Contents

Chapter 1: Introduction ................................................................. 7
  Installation Overview ...................................................................................... 8
  Local Deployment .............................................................................................. 9
  Local and Remote Deployment ........................................................................ 10
  Working with Firewalls and DMZs ................................................................. 11
  Security ........................................................................................................... 11
  Tunnel Setup Overview ................................................................................... 12
  Required Ports for SSL Tunnels .................................................................... 12

Chapter 2: Preparing the Servers ......................................................... 13
  Determine Your Deployment Size .................................................................... 14
  Set up the NMS server (hosts your primary hub) ........................................... 15
    Oracle Instant Client Installation ................................................................. 15
  Set up the NIS server (hosts the database) .................................................... 16
    SQL Server Installation and Configuration .................................................. 17
    MySQL Installation and Configuration ........................................................ 18
    Oracle Installation and Configuration ........................................................ 20
  Set up the UMP server (hosts your management portal) ............................... 22
  Server Setup Checklist ................................................................................... 23

Chapter 3: Installing NMS (the Primary Hub) ........................................ 25
  Installing in GUI Mode .................................................................................... 26
  Installing in Console Mode on Linux or Solaris ............................................. 27
  Installing in Silent Mode .................................................................................. 28
  Installation Parameters .................................................................................... 29
    MySQL Database Parameters (GUI and console mode) ............................. 29
    SQL Server Database Parameters (GUI and console mode) ....................... 30
    Oracle Database Parameters (GUI and console mode) ............................... 30
    Hub Parameters (GUI and console mode) .................................................... 31
    Database Parameters (silent mode) ............................................................ 32
    Hub Parameters (silent mode) .................................................................... 34
  Uninstalling NMS ............................................................................................. 35

Chapter 4: Installing Robots and Secondary Hubs ................................. 37
  Client Installation Overview ........................................................................... 38

Uninstalling NMS ............................................................................................ 35
Chapter 1: Introduction

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

- **Introduction** (see page 7) provides an overview of the installation phases.
- **Preparing the Servers** (see page 13) explains how to set up the servers that will host your NMS primary hub, the database, and the Unified Management Portal software.
- **NMS Installation** (see page 25) explains how to set up your primary hub.
- **Nimsoft Client Installation** (see page 37) details how to deploy the hub and robot software onto the systems you want to monitor.
- Other sections cover bulk robot installation (see page 53) (using the ADE probe to distribute robot installer packages), installation in a Microsoft Cluster, and MySQL installation on Windows (see page 75).

**Notes:** Nimsoft Unified Management Portal (UMP) and Unified Reporter (UR) have their own installation guides. If you are upgrading NMS, see the NMS 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 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 Nimsoft Monitor Server (NMS).** This process installs the foundation for Nimsoft Monitor, which consists of the:
   - Primary hub, which includes a robot and service probes
   - Nimsoft message bus, which enables communication between the hub, its robots and probes and between the hub and the database
   - NMS 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
   - Nimsoft Administrator account on the primary hub server and database server

3. **Installing secondary hubs (optional) and robots.** These elements create the Nimsoft infrastructure that will manage the monitoring probes, collect their data, and route it to the primary hub.

   You can install Nimsoft 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** (see page 10)
- **Local and Remote Deployment** (see page 10)
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 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 (see page 40)
  - Installing Infrastructure on Linux or Solaris Clients (see page 43)
- **On existing hubs after installation** by configuring the hubs. This can be done in either **Admin Console**, the Nimsoft web-based management console, or **Infrastructure Manager**, the Nimsoft 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 NMS web page.

The following illustration shows the components installed and the ports that need to be opened in a scenario with a DMZ and two firewalls.
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 to keep track of information and requirements as you go through the process of setting up your servers.
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.

<table>
<thead>
<tr>
<th></th>
<th>Hubs</th>
<th>Robots</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>1</td>
<td>100</td>
</tr>
<tr>
<td>Medium</td>
<td>5</td>
<td>250</td>
</tr>
<tr>
<td>Large</td>
<td>20</td>
<td>500</td>
</tr>
<tr>
<td>Major</td>
<td>50</td>
<td>1000</td>
</tr>
</tbody>
</table>

Plan to deploy more than 50 hubs and 1000 robots? Use the specifications for a major deployment as a starting point, and consult with Nimsoft professional services or a Nimsoft 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 Nimsoft sales representative if you have questions about your hardware needs.
Set up the NMS server (hosts your primary hub)

Your NMS server must meet the following requirements. For supported software versions, see the Nimsoft Monitor Compatibility Matrix:


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

**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.

**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.


**Oracle Instant Client Installation**

1. Go to [www.oracle.com](http://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 (hosts the database)

Your NIS server must meet the following requirements. For supported software versions, see the Nimsoft Monitor Compatibility Matrix:

<table>
<thead>
<tr>
<th>Deployment</th>
<th>Processor</th>
<th>Memory</th>
<th>Storage recommendations</th>
<th>Software</th>
</tr>
</thead>
</table>
| 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 | ■ 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 |
| Large      | Two quad-core | 12 to 18 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 |
| Major      | Two quad- or eight-core | 18 to 24 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 |

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
- MySQL installation and configuration
- Oracle installation and configuration (see page 20)

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


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 Nimsoft 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.

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).

Your NIS server is ready.

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

- Specify the following options to the SQL Server Express setup program:
  SAPWD=<password> SECURITYMODE=SQL DISABLENETWORKPROTOCOLS=0
- Use this format when specifying the server name:
  <server_name>\SQLEXPRESS
- Use port 1433 (the default) when you install NMS.
MySQL Installation and Configuration

For additional instructions on performing these steps, go to dev.mysql.com/doc http://dev.mysql.com/doc.


2. Install the software.

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.

      Your NIS server is ready.
Set up the NIS server (hosts the database)

Oracle Installation and Configuration

1. Install the software:
   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 http://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:

```sql
create user <db_owner> IDENTIFIED BY <owner_password> DEFAULT
TABLESPACE <ts_name>;
grant unlimited tablespace to <ts_name>;
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
(0x00007f6030b3000)
libd1.so.2 => /lib64/libd1.so.2 (0x00007f602e000)
libm.so.6 => /lib64/libm.so.6 (0x00007f6025000)
libpthread.so.0 => /lib64/libpthread.so.0 (0x00007f6023000)
libc.so.6 => /lib64/libc.so.6 (0x00007f6020000)
libnnz11.so => /root/instantclient_11_1/libnnz11.so
(0x00007f6020000)
libaio.so.1 => /lib64/libaio.so.1 (0x00007f6020000)
libnnz11.so => /root/instantclient_11_1/libnnz11.so
(0x00007f6020000)
```

Your NIS server is ready.
Set up the UMP server (hosts your management portal)

Your UMP server must meet the following requirements. For supported software versions, see the Nimsoft Monitor Compatibility Matrix:

See the UMP Installation Guide for installation instructions.

<table>
<thead>
<tr>
<th>Deployment</th>
<th>Processor</th>
<th>Memory</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>Install on the NMS server.</td>
<td>64-bit XEON-class, 2.0 GHz or better</td>
<td>Supported version of Windows, Linux or Solaris</td>
</tr>
<tr>
<td>Medium</td>
<td>One quad-core</td>
<td>4 to 8 GB</td>
<td>Linux and Solaris: minimum 4 GB swap space (6 GB recommended)</td>
</tr>
<tr>
<td>Large</td>
<td>Two quad-core</td>
<td>8 to 12 GB</td>
<td>Linux: standard C++ library</td>
</tr>
<tr>
<td>Major</td>
<td>Two quad-core</td>
<td>16 GB</td>
<td></td>
</tr>
</tbody>
</table>

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

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.

<table>
<thead>
<tr>
<th>Deployment size</th>
<th>□ Small □ Medium □ Large □ Major</th>
</tr>
</thead>
</table>
| **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 NMS (Primary Hub)

The NMS installer can be run in three modes:

- **Graphical user interface** (GUI) mode on Windows, Linux and Solaris
- **Console mode** on Linux and Solaris
- **Silent mode** on Windows, Linux and Solaris (you specify installation parameter values in a file that is used to complete the installation)

If you are installing on a Microsoft high-availability platform, refer to *Installing NMS in an Active/Passive Microsoft Cluster* (see page 67).

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

- **To upgrade an existing installation,** see the *NMS Release Notes and Upgrade Guide* available from **Downloads at support.nimsoft.com.**
- **To reinstall,** uninstall the prior version as explained in *Uninstalling NMS* (see page 35), 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 Nimsoft 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 (see page 29)
     - SQL Server Database Parameters (see page 30)
     - Oracle Database Parameters (see page 30)
     - Hub Configuration Values (see page 31)
   - 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.

NMS installation is complete. You are ready to deploy and install Nimsoft Monitor infrastructure on client systems.
Installing in Console Mode on 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 Nimsoft 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** (see page 29)
     - **SQL Server Database Parameters** (see page 30)
     - **Oracle Database Parameters** (see page 30)
     - **Hub Configuration Values** (see page 31)
   - 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.

NMS installation is complete. You are ready to deploy and install Nimsoft Monitor infrastructure on client systems.

NMS launches. If it does not, execute:
```
  cd /etc/init.d
  nimbus start
```
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 CA Nimsoft Monitor, click the link for the current version of Nimsoft 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:
   ```bash
tail -f /tmp/ia/iaoutput.txt
```

7. NMS launches. If for some reason it does not, execute:
   - Windows: `net start Nimsoft 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 (see page 37) to deploy and install Nimsoft infrastructure on client systems.
Installation 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)** (see page 30)
- **SQL Server Database Parameters (GUI and console mode)** (see page 30)
- **Oracle Database Parameters (GUI and console mode)** (see page 30)
- **Hub Parameters (GUI and console mode)** (see page 31)

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)** (see page 34)
- **Hub Parameters (silent mode)** (see page 34)

MySQL Database Parameters (GUI and console mode)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Server</td>
<td>Database server IP address</td>
</tr>
<tr>
<td>Database Name</td>
<td>Desired name (new) or actual name (existing)</td>
</tr>
<tr>
<td>Database Port</td>
<td>Database server port (typically 3306)</td>
</tr>
<tr>
<td>Database Administrator Password</td>
<td>Either:</td>
</tr>
<tr>
<td></td>
<td>- Use the MySQL administrative account (root). If you are creating a new database, enter the desired_password for the root account to be created.</td>
</tr>
<tr>
<td></td>
<td>- Use an account other than root by checking <strong>Nimsoft SLM Database User Account</strong>. 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).</td>
</tr>
</tbody>
</table>
**SQL Server Database Parameters (GUI and console mode)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Server</td>
<td>■ Database server hostname or IP address</td>
</tr>
<tr>
<td></td>
<td>■ Hostname\instance_name if you have a named instance on a standard port (i.e. 1433)</td>
</tr>
<tr>
<td></td>
<td>■ Hostname if you have a named instance on a <strong>non</strong>-standard port</td>
</tr>
<tr>
<td>Database Name</td>
<td>Desired name (new) or actual name (existing)</td>
</tr>
<tr>
<td>Database Port</td>
<td>Database server port (typically 1433)</td>
</tr>
<tr>
<td>Database User</td>
<td>Database administrative account (root)</td>
</tr>
<tr>
<td>Database Password</td>
<td>Password for database administrator account or desired password if the account is to be created</td>
</tr>
</tbody>
</table>

**Oracle Database Parameters (GUI and console mode)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Server</td>
<td>Database server IP address</td>
</tr>
<tr>
<td>Service Name</td>
<td>Desired database name (new) or actual name (existing)</td>
</tr>
<tr>
<td>Database Port</td>
<td>Database server port (typically 1521)</td>
</tr>
<tr>
<td>SYS Password</td>
<td>Password for the server system administrator account</td>
</tr>
<tr>
<td>Nimsoft DB User</td>
<td>Desired name for the Nimsoft database administrator account, which will be created by the installer</td>
</tr>
<tr>
<td>Nimsoft DB Password</td>
<td>Desired password for the Nimsoft database administrator</td>
</tr>
<tr>
<td>Tablespace Name</td>
<td>Desired name (new) or actual name (existing)</td>
</tr>
<tr>
<td>Tablespace Location</td>
<td>Desired location or leave blank to use the default (new)</td>
</tr>
<tr>
<td>Database Size</td>
<td>Desired size (new)</td>
</tr>
<tr>
<td>Auto Extend Size</td>
<td>Desired size or leave blank to use the default</td>
</tr>
<tr>
<td>Maximum Size</td>
<td>Desired size or leave blank to use the default</td>
</tr>
</tbody>
</table>
## Hub Parameters (GUI and console mode)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub Domain</td>
<td>Desired name for this NMS domain (default is the name of the server with <strong>dom</strong> appended).</td>
</tr>
<tr>
<td>Hub Name</td>
<td>Desired name for this hub (default is the name of the server with <strong>hub</strong> appended).</td>
</tr>
<tr>
<td>Robot Name</td>
<td>Desired name for the hub robot (default is the name of the server with <strong>robot</strong> appended).</td>
</tr>
<tr>
<td>Password</td>
<td>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.</td>
</tr>
<tr>
<td>First Probe Port</td>
<td>Use the default (48000) and let the system assign ports as needed unless you have a reason to specify an initial port for Nimsoft probes.</td>
</tr>
<tr>
<td>(optional)</td>
<td></td>
</tr>
<tr>
<td>License</td>
<td>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).</td>
</tr>
</tbody>
</table>
| Select IP for Hub | The installer displays all network interfaces attached to the computer. Select the IP address you want to use for NMS traffic.  
**Note:** Unless you have a specific reason to do so, do not choose a Link Local address, which is an address that starts with 169.254 (IPv4) or fe80: (IPv6). A warning displays if you do. If you want to proceed using a Link Local address, click the Allow Link Local Address box. |
Database Parameters (silent mode)

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_INSTALL_DIR</td>
<td>Target folder for installed files</td>
<td>■ C:\Program Files\Nimsoft (default for 32-bit Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ C:\Program Files (x86)\Nimsoft</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ /opt/nimsoft (Linux/Solaris default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Existing directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Directory to be created by installer</td>
</tr>
<tr>
<td>NIMDBCARECREATE</td>
<td>Create database?</td>
<td>■ true (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ false</td>
</tr>
<tr>
<td>NIMDBTYPE</td>
<td>Database Type</td>
<td>■ mysql, oracle or mssql (defaults)</td>
</tr>
<tr>
<td>MSSQLAUTHTYPE</td>
<td>Microsoft SQL Authentication Type</td>
<td>■ sql (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ trusted</td>
</tr>
<tr>
<td>DB_SERVER</td>
<td>Database server hostname or IP address</td>
<td>■ Hostname or IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Hostname\instance_name if you have a named instance on a standard port (i.e. 1433)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Hostname if you have a named instance on a non-standard port</td>
</tr>
<tr>
<td>DB_PORT</td>
<td>Database port</td>
<td>■ 3306 (MySQL default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 1521 (Oracle default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 1433 (MSSQL default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ User-specified port</td>
</tr>
</tbody>
</table>
### Installation Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>USER_INSTALL_DIR</strong></td>
<td>Target folder for installed files</td>
<td>■ C:\Program Files\Nimsoft (default for 32-bit Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ C:\Program Files (x86)\Nimsoft (default for 64-bit Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ /opt/nimsoft (Linux/Solaris default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Existing directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <em>Directory to be created by installer</em></td>
</tr>
<tr>
<td><strong>NIMDBNAME</strong></td>
<td>Database name</td>
<td>■ NimsoftSLM (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Desired database name (new database)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Actual database name (existing database)</td>
</tr>
<tr>
<td><strong>DB_ADMIN_USER</strong></td>
<td>Nimsoft database administrator username</td>
<td>■ Sys (required user for Oracle)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ DB admin username (MySQL and SQL server)</td>
</tr>
<tr>
<td><strong>DB_ADMIN_PASS</strong></td>
<td>Database administrator password</td>
<td>■ SYS password (Oracle)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Actual DB admin password (MySQL and SQL server)</td>
</tr>
<tr>
<td><strong>NIMDB_USER</strong></td>
<td>Nimsoft database user account</td>
<td>■ Nimsoft (default for new DB; required on Oracle)</td>
</tr>
<tr>
<td>(Oracle: required</td>
<td></td>
<td>■ root (optional for MySQL)</td>
</tr>
<tr>
<td>MySQL: optional)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NIMDB_PASS</strong></td>
<td>Nimsoft database account password</td>
<td>■ SID (Oracle)</td>
</tr>
<tr>
<td>(Oracle: required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MySQL: optional)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DROP_COLUMNS</strong></td>
<td>Drop the <em>inserttime</em> column from the database</td>
<td>■ 1 (drop columns, default)</td>
</tr>
<tr>
<td>(MySQL and Oracle)</td>
<td>schema</td>
<td>■ 2 (keep but do not create in new table)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 3 (keep and create in new table)</td>
</tr>
</tbody>
</table>
Hub Parameters (silent mode)

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMSHUB</td>
<td>Hostname or IP address for the primary hub</td>
<td>Hostname or IP address</td>
</tr>
<tr>
<td>NMSDOMAIN</td>
<td>NMS domain name</td>
<td>Actual domain name (if it exists)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User-specified domain name (if being created)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;no value&gt; (default domain name is the server name with dom appended)</td>
</tr>
<tr>
<td>NMSNETWORKIP</td>
<td>NMS Network Interface IP</td>
<td>IP address of primary hub NIC</td>
</tr>
<tr>
<td>NMS_PROBE_PORT</td>
<td>NMS first probe port</td>
<td>48000 (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any available port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;no value&gt; (probe ports will be auto assigned)</td>
</tr>
<tr>
<td>IPV6_ENABLED=0</td>
<td>Enable IPV6</td>
<td>0 (false, default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 (true)</td>
</tr>
<tr>
<td>NMSLICENSE</td>
<td>Nimsoft License string</td>
<td>License string provided by Nimsoft Licensing</td>
</tr>
<tr>
<td>NMS_PASSWORD</td>
<td>Password created for NMS Administrator account</td>
<td>User-specified</td>
</tr>
</tbody>
</table>
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:
   \( \text{uninstall} -i \text{console} \)
Chapter 4: Installing Robots and Secondary Hubs

After you install NMS, you install Nimsoft infrastructure components on client systems in your managed environment. In addition to the primary hub and database, Nimsoft infrastructure includes:

- **Secondary hubs.** Most deployments will have at least one additional hub; for load balancing, enterprise deployments can have several to many. Secondary hubs are used:
  - To provide failover capability if the primary hub is unavailable.
  - For Nimsoft United Management Portal (UMP) and Nimsoft Alarm Server (NAS).
  - For data collection and dispersion. In an enterprise deployment, tunnels and queues can connect secondary hubs to form a hierarchy that securely transports monitoring data to the primary hub.

Secondary hubs are typically dedicated servers.

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 contains the following topics:

- Client Installation Overview (see page 38)
- Installing a Robot on Windows (see page 39)
- Installing a Secondary Hub on Windows (see page 40)
- Installing Robots and Secondary Hubs on Linux or Solaris (see page 43)
- Removing a Robot (see page 50)
Client Installation Overview

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

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

- **Pull** – Administrators and users download the install packages from the NMS web page to the client system, then execute the install packages on the client systems. This model is explained in this chapter.

- **Push** – An administrator pushes the software from the NMS system to robots either individually or in bulk. This is explained in *Bulk Deployment using the Automated Deployment Engine probe (ADE)* (see page 53).

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

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

1. On the client computer, 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) to let the system will use default port numbers, or specify the first port to be used to start probes.
     - Select **Passive mode** if you want to set the hub as passive.

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 Nimsoft hub on your network. If a hub is:
  - not found, then the robot, hub, and Distribution Server are installed
  - found, the robot-only software is installed

- **Custom.** This mode lets you decide which Nimsoft 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** (see page 41)
- **Custom Installation** (see page 41)
- **DMZ Installation** (see page 42)

**Note:** If Nimsoft 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 field blank to let the system assign ports automatically.
   - If you choose to install the DMZ wizard, refer to DMZ Installation (see page 42) 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 Nimsoft software. Execute:
  /opt/nimsoft/bin/niminit stop
  /opt/nimsoft/bin/inst_init.sh remove

■ You can run nimldr in express mode (see page 45) to perform a non-interactive installation.

Running nimldr

Perform these steps on each client system that requires a Nimsoft 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:
     ```bash
     # ./nimldr
     ```
   - Different network segment, execute:
     ```bash
     # ./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 (see page 45).

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

   ```bash
   tail -f /opt/nimsoft/tmp/nimlrd.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 the 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.

If you want to stop and start the robot, enter the appropriate command for your operating system.

<table>
<thead>
<tr>
<th>OS Version</th>
<th>Robot Start/Stop Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris</td>
<td>/etc/init.d/nimbus start /etc/init.d/nimbus stop</td>
</tr>
<tr>
<td>Linux versions that are RC-compatible:</td>
<td></td>
</tr>
<tr>
<td>RHEL 5.x and prior</td>
<td></td>
</tr>
<tr>
<td>CentOS 5.x and prior</td>
<td></td>
</tr>
<tr>
<td>SUSE</td>
<td></td>
</tr>
<tr>
<td>Debian</td>
<td></td>
</tr>
<tr>
<td>Linux versions using Upstart Method:</td>
<td></td>
</tr>
<tr>
<td>RHEL 6.0 and newer</td>
<td>(sudo, su -c, or root user) initctl start nimbus</td>
</tr>
<tr>
<td>CentOS</td>
<td></td>
</tr>
<tr>
<td>Ubuntu</td>
<td></td>
</tr>
</tbody>
</table>
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.

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

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.

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where should nimldr store temporary files?</td>
<td>■ opt/nimsoft/tmp (default)</td>
</tr>
<tr>
<td></td>
<td>■ Directory of your choice</td>
</tr>
<tr>
<td>Is this a Cloud installation?</td>
<td>■ Yes (cloud install)</td>
</tr>
<tr>
<td></td>
<td>■ No (all other installs)</td>
</tr>
<tr>
<td>Do we have the installation file locally?</td>
<td>■ Yes</td>
</tr>
<tr>
<td></td>
<td>■ No</td>
</tr>
<tr>
<td>Where do we have the installation file(s)?</td>
<td>Path to installation file(s)</td>
</tr>
<tr>
<td>Is there a host running a Nimsoft hub we can query for the installation file?</td>
<td>■ Yes</td>
</tr>
<tr>
<td></td>
<td>■ No</td>
</tr>
<tr>
<td>What is the IP address of the host running a Nimsoft hub?</td>
<td>Hub IP address</td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>What is the Nimsoft Domain called?</td>
<td>■ Domain name (if it exists)</td>
</tr>
<tr>
<td></td>
<td>■ Desired name (if it is being created)</td>
</tr>
<tr>
<td></td>
<td>■ * (asterisk) to search for domains</td>
</tr>
<tr>
<td>What is the Nimsoft hub called?</td>
<td>■ Hub name (if it exists)</td>
</tr>
<tr>
<td></td>
<td>■ Desired name (if it is being created)</td>
</tr>
<tr>
<td></td>
<td>■ * to search for hubs</td>
</tr>
<tr>
<td>What is the installation file called?</td>
<td>install_platform</td>
</tr>
<tr>
<td>Which of these archives would you like to connect to?</td>
<td>Specify archive</td>
</tr>
<tr>
<td>Enter Nimsoft username and password.</td>
<td>■ Name/password of the Nimsoft account set up during NMS installation</td>
</tr>
<tr>
<td></td>
<td>■ administrator (typically)</td>
</tr>
<tr>
<td>Where do we have the installation files?</td>
<td>Install file directory (if local)</td>
</tr>
<tr>
<td>What are we installing?</td>
<td>■ 1 (robot only)</td>
</tr>
<tr>
<td></td>
<td>■ 2 (robot and hub, tunnel server, or tunnel client)</td>
</tr>
<tr>
<td>Would you like to install the Distribution Server (distsrv)?</td>
<td>■ Yes</td>
</tr>
<tr>
<td></td>
<td>■ No</td>
</tr>
<tr>
<td>Where should the Nimsoft software be installed?</td>
<td>/opt/nimsoft (default)</td>
</tr>
<tr>
<td>Automatically unregister robot from hub on termination?</td>
<td>■ Yes (default)</td>
</tr>
<tr>
<td></td>
<td>■ No (default)</td>
</tr>
<tr>
<td>Should this robot run in passive mode?</td>
<td>■ Yes (default, hub requests data from robot)</td>
</tr>
<tr>
<td></td>
<td>■ No (robot sends data to hub)</td>
</tr>
<tr>
<td>What is this Nimsoft Domain called?</td>
<td>Existing domain set up during NMS installation</td>
</tr>
<tr>
<td>Which Nimsoft hub should this robot connect to?</td>
<td>Hub name</td>
</tr>
<tr>
<td>What is this Nimsoft hub called?</td>
<td>Hub name</td>
</tr>
<tr>
<td>What is that Nimsoft hub's IP address?</td>
<td>IP address</td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Are you setting up a tunnel between this hub and another hub?</td>
<td>■ Yes ■ No</td>
</tr>
<tr>
<td>Would you like to initialize the security settings on this hub?</td>
<td>■ Yes (default) ■ No</td>
</tr>
<tr>
<td>Please specify the administrator user password.</td>
<td>Password for Nimsoft account set up during NMS installation</td>
</tr>
<tr>
<td>Are you setting up a Nimsoft tunnel between this hub and another hub?</td>
<td>■ No (default); installation completes and the installer exits ■ Yes; installation continues</td>
</tr>
<tr>
<td>Enter Nimsoft username and password.</td>
<td>Username and password for Nimsoft administrator account set up during NMS installation</td>
</tr>
<tr>
<td>Is this hub going to be a tunnel server?</td>
<td>■ Yes – go to Tunnel Server Questions (see page 47) ■ No</td>
</tr>
<tr>
<td>Is this hub going to be a tunnel client?</td>
<td>■ Yes – go to Tunnel Client Questions (see page 48)</td>
</tr>
</tbody>
</table>
**Tunnel Server Questions**

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

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the name of your organization?</td>
<td>Company name</td>
</tr>
<tr>
<td>What is the name of the organizational unit?</td>
<td>Organizational unit</td>
</tr>
<tr>
<td>What is the administrator email address?</td>
<td>Nimsoft administrator account address</td>
</tr>
<tr>
<td>What password should we use for the Server certificate?</td>
<td><em>Password</em> (you will use this when you set up the tunnel client)</td>
</tr>
<tr>
<td>What is the IP address of the tunnel client?</td>
<td>IP address of the system on which you will install the tunnel client</td>
</tr>
</tbody>
</table>
| 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**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the IP address of the tunnel server hub?</td>
<td>Tunnel server hub IP address</td>
</tr>
<tr>
<td>What port is the server listening on?</td>
<td>Port number assigned during NMS installation; typically 48000 (default)</td>
</tr>
<tr>
<td>What password was used to generate this certificate?</td>
<td>Password defined when tunnel client certificate was created during tunnel server setup</td>
</tr>
<tr>
<td>What file is the client certificate in?</td>
<td>Path and <em>filename</em> for client certificate that was copied from the tunnel server to the tunnel client</td>
</tr>
</tbody>
</table>
## Flags for nimldr

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

<table>
<thead>
<tr>
<th>Usage</th>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All installations</td>
<td>-?</td>
<td>Help</td>
</tr>
<tr>
<td></td>
<td>-d</td>
<td>Debug level, 0 (default)-5</td>
</tr>
<tr>
<td></td>
<td>-l</td>
<td>Installation logfile</td>
</tr>
<tr>
<td></td>
<td>-t</td>
<td>Location for temporary files during installation; default is /opt/nimsoft/tmp</td>
</tr>
<tr>
<td></td>
<td>-D</td>
<td>NimBUS domain name</td>
</tr>
<tr>
<td></td>
<td>-H</td>
<td>NimBUS hub name</td>
</tr>
<tr>
<td></td>
<td>-N</td>
<td>Override robot name</td>
</tr>
<tr>
<td></td>
<td>-p</td>
<td>NimBUS installation path; default is /opt/nimsoft</td>
</tr>
<tr>
<td></td>
<td>-f</td>
<td>Override package file name; default installation file is detected by the program</td>
</tr>
<tr>
<td></td>
<td>-u</td>
<td>Install as current user, not as root (NOT recommended)</td>
</tr>
<tr>
<td></td>
<td>-o</td>
<td>First probe port</td>
</tr>
<tr>
<td></td>
<td>-R</td>
<td>IP address for this robot (useful for systems with multiple network cards)</td>
</tr>
<tr>
<td></td>
<td>-a</td>
<td>Set the automatic unregister flag; default is no</td>
</tr>
<tr>
<td></td>
<td>-s</td>
<td>Set the robot to passive mode</td>
</tr>
<tr>
<td></td>
<td>-A</td>
<td>Set robotip_alias for NAT (special case--use with caution)</td>
</tr>
<tr>
<td></td>
<td>-v</td>
<td>Prints version of ./nimldr</td>
</tr>
<tr>
<td></td>
<td>-h</td>
<td>Prints this help text</td>
</tr>
</tbody>
</table>

| Installation file is on local system | -F   | Directory containing installation file (if installation file is on local system) |
| Installation file is on a NimBUS Distribution Server | -I   | IP address of NimBUS hub running a Distribution Server (note that this overrides the -H flag) |
|                                          | -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) |
Removing a Robot

If you need to remove a robot, use the appropriate command.

**Windows**
- To remove a robot, execute:
  
  \`\`\`\n  C:\Program Files\Nimsoft\unins000.exe
  \`\`\`

  where `C:\Program Files\Nimsoft` is the directory where the robot is installed.

**RedHat, SUSE, CentOS**
- To confirm that a robot is installed, execute:
  
  \`\`\`\n  rpm -q nimsoft-robot
  \`\`\`

- To remove a robot, execute:
  
  \`\`\`\n  rpm -e RPM\_package
  \`\`\`

  where `RPM\_package` is the robot name minus the .rpm extension.

**Debian, Ubuntu**
- To confirm that a robot is installed, execute:
  
  \`\`\`\n  dpkg -query \-s nimsoft-robot
  \`\`\`

- To remove a robot, execute:
  
  \`\`\`
  (sudo) dpkg \-r nimsoft-robot
  \`\`\`

**Solaris**
- To confirm that a robot package is installed, execute:
  
  \`\`\`\n  pkginfo nimsoft-robot
  \`\`\`

- To remove a robot, execute:
  
  \`\`\`
  (sudo or su \-c) pkgrm nimsoft-robot
  \`\`\`
Management consoles let you manage your Nimsoft infrastructure and control and view the collected data. Three consoles are available:

- **Infrastructure Manager** (Windows-based) enables you to configure your 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 installed with NMS on your NMS server. If your NMS server is Linux or Solaris, or if you want to run the application from a computer other than the NMS server, you can install it separately. See [Installing Infrastructure Manager](#) (see page 52) for details.

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

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

- **Unified Management Portal** (web-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 Nimsoft 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 > Nimsoft 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: Deploying Robots in Bulk

Bulk robot deployment lets you silently and simultaneously push robot software from the source system to multiple target systems. Nimsoft Monitor provides three methods of bulk deployment methods:

- **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.

- **Nimsoft 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 (see page 54). Then refer to:

- **Bulk Deployment with ADE and XML Distribution** (see page 55)
- **Bulk Deployment with a Third-Party Tool** (see page 60)
Before performing bulk deployment, ensure the following:

- A Nimsoft hub is installed on the source system.
- Your NMS Archive has the required robot installer archive packages: `robot_rpm`, `robot_deb`, `robot_sol`, and `robot_exe`.
  
  Recommendation: Perform bulk deployment from the primary hub because the packages are already there.
- 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 Nimsoft-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.
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 (see page 54).

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 (see page 57)
   - Parameter Values for host-profiles.xml (see page 58)
   **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** and **Solaris** — /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 (see page 56).
- 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”
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. To change delay time, change the value for `verifyDelay` in the ADE probe configuration file `automated_deployment_engine.cfg`. ADE polls the robot every 25 seconds.

For ADE 1.30: `verifyDelay` specifies a time period that ADE will poll the robot periodically. The default is now 100 seconds and ADE will poll the robot every 25 seconds.
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`.

```xml
<hosts>
    <host>
        <profile>CentOS</profile>
        <arch>64</arch>
        <hostname>172.19.9.31</hostname>
        <username>root</username>
        <password>mypassword</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>mypassword</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>
```
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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile</td>
<td>Operating system on target system</td>
<td>windows&lt;br&gt;linux (legacy support for previous RPM packages)&lt;br&gt;red hat enterprise linux&lt;br&gt;centos&lt;br&gt;suse linux enterprise server&lt;br&gt;opensuse&lt;br&gt;ubuntu&lt;br&gt;debian&lt;br&gt;solaris</td>
</tr>
<tr>
<td>arch</td>
<td>Architecture of target system</td>
<td>32&lt;br&gt;64&lt;br&gt;sparcv9</td>
</tr>
<tr>
<td>hostname</td>
<td>Target system name</td>
<td>Hostname or IP address&lt;br&gt;&lt;i&gt;On Windows, use the format you use to log into the system.&lt;/i&gt;</td>
</tr>
<tr>
<td>username</td>
<td>Admin or non-admin account (using &lt;b&gt;sudo&lt;/b&gt;) on target system</td>
<td>Any account on the target that has administrative permissions or supports &lt;b&gt;sudo&lt;/b&gt; for root-level permission</td>
</tr>
<tr>
<td>password</td>
<td>Account password</td>
<td>Password string&lt;br&gt;&lt;i&gt;See the optional rsakeyfile parameter.&lt;/i&gt;</td>
</tr>
<tr>
<td>domain</td>
<td>Nimsoft domain</td>
<td>Domain name (case-sensitive)</td>
</tr>
<tr>
<td>hubip</td>
<td>IP address of the hub to which this robot will belong</td>
<td>IP address</td>
</tr>
<tr>
<td>hub</td>
<td>Name of the hub to which this robot will belong</td>
<td>Hub name (case-sensitive)</td>
</tr>
<tr>
<td>hubrobotname</td>
<td>Name of the robot on the hub where you will run ADE (typically the primary hub)</td>
<td>Robot name (case-sensitive)</td>
</tr>
<tr>
<td>hubport</td>
<td>Port that the hub listens on</td>
<td>Port specified during hub setup (default is 48002)</td>
</tr>
</tbody>
</table>
The following parameters are optional. Do not include optional parameters without providing a value.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default/Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip_version</strong></td>
<td>IP address schema version</td>
<td>IPv4 or IPv6</td>
</tr>
<tr>
<td><strong>rsakeyfile</strong></td>
<td>Path to RSA public key certificate on the system hosting ADE</td>
<td>Format in XML:</td>
</tr>
<tr>
<td><strong>sudo_password</strong></td>
<td>Allows for the use of sudo over ssh during install. ssh password still required. Not applicable to root users.</td>
<td>Password string for sudo.</td>
</tr>
<tr>
<td><strong>installdir</strong></td>
<td>Installation directory on the target system</td>
<td>Desired path, for example /usr/local (Linux or Solaris) or C:\Users (Windows). <strong>Note:</strong> Linux/Solaris installers always place installation files in /nimsoft under the install directory. Windows installers place all installation files in the install folder. On Windows, you may want to include Nimsoft in the <strong>install_dir</strong> path (C:\Users\Name\Nimsoft) to organize the robot install files.</td>
</tr>
<tr>
<td><strong>tempdir</strong></td>
<td>Temporary directory on the target system</td>
<td>Any desired path, for example: /opt/tmp (on Linux or Solaris) or C:\tmp\supertmp (on Windows). On Windows, the path may not include spaces or double backslashes (\).</td>
</tr>
<tr>
<td><strong>origin</strong></td>
<td>Origin for messages</td>
<td>Typically set to the name of a hub in the Nimsoft domain, a Nimsoft robot, a company name, etc.</td>
</tr>
<tr>
<td><strong>robotname</strong></td>
<td>Name to be assigned to the deployed robot</td>
<td>Any valid robot name. Default is the hostname of the computer the robot is deployed to.</td>
</tr>
</tbody>
</table>
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 (SUSE and RedHat)
- Ubuntu (v10.04 and v12.04)
- Debian (v6 and v7)
- Solaris (Intel/AMD and sparcv9)

Before you deploy in bulk, make sure your source and target systems meet the prerequisites (see page 54).

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 (see page 37).
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 Nimsoft robot_MSI package has been deprecated.

2. Copy the `nms-robot-vars.cfg` (see page 64) 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` (see page 64) answer file to `/opt`.
3. Execute the appropriate command.
   - **RedHat, SUSE, or CentOS:**
     ```
     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 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.
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 (see page 64) 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
**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 Nimsoft Infrastructure Manager.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>Nimsoft Domain</td>
<td>HOST_ABC_DOM</td>
</tr>
<tr>
<td>hub</td>
<td>Nimsoft name of the hub to which the robot will be assigned</td>
<td>HOST_ABC_HUB</td>
</tr>
<tr>
<td>hubip</td>
<td>Hostname or IP address of the hub to which this robot will belong</td>
<td>10.0.0.10</td>
</tr>
<tr>
<td>hubrobotname</td>
<td>Name of the robot on the hub</td>
<td>HOST_ABC_ROBOT</td>
</tr>
<tr>
<td>hubport</td>
<td>Port that the hub listens on</td>
<td>48002</td>
</tr>
<tr>
<td>robotip</td>
<td>Hostname or IP address of the target system</td>
<td>10.0.0.10</td>
</tr>
<tr>
<td>robotname</td>
<td>Desired name for robot on target</td>
<td>HOST_MNO</td>
</tr>
<tr>
<td>first_probe_port</td>
<td>Port on source system to be used by the first probe</td>
<td>48000</td>
</tr>
<tr>
<td>origin</td>
<td>Desired origin value</td>
<td>HUBNAME</td>
</tr>
</tbody>
</table>

**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.
Removing a Robot

If you need to remove a robot, use the appropriate command.

**Windows**
- To remove a robot, execute:
  
  ```
  C:\Program Files\Nimsoft\unins000.exe
  ```
  
  where `C:\Program Files\Nimsoft` is the directory where the robot is installed.

**RedHat, SUSE, CentOS**
- To confirm that a robot is installed, execute:
  
  ```
  rpm -q nimsoft-robot
  ```
- To remove a robot, execute:
  
  ```
  rpm -e RPM_package
  ```
  
  where `RPM_package` is the robot name minus the `.rpm` extension.

**Debian, Ubuntu**
- To confirm that a robot is installed, execute:
  
  ```
  dpkg -query -s nimsoft-robot
  ```
- To remove a robot, execute:
  
  ```
  (sudo) dpkg -r nimsoft-robot
  ```

**Solaris**
- To confirm that a robot package is installed, execute:
  
  ```
  pkginfo nimsoft-robot
  ```
- To remove a robot, execute:
  
  ```
  (sudo or su -c) pkgrm nimsoft-robot
  ```
Appendix B: Installing NMS 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.

This section contains the following topics:

- Prerequisites (see page 67)
- Installing NMS on the Cluster (see page 68)
- Configuring the Nimsoft Robot Watcher Service (see page 69)
- Validation and Testing (see page 73)

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 Nimsoft service (from network administrator)

Recommended:
- Do not install any Nimsoft 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://technet.microsoft.com)
- [http://blogs.msdn.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 (see page 25), 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 (see page 69) to set up the Nimsoft Robot Watcher Service.
The Nimsoft 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 Availability Wizard launches. Select the Nimsoft Robot Watcher service, then click Next.

5. In the next screen Client Access Point, choose a name that the Nimsoft Service will use to register itself on the network.

   **Note:** One or more DHCP IP-4 addresses were configured automatically. All networks were configured automatically.
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:\). Specify **Disk Drive** for this service.

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 Nimsoft robot.

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disk Drives</strong></td>
<td></td>
</tr>
<tr>
<td>Cluster Disk 2</td>
<td>Online</td>
</tr>
<tr>
<td><strong>Other Resources</strong></td>
<td></td>
</tr>
<tr>
<td>Nimsoft Robot Watcher Service</td>
<td>Online</td>
</tr>
<tr>
<td><strong>IP Address:</strong> 10.130.220.96</td>
<td>Online</td>
</tr>
</tbody>
</table>

### Upgrade the Robot

Next, install a special version of the Nimsoft 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 Nimsoft 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 Nimsoft 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 Nimsoft service> (noted in the last step of Configuring the Nimsoft Robot Watcher Service)
   - robotip = <virtual IP address of the Nimsoft service> (noted in the last step of Configuring the Nimsoft 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 Nimsoft service (noted in the last step of Configuring the Nimsoft 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 Nimsoft Robot Watcher and select Take this resource offline. Then immediately right-click the service and choose Bring this resource online.
3. Right-click the Nimsoft Robot Watcher service and choose Properties.
4. On the Dependencies tab, set the dependencies for the Nimsoft Robot Watcher service. The following cluster resources must all be online and available before the Nimsoft Robot Watcher service should start:
   - Cluster shared disk
   - Virtual Nimsoft resource
   - Virtual IP address assigned to the virtual Nimsoft service

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 Nimsoft 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 Nimsoft 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 Nimsoft 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 Nimsoft Hub during the failover test.

1. Launch **Failover Cluster Manager** and expand the tree in the left frame.
2. Right-click the virtual Nimsoft 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.
Appendix C: MySQL Windows Installation

This section contains the following topics:

- **Prerequisites and Considerations** (see page 75)
- **Installation Steps** (see page 76)
- **Standard Post-installation Configuration** (see page 77)
- **Basic Tuning Configuration Changes** (see page 77)
- **Deployment Statistics and Estimations** (see page 79)
- **Schema and Data Management** (see page 80)

## Prerequisites and Considerations

- To verify that your version of Windows is supported, check the Nimsoft Compatibility Support Matrix, which is updated regularly.
- If table sizes are expected to exceed 4 GB, then MySQL must be installed on an NTFS or newer file system.
- Virus scanning software can sometimes generate erroneous alerts that incorrectly identify the datafile contents as malicious. This is due to the combination of the MySQL datafile update frequency and the fingerprinting used by some anti-virus packages.

  Recommendation: After installation, prevent any anti-virus software from scanning the main data directory (datadir) and any other directory used by MySQL for temporary datafile creation.

- Windows XP and later include a firewall that specifically blocks ports. If you intend to use MySQL through a network port, ensure the relevant ports are open before installation.
Installation Steps

MySQL should be installed by an administrator to help avoid problems with paths, environment variables or accessing the service control manager. Once installed, MySQL does not need to be run by an administrator.

Follow these steps:

1. Go to http://dev.mysql.com (not affiliated with CA Technologies). Download the:
   - Installer package from the Downloads tab
   - Installation instructions for your platform from the Documentation tab

2. Run the installer package. Note the following:
   - Acknowledge any security warnings.
   - When you select install type:
     - Complete is recommended.
     - Choose Custom if you want to specify datafile locations, such as on a separate, high-performance disk. Specify the paths where required (or do this after installation by rerunning the installer and selecting Modify).
     - In the Ready to install dialogue, select Continue. Ignore information about MySQL Enterprise.

3. When installation is complete, the installer allows you to Register MySQL as a Service. This is recommended, as it allows control of MySQL from Windows Service Manager and ensures the database starts automatically if required.

The paths, directories, system tables and service manager registration are all set up by the installer.

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

1. To enable mysql start during system startup and to simplify the server control, copy the server startup scripts to the relevant location. From the `mysql` directory, execute:
   
   ```
   cp support-files/mysql.server /etc/init.d/mysqld
   ```

   This allows the server to be started using:
   
   ```
   /etc/init.d/mysqld [start|stop|restart|status]
   ```

2. Create the empty file `/etc/my.cnf` (or modify one of the standard configurations as specified in Basic Tuning Configuration Changes (see page 77).

3. Insert the following into `my.cnf` in the `mysqld` section:
   
   ```
   [mysqld]
   innodb_file_per_table
   slow_query_log_file=[path/to/chosen/location/for/slowlog.log]
   datadir=[path/to/datafile/location]
   ```

Basic Tuning Configuration Changes

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

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:

   \[
   \frac{(\text{total RAM} - \text{global buffers})}{\text{total size of thread buffers}}
   \]

   a. From the MySQL command line, execute:

      ```
      show variables
      ```

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

      ```
      \text{key_buffer_size} \\
      \text{innodb_buffer_pool_size} \\
      \text{innodb_log_buffer_size} \\
      \text{innodb_additional_mem_pool} \\
      \text{net_buffer_length}
      ```

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

      ```
      \text{sort_buffer_size} \\
      \text{myisam_sort_buffer_size} \\
      \text{read_buffer_size} \\
      \text{join_buffer_size} \\
      \text{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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>innodb_buffer_pool_size</td>
<td>Typically 70% to 80% of available RAM.</td>
</tr>
<tr>
<td>innodb_log_file_size</td>
<td>256 MB is an adequate size (your value depends on recovery speed requirements).</td>
</tr>
<tr>
<td>innodb_log_buffer_size</td>
<td>4 MB is a standard setting and is effective for most installations unless large amounts of binary data are in use.</td>
</tr>
<tr>
<td>innodb_flush_log_at_trx_commit</td>
<td>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.</td>
</tr>
<tr>
<td>innodb_thread_concurrency</td>
<td>8 (the default) is a good starting point.</td>
</tr>
<tr>
<td>innodb_flush_method</td>
<td>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.)</td>
</tr>
<tr>
<td>innodb_file_per_table</td>
<td>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.</td>
</tr>
</tbody>
</table>

Go to [http://dev.mysql.com/doc/refman/5.5/en/server-system-variables.html](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.
Deployment Statistics and Estimations

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

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

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

Schema and Data Management

The table schema is as follows:

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Install status</th>
</tr>
</thead>
<tbody>
<tr>
<td>.../Nimsoft</td>
<td>Nimsoft product directory. Default is C:\Program Files\Nimsoft Monitoring.</td>
</tr>
<tr>
<td>msvcrtd.dll (Microsoft C library in the Windows system directory)</td>
<td>Updated if the existing version is old. This should not be the case on Window XP or Windows 2000 with an updated service pack.</td>
</tr>
<tr>
<td>New Registry sections</td>
<td>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</td>
</tr>
<tr>
<td>Start &gt; Programs &gt; Nimsoft Service Controller</td>
<td>Menu choice to start the Service Controller.</td>
</tr>
<tr>
<td>Services</td>
<td>The Nimsoft Watcher service can be managed with the service controller. To remove the service, execute: ...in\Nimsoft -remove</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>atl.dll (Windows system directory) syclit.dll stdole2.tlb</td>
<td>Updated if the existing version is old. This should not be the case on Window XP or Windows 2000 with an updated service pack.</td>
</tr>
<tr>
<td>asyclit.dll stdole2.tlb</td>
<td>Installed if nonexistent; updated if the existing version is old.</td>
</tr>
</tbody>
</table>