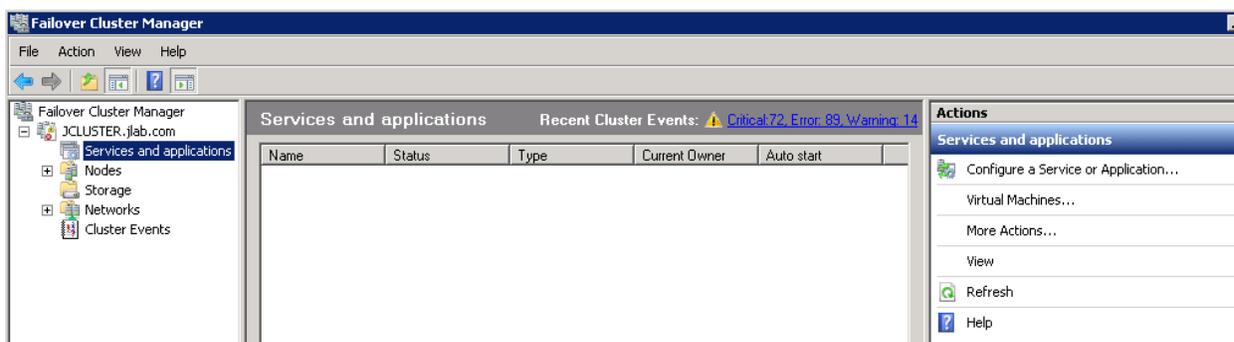
3. On the next screen, choose **Generic Service**, then click **Next**.

   Note: If you receive an error message **The Operation has Failed,** rebooting both cluster nodes may resolve the issue. If you continue to have problems, make sure all latest Windows Updates have been applied to both nodes, and that any anti-virus scanning is disabled.

4. The **High Availbliity Wizard** launches. Select the **NMS Robot Watcher** service, then click **Next**.

5. In the next screen **Client Access Point**, choose a name that the NMS Service will use to register itself on the network.
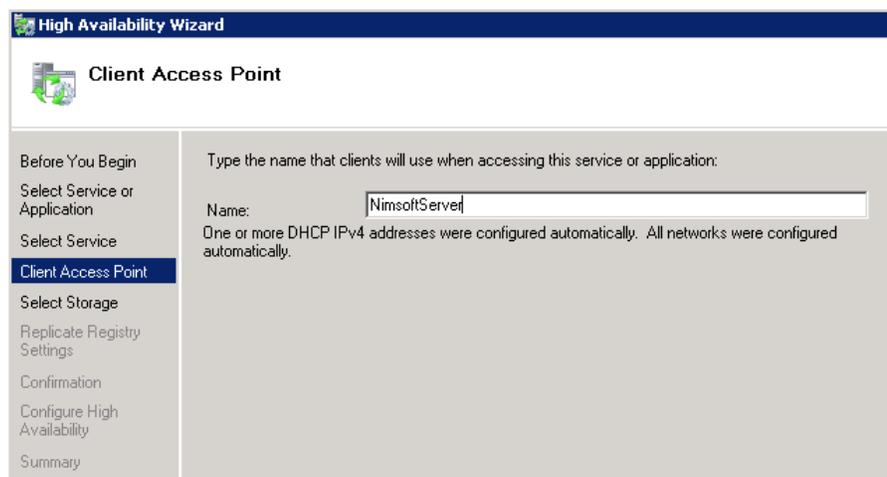
6. If asked to choose an IP address, use the available IP address that was received and approved by your network administrator. In some environments (DHCP), all networking may be configured automatically, and you may not need to enter any IP addresses in this screen.

7. Specify **Storage** for the service--this is the shared drive that NMS is installed on (S:\).

8. The service should be created and brought online with a virtual IP address.

   Be sure to *make a note* of the virtual IP address. You will need it when you configure the NMS robot.

Name	Status	
Disk Drives		
⊞ 💾 Cluster Disk 2	🟢 Online	
Other Resources		
⚙ Nimsoft Robot Watcher Service	🟢 Online	
IP Address: 10.130.228.96	🟢 Online	

Upgrade the Robot

Next, install a special version of the NMS Robot that has been modified to support IP virtualization.

Follow these steps:

1. Login to the active node of the cluster and launch Infrastructure Manager (or Admin Console):

2. Obtain **robot_update 5.70HF1** and import it into the NMS archive.

3. Deploy it to the primary hub.You will see two robots, one for each node of the cluster. Make sure you deploy to the active node's robot.

   Note: The distribution process (distsrv) may report that the deployment was **finished with unknown status**. This is not a problem and can be ignored.

Edit Robot Configuration
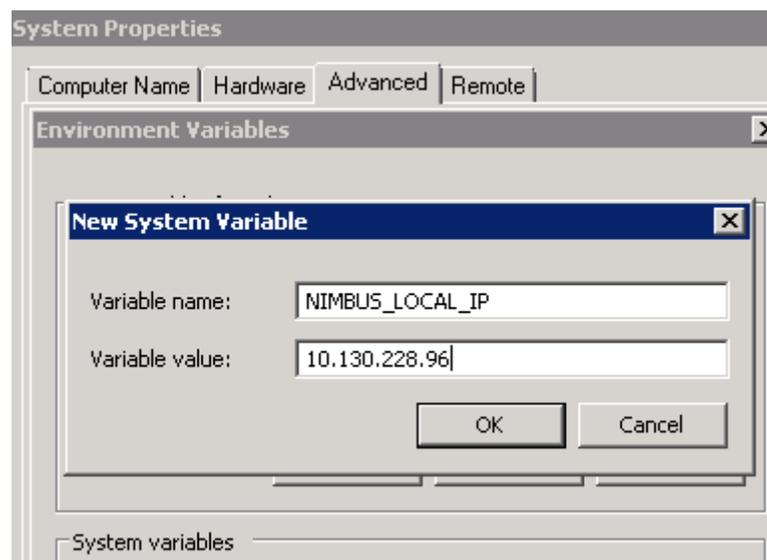
Follow these steps:

Should this be updated to use admin console or IM to do the configuration?

1. Navigate to the location where NMS is installed (S:\Nimsoft) and open the robot directory there.

2. Open the **robot** configuration file in a text editor.

3. Make the following changes. If one or more key-value pairs don't exist, add them.

   ▪ **hubip =<virtual IP address of the NMS service>** (noted in the last step of Configuring the NMS Robot Watcher Service)

   ▪ **robotip=<virtual IP address of the NMS service>** (noted in the last step of Configuring the NMS Robot Watcher Service)

   ▪ **strict_ip_binding=no** (default)

   ▪ **local_ip_validation=no** (default)

Create the NIMBUS_LOCAL_IP Environment Variable

The enhanced version of the robot (with controller 5.70HF1) requires the **NIMBUS_LOCAL_IP** environment variable on *both* nodes of the cluster.

Set the variable value to the virtual IP address of the NMS service (noted in the last step of Configuring the NMS Robot Watcher Service).

Check Dependencies

Follow these steps to restart the Robot Watcher service and check service dependencies:

1. Open the **Failover Cluster Manager** on the active node.

2. Right-click **NMS Robot Watcher** and select **Take this resource offline**. Then immediately right-click the service and choose **Bring this resource online**.

3. Right-click the NMS Robot Watcher service and choose **Properties**.

4. On the **Dependencies** tab, set the dependencies for the NMS Robot Watcher service. The following cluster resources must all be online and available before the NMS Robot Watcher service should start:

   - Cluster shared disk

   - Virtual NMS resource

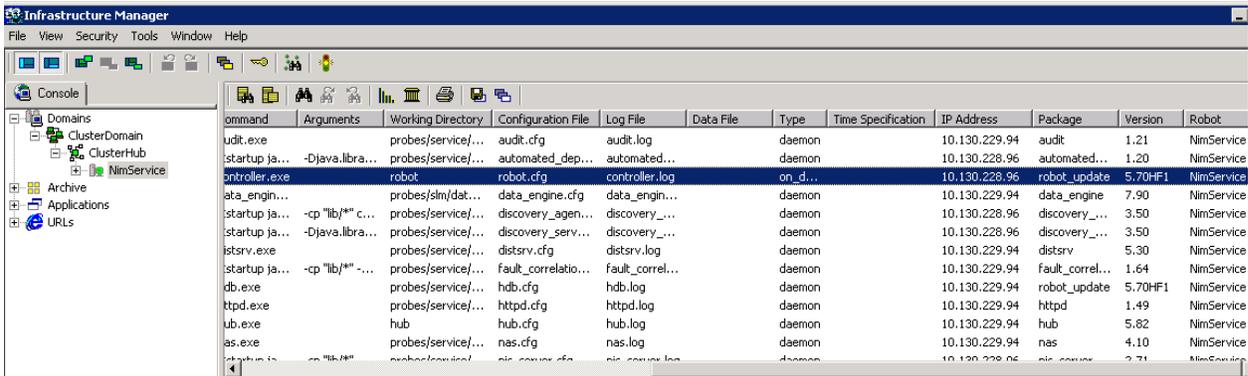   - Virtual IP address assigned to the virtual NMS service

Final Steps

1. Log in to Infrastructure Manager. You will see two robots (one for each node of the cluster). The robot on the active node should be green, the robot on the passive node is likely red.

2. Double-click the controller probe on the active node.

3. Under **Setup Options**, choose **Set Specific Name**. Specify a unique name for the robot.

   Recommendation: Use the same as the NMS Robot Watcher service you set up, rather than the physical hostname.

4. Right-click the robot that is on the second node and select **Remove**. This action:

   - Removes the robot from the hub's list of registered robots

   - Prevents alarms being generated due to its red (passive) state

5. You are left with one robot that represents the cluster. Probes beneath this robot may display in red or show they are security invalid. If so, right-click these probes and choose **Security > Validate**.

   Note: If you are using auto-generated licenses for any components, you must replace these with standard licenses.

Validation and Testing

Validate probe IP address binding by checking the IP Address column in Infrastructure Manager or Admin Console. The controller probe, as well as any Java-based probes, should report their IP address as the virtual IP address of the NMS Service. All other probes will report their IP addresses as the local IP address of the active node.

To test the failover and failback operation of NMS within the cluster, follow these steps:

Note: If you have Infrastructure Manager open on a separate workstation, or Admin Console in a browser window, you can observe the status of the NMS Hub during the failover test.

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

2. Right-click the virtual NMS hub and select **Move the service or application to another node**.
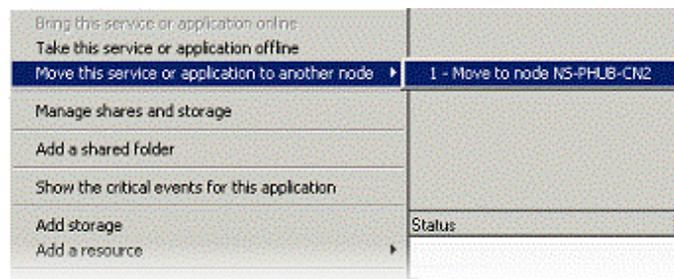
3. Select the other node in the cluster and confirm the operation. As the service moves to the passive node, Infrastructure Manager shows that the hub becomes unavailable by displaying it in red. Failover Cluster Manager shows the status of the cluster as the NMS service moves to the failover node.

4. 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.
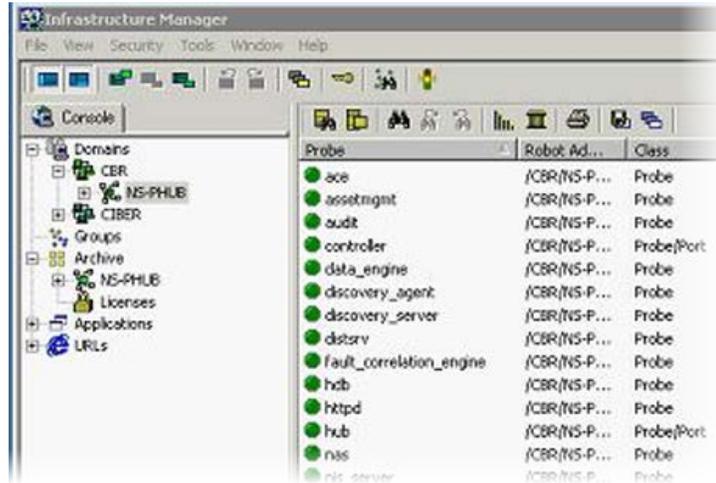
5. Repeat these steps to failback the service to the original node.

Uninstalling NMS

These are the only recommended methods to uninstall NMS.

To uninstall on 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. Some components may be shown as "NM_xxx".

4. Click **Uninstall/Change**, then follow the system prompts.

To uninstall on Linux or Solaris:

1. Go to *<NMS_install_dir>*/NM_Server_installation

   where *<NMS_install_dir>* is the directory where NMS was installed (default is **/opt/nimsoft**).

2. Run the uninstaller. Execute:
   ```
   uninstall -i console
   ```

Chapter 4: Installing Robots and Secondary Hubs

After you install the primary hub, you install:

■ **Secondary hubs.** Most deployments will have at least one additional hub; for load balancing, enterprise deployments can have several to many. Secondary hubs are typically dedicated servers. They are used:

— To provide failover capability if the primary hub is unavailable.

— In enterprise deployments, to host services and management consoles, such as Unified Management Portal (UMP) and Nimsoft Alarm Server (NAS).

— For data collection and dispersion. In an enterprise deployment, tunnels and queues connect secondary hubs to form a hierarchy that securely transports monitoring data to the primary hub.

Important! To enable secondary hubs to communicate on the message bus, you must do the following after installation:

— Set up queues connecting the secondary hubs to the primary hub.

— Set up tunnels between hubs separated by firewalls. This ensures secure communication.

■ **Robots.** Each robot is managed by a hub. The robots, in turn, manage the probes that collect monitoring data and perform other functions.

This section explains how to run the native installers to install robots one at a time (which you might do for the UMP server, which requires a hub or a robot). To install robots in bulk, refer to Deploying Robots in Bulk.

Note: While it is technically possible to have duplicate robot names within a domain, a best practice is to avoid   them. Duplicates can cause problems for the data engine (which puts metric data in the database) and complicate robot management.

This section contains the following topics:

Deployment Models

All software required by client systems resides on the NMS server. Installation packages available on the NMS home 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 home page to the client system, then execute the install packages on the client systems. This model is explained in this section.

- **Push** – An administrator pushes the software from the NMS server to robots either individually or in bulk. This is explained in Bulk Deployment using the Automated Deployment Engine probe (ADE) (page 59).

If you are installing infrastructure on remote sites, you may need to set up tunnels to enable secure communication. The DMZ wizard helps you set up tunnels between hubs.

Installing a Robot on Windows

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

- **Normal** installs a robot on a specific system.

- **Cloud** installs a 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, browse to your NMS web page (http://*<servername_or_server_IP_address>*:8080).

2. In the **Infrastructure Deployment (Installers)** table, click **Windows Robot**, then select **Run**.

3. Follow the prompts to complete the installation. Note the following:

   - For **Normal** installation, you must specify the domain you want the robot to be part of. Check either:

     – a domain (if more than one is available)

     – **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) and system will assign the first probe to port 48000 (or the first available port after that). Alternatively, specify any available port. The port number increments by 1 for each subsequent assignment.

     – Select **Passive mode** if you want the robot to hold its messages until the hub requests them.

When this process is complete:

- The robot probes (controller, spooler and hdb) are installed and activated.

- The robot can communicate with its hub.

- You can begin deploying monitoring probes to the robot.

Installing a Secondary Hub on Windows

Secondary hubs are installed with the **Windows Robot, HUB, Distribution Server** installation package. This package offers three installation modes:

- **Automatic.** This mode searches for a hub on your network. If a hub is:
    - not found, then the robot, hub, and Distribution Server are installed
    - found, only the robot software is installed
- **Custom.** This mode lets you decide which components to install:
    - Robot
    - Hub
    - Distribution server (distsrv)
    - Probe runtime libraries (required to run probes created with the Perl or Visual Basic SDKs)
    - DMZ wizard
- **DMZ**. This mode lets you set up a secure communication tunnel between hubs separated by a firewall, DMZ or both. This process installs a hub, then launches the DMZ wizard, which lets you configure the hub to be either a tunnel server or tunnel client. Note the following:
    - You must install and configure the tunnel server first. This process creates the client certificate, which is required when you set up the tunnel client.
    - After installation, you must set up queues to connect secondary hubs to the primary hub.

See the following sections for instructions on installing with these modes.

- Automatic Installation (page 49)
- Custom Installation (page 49)
- DMZ Installation (page 50)

Note: If NMS software is found on the system, the installer prompts you to either:

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

Automatic Installation

To install in **Automatic** mode, follow these steps:

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

   http://<*server_name_or__IP_address*>:8080

2. In the **Infrastructure Deployment (Installers)** table, download the **Windows Robot, Hub, Distribution Server** package.

3. Launch the **NimBUS Infrastructure** installer.

4. Follow the prompts to complete the installation. Note the following:

   ■ For **Setup Type**, select **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

To install in **Custom** mode, follow these steps.

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

   http://<*server_name_or__IP_address*>:8080

2. In the **Infrastructure Deployment (Installers)** table, download the **Windows Robot, Hub, Distribution Server** package.

3. Launch the **NimBUS Infrastructure** installer.

4. Follow the prompts to complete the installation. Note the following:

   ■ If no hub is found, you must choose an existing domain. All available domains are shown.

   ■ If you are installing 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 **First probe port** field blank (recommended) and system will assign the first probe to port 48000 (or the first available port after that). The port number will increment 1 for each subsequent assignment.

   ■ If you choose to install the DMZ wizard, refer to for details.

DMZ Installation

To install in **DMZ** mode, follow these steps.

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

   http://<*server_name_or__IP_address*>:8080

2. In the **Infrastructure Deployment (Installers)** table, download the **Windows Robot, Hub, Distribution Server** package.

3. Launch the **NimBUS Infrastructure** installer.

4. Follow the prompts to complete the installation. Note the following:

   - 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 can create a name for the hub. If you do not, the computer name will be used by default.

   - 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.

Installing Robots and Secondary Hubs on Linux or Solaris

The Nimsoft Loader utility (**nimldr**) installs robots and secondary hubs on Linux or Solaris. Note the following:

- The system's /etc/hosts file must map 127.0.0.1 to localhost, and its own IP address to its hostname.

- If a robot or hub is installed and running on the system, you must turn off all NMS processes and remove the NMS software. Execute:

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

- You can run nimldr in <u>express mode</u> (page 52) to perform a non-interactive installation.

Running nimldr

Perform these steps on each client system that requires a hub or robot.

1. Verify that the system's /etc/hosts file maps 127.0.0.1 to localhost, and its own IP address to its hostname.

2. Download and unpack the installers:

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

      http://<*server_name_or_IP_address*>:8080

   b. In the **Infrastructure Deployment (Installers)** table, click **UNIX installation utility (nimldr) for all platforms**, and save the archive on the client.

      Note: If the client system does not have a browser, download the installer to another computer and copy it to the client. Make sure the file is named **nimldr.tar.Z**.

   c. Uncompress **nimldr.tar.Z**, then extract the tar file:

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

      This creates the subdirectories that contain nimldr installers for various Linux and Solaris platforms.

3. Enter the appropriate sub-directory for your platform (for example, **LINUX_23_64**).

4. Launch the installer. If the client is on the:

    ■   Same network segment as the primary hub, execute:
        `# ./nimldr`

    ■   Different network segment, execute:
        `# ./nimldr -I <NMS_server_name_or_IP_address>`

5. Answer the installer's questions to complete the installation. The questions asked depend on the type of installation you are performing. For help, see Questions and Answers for the nimldr Installer (page 53).

    Note: Installation progress is logged in the **nimldr.log** file, typically located in **opt/nimsoft/tmp**. To view it, execute:

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

Installation is complete when the installer exits. The hub or robot is in an enabled, or started, status.

Note: Because of the time required for hub authentication and synchronization, it may take several minutes for a new robot to show up under the hub in Infrastructure Manager or Admin Console. Keep in mind that ports 48000 to 48002 need to be open between hubs.

Running nimldr in Express Mode

Express mode lets you run nimldr non-interactively. In this mode, nimldr uses defaults for much of the installation configuration. You provide required information with the following arguments.

Argument	Value
-R	IP address for the robot to bind with
-I	IP address of the Nimsoft hub running a distribution server (distsrv)
-X or **-E**	None, this specifies and express installation
-U	Username for logging into the target system
-S	Password for the target system

For example:
`./nimldr -R10.0.2.11 -I10.0.3.4 -E -Uadministrator -Spassword123`

Questions and Answers for nimldr

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

- In the installer, default answers are in brackets. Press **Enter** to use the default.

- Not all questions are asked; some questions are asked or not depending on your answers to previous questions.

- In the following table, answers in *italics* represent values that you will create.

- 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?	**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
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?	**Archive name**
Enter Nimsoft username and password.	**Username** and **password** for Nimsoft administrator account set up during NMS installation
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)

Question	Answer
Would you like to install the Distribution Server (distsrv)? *distsrv is the Nimsoft probe archive*	**Yes** **No**
Where should the Nimsoft software be installed?	**/opt/nimsoft** (default)
Automatically unregister robot from hub on termination?	**No** (default) **Yes**
Should this robot run in passive mode?	**No** (default; robot sends data to hub) **Yes** (hub must request data from robot)
What is this Nimsoft Domain called?	**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?	**No** (default; installation completes and the installer exits) **Yes** (installation continues)
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** (go to <u>Tunnel Server Questions</u> (page 54)) **No**
Is this hub going to be a tunnel client?	**Yes** (go to <u>Tunnel Client Questions</u> (page 55))

Tunnel Server Questions

The following values are used to generate the tunnel client certificate and save it to a file.

Question	Answer
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 will use this 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 Questions

Question	Answer
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

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

Usage	Flag	Description
All installations	-?	Help
	-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 Omit the flag (recommended) and system will assign the first probe to port 48000 (or the first available port after that), or specify any available port. The port number increments by 1 for each subsequent assignment.
	-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
	-A	set robotip_alias for NAT (special case--use with caution)
	-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)

Usage	Flag	Description
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)
	-U	Username for logging into hub (for archive, etc.)
	-S	Password for logging into hub
	-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, nas, 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	Number of restarts until robot should become active
	-M	DNS name of the system running the hub

Starting, Stopping, and Removing a Robot

Use the appropriate command to confirm that a robot is installed, or to start, stop or remove a robot.

OS Version	Action	Command
Windows	Start	C:\Program Files\Nimsoft\bin\nimbus.exe –start
	Stop	C:\Program Files\Nimsoft\bin\nimbus.exe –stop
	Remove	C:\Program Files\Nimsoft\unins000.exe
Solaris	Confirm	pkginfo nimsoft-robot
	Start	/etc/init.d/nimbus start
	Stop	/etc/init.d/nimbus stop
	Remove	(sudo or su -c) pkgrm nimsoft-robot

Linux, RC-compatible
  RHEL 5.x and prior
  CentOS 5.x and prior
  SUSE
  Debian
	Confirm	rpm -q nimsoft-robot

	Start	/etc/init.d/nimbus start
	Stop	/etc/init.d/nimbus stop
	Remove	rpm -e *RPM_package* (*RPM_package* = robot name minus .rpm)

Linux, Upstart Method
  RHEL 6.0 and newer
  CentOS and newer
  Ubuntu
	Confirm	rpm -q nimsoft-robot

	Start	initctl start nimbus
	Stop	initctl stop nimbus
	Remove	rpm -e *RPM_package* (*RPM_package* = robot name minus .rpm)
Debian Linux	Confirm	dpkg -query -s nimsoft-robot
	Start	/etc/init.d/nimbus start
	Stop	/etc/init.d/nimbus stop
	Remove	(sudo) dpkg -r nimsoft-robot
Ubuntu Linux	Confirm	dpkg -query -s nimsoft-robot
	Start	(sudo, su -c, or root) initctl start nimbus
	Stop	(sudo, su -c, or root) initctl stop nimbus
	Remove	(sudo) dpkg -r nimsoft-robot
AIX	Start	/usr/bin/startsrc –s nimbus
	Stop	/usr/bin/stopsrc –s nimbus
	Remove	/usr/bin/lssrc –s nimbus

Chapter 5: Deploying Robots in Bulk

Bulk robot deployment lets you silently and simultaneously push robot software from the source system to multiple target systems. Two methods are available:

- **Automatic Deployment Engine (ADE) distribution.** The ADE probe is installed with NMS. With this method, you specify robot setup parameters in an XML file (host-profiles.xml). The ADE probe uses this file to deploy robots to remote systems. This mode:

    - Supports public key authentication for SSH

    - Can deploy robots in bulk to systems that might not have a windowing environment

    Note: You can also do ADE bulk deployment in **Unified Service Manager (USM)**, which provides a graphical user interface for specifying ADE parameters. USM is accessed through the Unified Management Portal (UMP). For details, see Automatic Robot Deployment in *User Information* in the UMP online help.

- **NMS robot installers with a third-party deployment tool.** Almost any third-party distribution mechanism (such as Puppet, Chef, Ansible, or Altaris) can be used as long as it can copy a robot installer and answer file to remote targets, then execute the installer.

Before you deploy in bulk, make sure your source and target systems meet the prerequisites (page 60). Then refer to:

- Bulk Deployment with ADE and XML Distribution (page 61)
- Bulk Deployment with a Third-Party Tool (page 66)

Prerequisites for Bulk Deployment

Before performing bulk deployment, ensure the following:

- Your primary hub is the source system.

- Your NMS Archive has the required robot installer archive packages: **robot_exe**, **robot_rpm**, **robot_deb**, **robot_sol**, and **robot_aix**.

- Your target systems are supported. See the Nimsoft Compatibility Support Matrix.

- **For Windows systems:**

  – All appropriate firewall ports are configured to allow remote WMI and DCOM connections, as well as Windows shares. These ports are open and available on a default Microsoft Server installation. ADE deployment is designed to work with settings available in a default install. We recommend you do NOT change the default settings.

  – The source system and target systems are in the same Windows domain, unless the target systems are in the default Windows domain **workgroup**.

  – You have local administrative privileges on the target systems. In addition, the user listed in the *host-profiles.xml* for target Windows systems must have remote access and remote execution privileges. We recommend that this user is an administrator

- **For Linux systems:**

  – The source and target systems must have **/bin/bash**, **ssh** (secure shell), and **glibc**. Most NMS-supported Linux distributions include bash and ssh by default; all versions include glibc by default.

  – You must have access to *root* or a non-administrative account that supports **sudo** to perform per-command, root-level operations.

Bulk Deployment with the ADE Probe

Follow these steps to use the ADE probe and an XML file to deploy robots.

1. Ensure your source and target systems meet the prerequisites (page 60).

2. Create a **host-profiles.xml** file to specify the hosts on which to install robots, and the information needed for installation. The format for this file is described in:

   ■ Example host-profiles.xml (page 63)

   ■ Parameter Values for host-profiles.xml (page 64)

   Note: Specify the Windows hostname in the form you use to log in to the machine.

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

   ■ **Windows** — C:\Program Files (x86)\Nimsoft\probes\service\automated_deployment_engine

   ■ **Linux**, **Solaris**, and **AIX** — /opt/nimsoft/probes/service/automated_deployment_engine

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

After **host-profiles.xml** has processed, ADE renames it to **host-profiles-YYYY-MM-DD_HH-mm-ss** to reflect the date and time of deployment. Renaming the file also ensures that if the ADE probe restarts, deployment does not automatically restart.

Notes:

■ For details on deployment activity, tail the **automated_deployment_engine.log** file.

■ For details about how ADE distributes robots, see How ADE Works (page 62).

■ ADE will not deploy robots from a host-profiles.xml file that has not changed. To restart distribution, remove the date and time from the host-profiles.xml filename, and change its size by a nominal amount (edit the file and add an additional line.) Deployment begins within 30 seconds.

■ ADE 1.30 REST users: If you are using ADE REST calls and your passwords are encrypted, include the following in the authentication portion of the REST XML:

```
"nimcrypt" , "true"
```

How ADE Works

ADE installs robots in groups. The number of CPU cores on the hub where the ADE probe is running determines the group size.

- When a secondary hub is specified under **hubname**:

  a. ADE deploys a copy of itself to the secondary hub.

  b. The primary hub distributes the deployment job to the secondary hub.

  c. The secondary hub carries out the robot deployment.

- If you have more than one ADE probe, deployment tasks are executed in this order:

  a. The primary ADE executes its robot deployment tasks

  b. The primary ADE deploys secondary ADE probes.

  c. The secondary ADE probe(s) execute their robot deployment tasks.

- After deploying a robot, ADE waits for 100 seconds (default) for the robot to start before reporting its status in the history tab. During this time it polls the robot every 25 seconds to see if it is running. If the robot does not respond after 100 seconds, the hub declares the robot inactive.

  To change the delay time, change the value for **verifyDelay** in the ADE probe configuration file **automated_deployment_engine.cfg**. Note that this also changes the polling interval, which is 1/4 of the delay time.

Example host-profiles.xml

Ensure your host-profiles.xml file follows this format.

Note for Linux and Solaris users: The XML field that defines the path to the public key is on the hub system at <rsakeyfile>/path/to/public_key_file</rsakeyfile>.

```
<hosts>
  <host>
    <profile>CentOS</profile>
    <arch>64</arch>
    <hostname>172.19.9.31</hostname>
    <username>root</username>
    <password>root_password</password>
    <domain>AutoEnv</domain>
    <hubip>172.19.4.18</hubip>
    <hub>w2k8-x64-Primaryhub</hub>
    <hubrobotname>w2k8-x64-Primary</hubrobotname>
    <hubport>48002</hubport>
    <robotname>CentOS6-x64</robotname>
    <tempdir>/opt/tmp</tempdir>
  </host>

  <host>
    <profile>Windows</profile>
    <arch>32</arch>
    <hostname>172.19.9.63</hostname>
    <username>Administrator</username>
    <password>admin_password</password>
    <domain>AutoEnv</domain>
    <hubip>172.19.4.18</hubip>
    <hub>w2k8-x64-Primaryhub</hub>
    <hubrobotname>w2k8-x64-Primary</hubrobotname>
    <hubport>48002</hubport>
    <robotname>w2k8-x86</robotname>
    <tempdir>c:\tmp\supertmp</tempdir>
  </host>
</hosts>
```

Parameter Values for host-profiles.xml

Create your host-profiles.xml file with these values. The only values that are case-sensitive are the names of the Nimsoft domain, hub and robot.

Parameter	Value
profile	Operating system on target system: ■ **windows** ■ **linux** (legacy support for previous RPM packages) ■ **rhel** (Red Hat Enterprise Linux0 ■ **centos** ■ **suse** (SUSE Linux Enterprise Server) ■ **opensuse** ■ **ubuntu** ■ **debian** ■ **solaris** ■ **aix** ■ **zlinux**
arch	Architecture of target system: ■ **32** (32-bit) ■ **64** (64-bit) ■ **ppc** (AIX 32-bit) ■ **ppc64** (AIX 64-bit) ■ **sparcv9** (Solaris) ■ **s390x** (zLinux)
hostname	Target system **hostname** or **IP address**. *On Windows, use the format you use to log into the system.*
username	Any account on the target that has administrative permissions or supports **sudo** for root-level permission .
password	Account password. *See the optional rsakeyfile parameter.*
domain	Domain name (case-sensitive).
hubip	IP address of the hub to which this robot will belong.
hub	Name of the hub to which this robot will belong (case-sensitive).
hubrobotname	Name of the robot on the hub where you will run ADE (case-sensitive, typically the primary hub).
hubport	Port that the hub listens on; specified during hub setup (default is 48002).

The following parameters are optional. Do not include optional parameters without providing a value.

Parameter	Value
ip_version *optional*	IP address schema version: ■ **IPv4** ■ **IPv6**
rsakeyfile *optional; key files with passphrases are not supported*	Path to RSA public key certificate on the system hosting ADE in this format: <rsakeyfile> */path/to/xml/on/local/system* </rsakeyfile>
sudo_password *optional*	Password string for sudo. **Note:** Enables use of **sudo** over ssh during install. ssh password still required. Not applicable to root users.
installdir *optional*	Path to installation directory on the target system. For example: ■ **C:\Users** (Windows) ■ **/usr/local** (Linux or Solaris) **Note:** Linux and Solaris installers put installation files in a nimsoft/install directory. Windows installers put them in an install folder. On Windows, you may want to include *Nimsoft* in the **install_dir** path (C:\Users*user_name*\Nimsoft) to organize the robot install files.
tempdir *optional*	Desired path for a temporary directory on the target system. For example: ■ **C:\tmp\supertmp** (Windows; path may not include spaces or double back-slashes) ■ **/opt/tmp** (Linux or Solaris)
origin *optional*	Origin for messages. Typically set to the name of a hub in the Nimsoft domain, a Nimsoft robot, a company name, etc.
robotname *optional*	Name to be assigned to the deployed robot. Default is the hostname of the system to which the robot is deployed.

Bulk Deployment with a Third-Party Tool

Many IT environments already have a mass software deployment mechanism in place (such as Puppet and Yum on Linux, or Altiris on Windows). Almost any third-party distribution mechanism can be used as long as it can:

- Copy a robot installer to a remote system

- Copy an answer file

- Execute the installer

32-bit and 64-bit installers are provided for the following operating systems:

- Windows

- Linux (SLES, OpenSUSE and RedHat)

- Ubuntu 10.04 and 12.04

- Debian 6 and 7

- Solaris (Intel/AMD and sparcv9)

- AIX 5, 6 and 7

Before you deploy in bulk, make sure your source and target systems meet the prerequisites (page 60).

Note: The robot installers are designed to execute silently and require an answer file. For manual installation of a robot without need for an answer file, refer to Installing Robots and Secondary Hubs (page 45).

Deploying to Windows

Your third-party deployment tool must perform the following actions.

1. Copy the appropriate installer to any folder on the target system. The Windows installers for automatic deployment are:

    nimsoft-robot.exe
    nimsoft-robot-x64.exe

    Note: The NMS robot_MSI package has been deprecated.

2. Copy the **nms-robot-vars.cfg** (page 71) answer file to the same folder.

3. Execute:

    `<EXE_package>.exe /VERYSILENT /SUPPRESSMSGBOXES /NORESTART`

    This installs the files in C:\Program Files Nimsoft. You can append optional arguments (enclosed in square brackets) to the command:

    ■ To specify the installation folder:

    `[ /DIR="c:\path\to\install" ]`

    ■ To specify the log file:

    `[ /LOG="name_of_install_log.txt" ]`

    Note: The folder and file name must be enclosed in quotation marks.

After installation, the robots start automatically.

Deploying to Linux

Your third-party deployment tool must perform the following actions.

Note: If you are not using root access, use either **sudo <command>** *or* **su -c "<command>"**. You can also use su to get the root shell, then execute the command.

1. Copy the appropriate installer to **/opt** on the target system. The Linux installers are:

    ■   **SUSE**, **SLES**, or **RHEL**:
        nimsoft-robot.rpm
        nimsoft-robot-x64.rpm

    ■   **Debian**:
        nimsoft-robot+debian_amd64.deb
        nimsoft-robot+debian_i386.deb

    ■   **Ubuntu**:
        nimsoft-robot+ubuntu_amd64.deb
        nimsoft-robot+ubuntu_i386.deb

2. Copy the **nms-robot-vars.cfg** (page 71) answer file to **/opt**.

3. Execute the appropriate command.

    ■   **RedHat**, **SUSE**, or **CentOS**:To install in /opt/nimsoft, execute:

        rpm -ivh nimsoft-robot.<arch>.rpm

    where *<arch>* is the architecture of the target system (**i386** or **amd64**).

    To specify the installation directory, execute:

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

    where *<directory>* is the full path/name of the installation 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, installation is complete.

    ■   **Debian** or **Ubuntu**:

        (sudo or root user) dpkg -i nimsoft-robot+<OS>_<arch>.deb

    where *<OS>* is **debian** or **ubuntu** and *<arch>* is the architecture of the target system (**i386** or **amd64**).

4. After the installer exits, execute the following to configure the robot:
   ```
   cd /opt/nimsoft/install
   (sudo, su -c, or root user) bash RobotConfigurer.sh
   ```

5. Execute the following to start the robot:

   ■ **RedHat**, **SUSE**, or **CentOS**:
     ```
     /etc/init.d/nimbus start
     ```

   ■ **Debian**:
     ```
     /etc/init.d/nimbus start
     ```

   ■ **Ubuntu**:
     ```
     (sudo, su -c, or root user) initctl start nimbus
     ```

Installation is complete.

Deploying to Solaris

Your third-party deployment tool must perform the following actions.

1. Copy the appropriate installer to **/opt** on the target system. The Solaris installers are:

   nimsoft-robot-i386.gz
   nimsoft-robot-amd64.gz
   nimsoft-robot-sparcv9.gz

2. Copy the **nms-robot-vars.cfg** (page 71) answer file to **/opt**.

3. Execute the following:
   ```
   gunzip nimsoft-robot-<arch>.gz
   (sudo or su -c) pkgadd -d /opt/nimsoft-robot-<arch>
   ```

   where *<arch>* is the architecture of the target system (**i386**, **amd64**, or **sparcv9**).

4. After the installer exits, execute the following (under sudo, su -c, or as root user) to configure and start the robot:
   ```
   cd /opt/nimsoft/install
   bash RobotConfigurer.sh
   /etc/init.d/nimbus start
   ```

Installation is complete. To view status of the robot, ssh to the machine, then execute:
   ```
   ps -ef | grep nimbus
   ```

Deploying to AIX

Your third-party deployment tool must perform the following actions.

1. Copy the appropriate installer to the target system:

   nimsoft-robot.aix<*version*>**.ppc.rpm** *(32-bit systems)*
   nimsoft-robot.aix<*version*>**.ppc64.rpm** *(64-bit systems)*

   where <*version*> corresponds to your AIX version. To determine whether the target's kernel is 32-bit or 64-bit, execute:

   ```
   # getconf KERNEL_BITMODE
   ```

2. Copy the **nms-robot-vars.cfg** (page 71) answer file to **/opt**.

3. Execute:

   ```
   rpm -ivh nimsoft-robot.aix<version>.<arch>.rpm
   ```

   where <*version*> is the AIX version and <*arch*> is **ppc** or **ppc64**.

   To specify the installation directory, execute:

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

   where <*directory*> is the full path/name of the installation directory.

   Note: The **rpm** flags function as follows:

   -i installs the software packaged

   -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.

4. After the installer exits, execute the following (as *sudo*, *su -c*, or *root*) to configure the robot:

   ```
   cd /opt/nimsoft/install

   bash RobotConfigurer.sh
   ```

5. Enable the Nimbus service. Execute:

   ```
   /opt/nimsoft/install/service-ctrl.sh
   ```

6. Start the robot. Execute:

   ```
   /usr/bin/startsrc -s nimbus
   ```

Note: As of the release of robot 7.6 (controller, hdb, and spooler probes), cdm 4.9, logmon 3.8, and processes 3.4, these components have been tested and recognized for use in a VIOS environment. Installation and administration for these components is the same as on a non-VIOS AIX system.

Answer File Syntax and Parameters

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:

- There are no spaces between parameter and value.

- All text within brackets must be replaced with actual values. For example:

  ```
  domain=YourNimsoftNMSdom
  ```

- 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.

- A best practice is to prepare a simple answer file with only *required* fields during initial robot deployment, and add optional fields later. Bulk changes to robot configuration are quickly accomplished using drag and drop in Infrastructure Manager.

Parameter	Definition	Example value
domain	NMS Domain	HOST_ABC_DOM
hub	NMS 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 on the hub	HOST_ABC_ROBOT
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_MNO
first_probe_port *optional*	Port on source system to be used by the first probe	48000
origin *optional*	Desired origin value	HUBNAME

Note: For a description of additional robot configuration parameters (those that are set using the Controller probe GUI), refer to the Controller probe online help.

Chapter 6: Installing and Accessing Management Consoles

Management consoles let you manage your NMS components and control and view the collected data. Three consoles are available:

- **Admin Console** (browser-based) also lets you configure your infrastructure and view monitoring information. Admin Console is installed on the primary hub. Access it from your NMS home page: http://*<server_name_or_IP_address>*:8080

- **Infrastructure Manager** (a Windows application) enables you to configure your NMS infrastructure and view monitoring information. Infrastructure Manager is a legacy application whose functionality has been and will continue to be implemented in Admin Console. At the present, some configuration tasks can only be accomplished using Infrastructure Manager.

  On Windows systems, Infrastructure Manager is automatically installed when you install the primary hub. If your primary hub server is Linux or Solaris, or if you want to run the application from a computer other than the primary hub, you can install it separately. See Installing Infrastructure Manager (page 74) for details.

  Some users prefer to use Infrastructure Manager to manage hubs and robots, and to use Admin Console to manage monitoring probes.

- **Unified Management Portal** (browser-based; referred to as UMP) is an extensible portal that offers a broad range of features and is used primarily to display and view monitoring data. UMP is installed after NMS installation is complete. See the *UMP Installation Guide* available from the documentation library or the **Downloads** tab at Nimsoft Technical Support.

Installing Infrastructure Manager

Follow these steps:

1. On the client computer where you want to install Infrastructure Manager, browse to your NMS web page (http://*<servername_or_server_IP_address>*:8080).

2. Under **Management (Admin Console)**, click **Legacy Infrastructure Manager** to download the installer file, then open it and select **Run**.

3. Follow the prompts to complete the installation. Note that:

   ■ You must select which components to install: Infrastructure Manager and/or Alarm SubConsole. Normally both should be installed.

   ■ If you chose to install the Microsoft SOAP Toolkit, the toolkit setup wizard launches.

4. Verify that the installation was successful by launching the console:

   ■ **Start > Programs > Monitoring > Infrastructure Manager**

Note: As an alternative to installing Infrastructure Manager, you can also access Admin Console, a browser-based management console that provides many of the features of Infrastructure Manager. The link to Admin Console is available on the NMS web page (http://*<servername_or_server_IP_address>*:8080) under **Management (Admin Console)**.

Appendix A: Modifications to Windows Systems

When you install NMS hubs and robots, the following components are installed on your system. To see which version of NMS is installed, go to **Control Panel > Programs and Features**.

Component	Install status
.../Nimsoft	NMS product directory. Default is **C:\Program Files\Nimsoft Monitoring**.
msvcrt.dll (*Microsoft C library in the 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 sections store variables used internally by NMS.
	   HKEY_LOCAL_MACHINE\Software\Nimsoft Software
	   HKEY_LOCAL_MACHINE\Software\Nimsoft Software AS
	   HKEY_LOCAL_MACHINE\Software\Nimsoft Corporation

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

If you select a VB runtime during installation, the following components are installed.

Component	Status
atl.dll (*Windows system directory*) sycfilt.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	Installed if nonexistent; updated if the existing version is old.