CA Nimsoft Monitor

Discovery User Guide

v6.50

March 2013

Document Revision History

Document Version	Date	Changes
6.50	April 2013	First edition of the guide, covering Nimsoft Discovery as implemented in NMS v6.50.

Legal Notices

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Nimsoft LLC disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Nimsoft LLC shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Nimsoft LLC and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Nimsoft LLC as governed by United States and international copyright laws.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Nimsoft LLC's standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Trademarks

Nimsoft is a trademark of CA.

Adobe®, Acrobat®, Acrobat Reader®, and Acrobat Exchange® are registered trademarks of Adobe Systems Incorporated.

Intel® and Pentium® are U.S. registered trademarks of Intel Corporation.

Java(TM) is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape(TM) is a U.S. trademark of Netscape Communications Corporation.

Oracle® is a U.S. registered trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of the Open Group.

ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

For information on licensed and public domain software, see the *Nimsoft Monitor Third-Party Licenses and Terms of Use* document at: http://docs.nimsoft.com/prodhelp/en_US/Library/index.htm?toc.htm?1981724.html.

Contact CA Nimsoft

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Appendix C: cm_data_import Probe 47

Chapter 1: Overview

This introductory section describes the objectives of this guide, the high-level concepts surrounding Nimsoft discovery, and how to put it to work in your environment.

This section contains the following topics:

About this Guide

This guide describes how to implement and make use of device discovery within CA Nimsoft Monitor Server. Discovery is made up of a number of components that are each covered in detail their respective online help entries. However this guide looks at the collection of components from a high level, showing how all pieces fit together to implement device discovery.

After reading this guide, CA Nimsoft Monitor administrators should have an understanding of:

- IT device discovery
- How the probe components that make up discovery are deployed within an IT environment
- How Authentication Profiles, IP address Scopes, and Schedules are configured and run in the Discovery Wizard
- How file-based import works
- Some best practices for the use of discovery for the network and device monitoring purposes.

About Discovery

Components in the CA Nimsoft Management Server automate discovery of hosts and devices throughout your network, recording any device within a discovery scope that responds to a request on any configured protocol, including a simple ICMP ping.

When you have installed CA Nimsoft Monitor, the Discovery Wizard opens and you are prompted to discover devices on your network. The Discovery Wizard allows you to set authentication credentials and define IP address scopes to scan for automated discovery. Automated discovery scans can be initiated on-demand, or be scheduled to run on regular intervals. You can augment automated discovery with file-based device import, which allows you to import a list of devices into the device inventory.

The automated network device discovery process – using multiple network protocols – finds virtually all connected resources on the network and provides detailed information on device type, configuration and asset/inventory data. By using ICMP, ARP, DNS, SNMP (v1, v2 and v3), WMI, SSH, NetBIOS, and LDAP, discovery finds a wide range of devices and device information.

Discovery Components

The most visible component of discovery is the **Discovery Wizard**. The Discovery Wizard is launched from any discovery_agent listed in the Discovery tree within USM (Unified Service Manager). Discovery Wizard allows you to set up:

- **automated discovery** -- populates the device inventory by scanning the network according to authentication profiles and scanning scopes that are set up in the Wizard
- **file-based import** -- imports a list of one or more hosts or network devices into the device inventory.

These topics are covered fully in the section on the Discovery Wizard (see page 15).

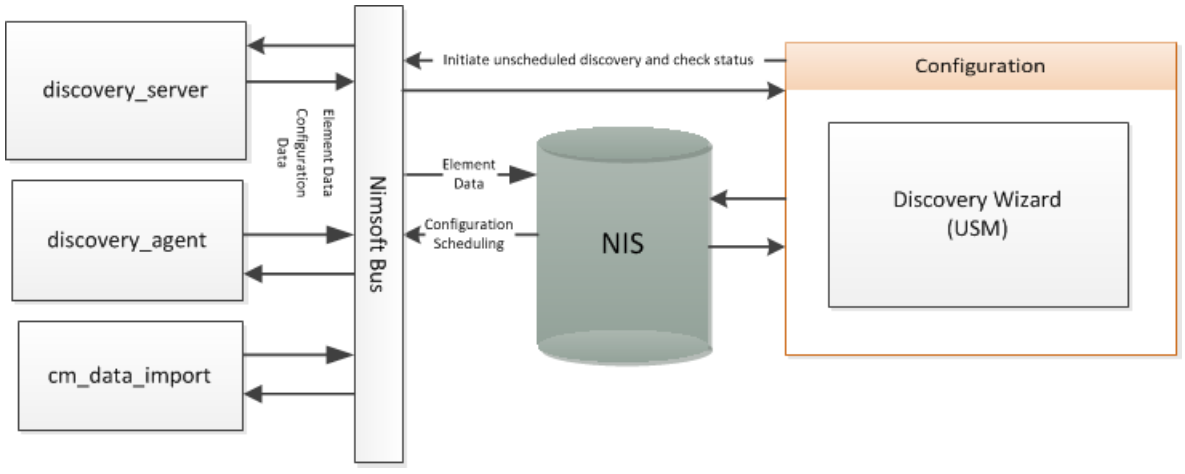
Discovery is accomplished by three standard service probe components in NMS (all installed on the primary Hub in a typical deployment):

- the **discovery_server** probe --discovers Nimsoft infrastrucure components, keeps a list of monitored servers and devices in the Nimsoft Domain, and also finds and communicates with the discovery_agent probes. More information is available in the section Discovery Server Probe (see page 29).
- the **discovery_agent** probe --does the work of scanning the network, collecting as much system information about discovered devices as possible. Some users, particularly service providers and those with very large networks, find it useful to deploy multiple discovery agents in various locations. Discovery of a large network can be divided across administrative boundaries—so that different users have access to different parts of the network—or in situations where there is no direct connectivity to devices at a remote site because of firewall constraints or network-address translation (NAT). More information is available in the section Discovery Agent Probe (see page 41).
- the **cm_data_import** probe -- processes an XML file that lists information describing hosts and devices, and adds this information to the device inventory. When you run file-base import from Discovery Wizard, the cm_data_import probe carries out the work. More information on this probe is available in the section cm_data_import Probe (see page 47).

Discovered device data is stored in the **NIS** database (Nimsoft Information Store), which is the central repository for all persistent data produced and consumed by Nimsoft Monitor components.

Discovery Architecture

This diagram illustrates the components of discovery:



Note: This diagram does not reflect the actual distribution of components in the environment; it depicts the flow of data among key pieces of the architecture.

Benefits of Discovery

Discovery is primarily a way to reduce manual effort while maintaining an accurate inventory of systems in your managed domain. In USM you can enable device monitoring and management on these systems as required, engaging the broad array of Nimsoft probes that gather QoS data from the monitored devices and generate alarms in response to events, outages, and QoS variations.

Using the data that Discovery collects, Topology and Root Cause Analysis can deduce the structure of the network and model it. The model is viewable in the Relationship Viewer portlet in the Unified Management Portal (UMP). More information on the topics of topology and root cause analysis is available in the Topology and Root Cause Analysis User Guide.

An alternative to automated discovery is to provide a file that lists devices and import this information into the device inventory. Use of file-based import is covered in the section Using File-based Import (see page 25).

Note: Devices that are imported into Nimsoft via file-based import are not reflected in Topology or in Root Cause Analysis. Topology depends on SNMP information gathered by the discovery agent about the devices.

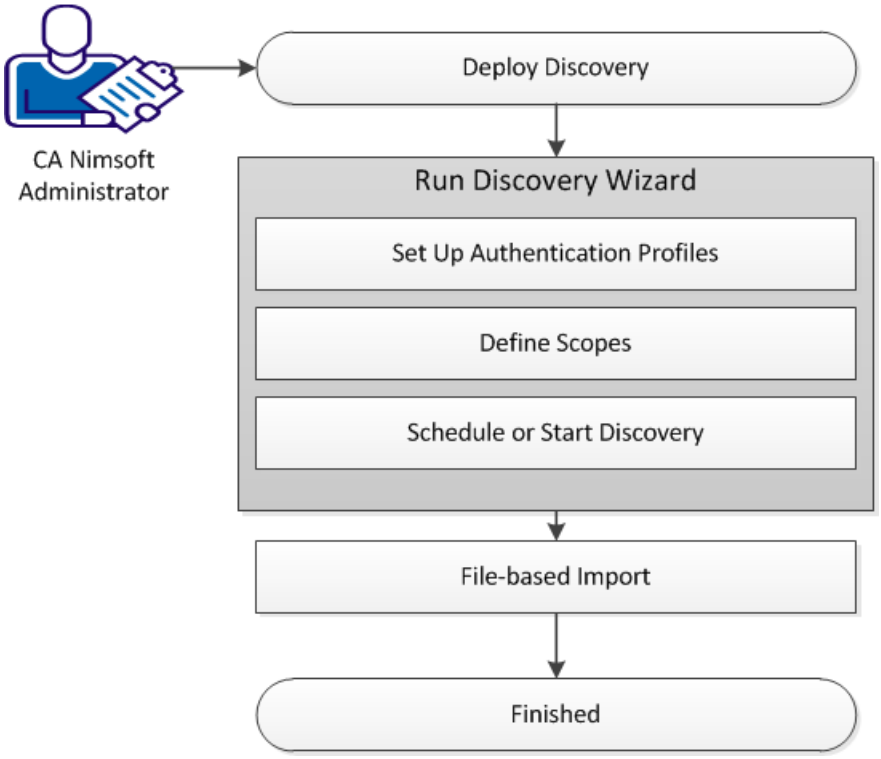
Chapter 2: Setting up Discovery

This section discusses how to set up discovery correctly.

This section contains the following topics:

Overview of Set Up and Configuration

This section gives a high-level overview of the entire process. Sections to follow cover each step in more detail and provide valuable tips to improve performance and simplify configuration tasks.



The basic steps are as follows:

1. Deploy Discovery (see page 12)--the components required for discovery are put in place with a basic install of Nimsoft Monitor.
2. Run Discovery Wizard (see page 15) in USM to configure and start or schedule discovery. In the case of a new or updated Nimsoft Monitor installation, Discovery Wizard will launch automatically the first time UMP is opened.
    1. Set up authentication profiles
    2. Define scopes (sets of IP addresses, IP ranges, and IP masks)
    3. Schedule or start discovery
3. File-based import (see page 25) (optional)--prepare an XML file with device information and import this information into the device inventory.

Prerequisites and Supported Platforms

Discovery is included in, and required by, CA Nimsoft Monitor Server (NMS). See the Nimsoft Monitor Compatibility Support Matrix for details on supported NMS platforms.

Deploy Discovery

The components (probes) required for discovery are put in place with a basic install of CA Nimsoft Monitor:

- the **discovery_server** probe --discovers Nimsoft infrastructure components, keeps a list of monitored servers and devices in the Nimsoft Domain, and finds and communicates with the discovery_agent probe(s)
- the **discovery_agent** probe --scans the network, collecting as much system information about discovered devices as possible
- the **cm_data_import** probe -- supports file-based import.

Keep the following in mind if you wish to modify the default discovery probe deployment:

- For minimal discovery, only the discovery_server probe is required. No network scanning is performed.
- To add file-based import, the cm_data_import probe needs to be on the same system that hosts the discovery_server probe.
- To add network scanning, deploy the discovery_agent probe on the primary hub or elsewhere.
- For optimal discovery in larger environments, more than one discovery agent can be deployed. Some users, particularly service providers and those with very large networks, find it useful to deploy multiple discovery agents in various locations. Discovery of a large network can be divided across administrative boundaries—so that different users have access to different parts of the network—or in situations where there is no direct connectivity to devices at a remote site because of firewall constraints or network-address translation (NAT). To avoid duplicate entries, deploy discovery agents such that each one discovers an exclusive part of the network.

Tip: The discovery agent requires read-only SNMP access to network devices. To simplify discovery configuration, you should consider setting up as many of your network devices as possible to use a "universal" read-only community string (SNMP v3 recommended over v1 or v2c). For example, you could define a read-only (get-only) community string to be "**nms_get_only**". Then set up every device possible to allow read-only SNMP access via that particular community string. This minimizes the number of SNMP authentication credentials that must be attempted on network nodes, and vastly simplifies your discovery configuration.

Chapter 3: Discovery Wizard

This section contains the following topics:

Running the Discovery Wizard

The Discovery Wizard leads you through the process of configuring discovery, and allows you to schedule future discovery scans or to run discovery immediately. One or more discovery agents scan the network, using the authentication profiles and scopes you define.

The following sections tell you how to run the Discovery Wizard.

Launch the Discovery Wizard

The first time you open the Unified Management Portal (UMP) it opens to the Unified Service Manager portlet and the Discovery Wizard is automatically launched.

Note: The Discovery Wizard will not run after an update of CA Nimsoft Monitor if there are existing scopes that define *excluded* IP addresses. You must either choose to accept the system prompt to delete excluded ranges, or remove them manually from the NIS database before Discovery will run.

After the first time you open UMP, you can launch the Discovery Wizard manually if you want to run discovery or change your discovery settings. You can launch the Discovery Wizard from the Discovery tree or from the **Actions** menu.

For either method, the wizard opens in the context of the node you launched it from. If you launch it from a discovery agent node, the Authentication tab is displayed. If you launch it from a scope node, the Scopes tab is displayed with the properties of the scope you selected.

Follow these steps:

1. Hover the cursor over or click the name of a discovery agent or scope in the tree.

   Discovery agents are indicated by the magnifying glass icon (), and scopes are indicated by the network icon () for network scopes or the directory icon () for LDAP scopes.

2. Click the gear icon () to the right of the discovery agent or scope name in the tree, or choose **Discovery Wizard** from the **Actions** menu.

   Note: The **Discovery Wizard** menu option is enabled only when you click on a discovery agent or scope in the tree.

Create Authentication Profiles

The Authentication tab of the Discovery Wizard allows you to create, edit, view and delete authentication profiles for discovery. An authentication profile contains credential information necessary for the discovery_agent probe to access and gather information about computer systems and devices in your network.

Authentication profiles can be defined for these authentication protocols:

- LDAP
- Shell
- SNMP
- WMI

Click the name of an authentication profile in the left pane to view its properties in the pane to the right.

To modify an existing authentication profile, select it and edit the fields as necessary, then click **Save**. To delete an authentication profile, click the trash can icon () next to the name of the profile in the left pane, then click **Save**.

Follow these steps:

1. Click the plus icon () next to the profile type (for example, **ldap**) in the left pane of the Authentication tab.
2. Enter information in all required fields.

   Required fields are outlined in red. For a description of each field, see the subsequent topic for the appropriate authentication profile.
3. Click **Save**.
4. Click **Next**.

LDAP

LDAP (Lightweight Directory Access Protocol) is a protocol for accessing distributed directory information services. CA Nimsoft Discovery can query LDAP providers for a directory of known hosts and devices.

Description

Name for the authentication profile.

ID

This read-only field is the Nimsoft system ID for this authentication profile, assigned when the profile is saved. It identifies the profile uniquely for re-use in other areas of USM that reference authentication profiles.

LDAP Provider

The LDAP provider profile contains information about the LDAP directory service you are using. By default, this is **Active Directory**. To create an LDAP provider profile, click the plus icon ( ). To edit an LDAP provider profile, click the gear icon ( ).

Host

IP address of the LDAP server host machine.

Port

Port number to use for communication with the LDAP server host machine (default is 389).

Base DN

The LDAP query for locating items of type computer system in the LDAP directory.

For example:

CN=Computers,DC=somewhere,DC=com

Principal

Identity of the principal to use to authenticate the discovery agent to the LDAP provider service.

For example:

CN=someone,OU=MANAGER,DC=somewhere,DC=com

Password

Password for your LDAP server. Check the **Show new passwords** check box to see the text as you enter it.

Authentication

Authentication type:

- None
- simple - sends FQDN of the client and its password in clear text; supported by LDAP v1 and v2 servers
- DIGEST-MD5 - Digest Access Authentication, required by LDAP v3 servers; uses MD5 cryptographic hashing
- CRAM-MD5 - Challenge-Response Authentication Mechanism, supported by LDAP v3 servers; mostly superseded by DIGEST-MD5

LDAP Provider

The LDAP provider profile contains information about the LDAP directory service you are using. The provider profile is selected in the Authentication tab of the Discovery Wizard for LDAP authentication profiles.

The LDAP provider profile identifies the names of attributes associated with computer systems in the LDAP directory. The attribute values provide information about the systems.

If you do not use Active Directory, or if you have custom names for Active Directory attributes for computer systems, you must specify the attribute names in the fields of this dialog. If you use Active Directory with the default attribute names for computer systems, use the default values below.

Note: For the **OS Type**, **Version**, and **Description** attributes, typically use the defaults given.

Description

Name for the profile.

Computer Name

Name of the LDAP attribute which holds the computer name (as identified by LDAP and contained in its directory of computer names). This attribute is often given the appellation “name” but can differ depending on implementation of LDAP in your environment. Contact your LDAP administrator for details.

OS Type Attribute

Name of the attribute which holds the operating system value. CA Nimsoft Monitor uses this value to compute the base os_type (such as Windows, Unix, or Solaris) and records the full value as the os_name. Default is operatingSystem.

OS Version Attribute

Name of the attribute which holds the operating system version. CA Nimsoft Monitor records this value as the os_version. Default is operatingSystemServicePack.

OS Description Attribute

Name of the attribute which holds the operating system description.CA Nimsoft Monitor records this value as the os_description. Default is operatingSystemVersion.

Domain Attribute

Name of the attribute which holds the computer system's DNS name, as recorded by the LDAP provider. CA Nimsoft Monitor records this value as the ad_domain.

Shell

Shell is used primarily to access and discover Unix and Linux systems.

Description

Name for the authentication profile.

ID

This read-only field is the Nimsoft system ID for this authentication profile, assigned when the profile is saved. It identifies the profile uniquely for re-use in other areas of USM that reference authentication profiles.

User

User name.

Password

The user password. Check the **Show new passwords** check box to verify the text as you enter it.

SSH or Telnet

Select the communication protocol to use, SSH (Secure Shell) or Telnet (no secure authentication or encryption).

SNMP

SNMP (Simple Network Management Protocol) is a widely-used standard protocol for managing devices on IP networks.

CA Nimsoft Discovery supports SNMP versions 1, 2c, and 3. SNMP v3 adds security features which v1 and v2c lack. As a result, authentication profile configuration fields in the Discovery Wizard that deal with security and privacy (encryption) are only active when **3** is selected in the **Version** pull-down menu.

We recommend the following best practices:

- Create a minimal set of SNMP Authentication Profiles that will, in aggregate, provide SNMP access to all your network devices and hosts that support SNMP.
- Set up as many of your network devices as possible to use a "universal" read-only community string. For example, you could define a read-only (get-only) community string to be **nms_get_only**. Create an authentication profile that uses that community string. Then set up every device possible to allow read-only SNMP access via the universal community string. This minimizes the number of SNMP authentication credentials that must be attempted on network nodes, and simplifies your discovery configuration.
- If there are devices that accept unique SNMP community strings, create one authentication profile for each of those community strings.

Field (SNMP v1 or v2)	Required	Description
Description	Yes	Name for the authentication profile
ID		This read-only field is the Nimsoft system ID for this authentication profile, assigned when the profile is saved. It identifies the profile uniquely for re-use in other areas of USM that reference authentication profiles.
Version	Yes	The SNMP version supported by the monitored device. When version 1 or 2 is selected, only the Community field is active.
Community	Yes	The SNMP community string. Check **Show new passwords** to verify the text as you enter it. Be aware that this string is sent across the network in clear text as part of SNMP v1 or v2c requests, which may pose a security risk.

Field (SNMP v3)	Required	Description
Description	Yes	Name for the authentication profile
ID		This read-only field is the Nimsoft system ID for this authentication profile, assigned when the profile is saved. It identifies the profile uniquely for re-use in other areas of USM that reference authentication profiles.

Version	Yes	SNMP version supported by the monitored device. Versions 1, 2c, and 3 are supported. When v3 is selected, other fields for security and privacy are enabled.
Password	See note	The password associated with the SNMP v1/v2c device or SNMP v3 user. Check **Show new passwords** to verify the text as you enter it. **Note:** This field is enabled and required if either **AuthNoPriv** or **AuthPriv** security is selected. See the description for the Security field below.
User	Yes	SNMP v3 user name used to access the monitored device. Required for all SNMP v3 security levels. See the description for the Security field below.
Method	Yes	SNMP v3 method of encryption, when **AuthPriv** security is selected (see the description for the Security field below): ■ **None** ■ **MD5** - MD5 Message-Digest Algorithm (HMAC-MD5-96) ■ **SHA** - Secure Hash Algorithm (HMAC-SHA-96)
Security	Yes	SNMP v3 security level of the user. Depending on what level of security is selected, other security fields are enabled or disabled. ■ **NoAuthNoPriv** - messages sent unauthenticated and unencrypted ■ **AuthNoPriv** - messages sent authenticated but unencrypted ■ **AuthPriv** - messages sent authenticated and encrypted
Priv.Password	See note	SNMP v3 privacy password to use if **AuthPriv** security level is selected. Must be at least eight characters. Do not confuse with the user password (authentication). **Note:** This field is enabled and required if **AuthPriv** security is selected
Priv.Protocol	See note	SNMP v3 privacy (encryption) protocol to use. ■ **DES** - Data Encryption Standard ■ **AES** - Advanced Encryption Standard **Note:** Enabled and required if **AuthPriv** is selected.

WMI

WMI (Windows Management Interface) discovery scans servers and hosts running Windows to gather system information. WMI discovery runs only on discovery agents hosted on Windows systems.

Description

Name for the authentication profile.

ID

This read-only field is the Nimsoft system ID for this authentication profile, assigned when the profile is saved. It identifies the profile uniquely for re-use in other areas of USM that reference authentication profiles.

User

User name, in the form of **Domain\user name**.

Password

User password. Check the **Show new passwords** check box to view the text as you enter it.

Create Scopes

The Scopes tab of the Discovery Wizard is where you create or edit scopes. A scope specifies the portion(s) of the network where devices are to be discovered. You can also assign authentication profiles to a scope for use in discovery.

You can define either a network scope or an LDAP scope. A network scope can use any combination of SNMP, Shell, and WMI authentication profiles. To discover systems via LDAP, define an LDAP scope.

The discovery process records *any* device within a discovery scope that responds to a request on any protocol, including a simple ICMP ping. This means you can include end nodes (such as servers, network printers, network storage systems, or workstations) in a discovery scope, even if they don't respond to requests via SNMP or other management protocols.

If no authentication profile is assigned to a discovery scope, basic discovery is performed using protocols that do not require authentication, but discovery may not be complete and information about discovered systems is limited.

Best Practices for Creating Scopes

For each discovery agent, review the assigned scopes to minimize predictable timeouts. Follow these guidelines:

- To optimize performance and avoid duplicate entries, each discovery agent should discover an exclusive part of the network.
- The discovery agent tries each credential on each IP address and waits for a timeout (or success) with each attempt. Use a single credential in a scope that has a high probability of immediate success on the nodes in that scope to speed up discovery.
- When applying an authentication credential to a scope, make sure that most, if not all, devices defined by that scope will accept the credential.
- If you include devices that do not respond to requests on any management protocol, place them in a discovery scope with no authentication profiles assigned to the scope.
- When using SNMP, for a device that accepts only a unique SNMP community string, create a network scope with a **Single** type IP range that specifies the device's IP address. Assign the corresponding authentication profile to the network scope.
- When using SNMP, to avoid unnecessary authentication traps/alerts, assign only one SNMP authentication credential per discovery scope.

Create a Network Scope

A network scope assigns authentication profiles to be used and specifies one or more network addresses, address ranges, or masks where devices are to be discovered.

Follow these steps:

1. Click **New scope** in the left pane of the Scopes tab.
2. Enter a name for the scope in the **Description** field.
3. In the **Authentication profiles** pane, select the check boxes for the authentication profiles you want to assign to this scope.

   If you have a large number of authentication profiles in the list, enter the name of the profile you want in the filter field above the list.

   To view only the profiles you selected, select the **Hide unused profiles** check box.
4. In the **Network definition** pane, choose one of the following from the pull-down menu to specify an area of your network where you want to perform discovery:
   - **Mask** - Bitmask for a subnet using Classless Inter-Domain Routing (CIDR) notation with a base IP address and a routing prefix. For example, 195.51.100.1/24.
   - **Range** - Range of IP addresses
   - **Single** - Single IP address

5. Enter the appropriate IP address(es) in the fields next to the pull-down menu.
6. To add an IP range, click **New ip range** above the **Network definition pane** and repeat the previous two steps.
7. When you have finished defining IP ranges, click **Save**.
8. Click **Next**.

Create an LDAP Scope

For LDAP, CA Nimsoft Monitor queries LDAP providers for a directory of known hosts and devices, rather than searching for devices on the network. When defining an LDAP scope, you assign authentication profiles to use to access LDAP providers.

If you have one or more LDAP authentication profiles, an **ldap** scope is included in the list of scopes in the Scopes tab.

Note: If you do not see the **ldap** scope listed in the left pane of the Scopes tab, go back to the Authentication tab and create at least one LDAP authentication profile.

Follow these steps:

1. Click **ldap** in the left pane of the Scopes tab.

   The LDAP properties are displayed in the pane to the right.

   If you have a large number of scopes listed in the left pane, enter **ldap** in the filter field above the pane to find the ldap scope.

2. Uncheck the **Hide unused profiles** check box.

   All LDAP authentication profiles are listed in the **Authentication profiles** pane. A key icon (🔑) next to the name of an authentication profile indicates that CA Nimsoft Monitor successfully used the credentials in the profile.

3. Select the check box for the LDAP authentication profiles you want to use for discovery.

   If you have a large number of LDAP authentication profiles in the list, enter the name of the profile you want in the filter field above the list.

   To view only the profiles you selected, select the **Hide unused profiles** check box.

4. Click **Save**.
5. Click **Next**.

Schedule Discovery

In the Schedule tab, you can schedule discovery to run in the future, and/or you can run discovery immediately. You can schedule either a single discovery run or recurring runs.

A scheduled discovery does not interrupt a discovery that is already running. If at the time a discovery run is scheduled another discovery run is in progress, the scheduled discovery is ignored.

If you select **Run discovery now** and discovery is in progress, the current discovery run is terminated and the new run is executed.

Schedule Discovery

1. Select the **Schedule discovery** check box.
2. Enter information in the date and time fields.

   The time field is in 24-hour format. The time is the local time for the user.
3. To schedule recurring runs, select the **Recurring every** check box, and enter the number of hours for the recurrence interval.
4. Click **Finish**.

Run Discovery

1. Select the **Run discovery now** check box.
2. Click **Finish**.

File-Based Import

Using file-based import, CA Nimsoft administrators can import device and host information into CA Nimsoft Monitor without network scans or manual entry. Because it is not necessary to scan the IT environment, file-based import of devices causes fewer security alerts, and can be faster than automated discovery using the Discovery Wizard.

Note: If a system is discovered by an automated scan of the network and is also included in a file-based import, the file-based import takes precedence. If information about the system differs, the information in the XML file for file-based import is the information that is stored in the database.

Follow these steps:

1. Create an XML file containing information about computers or network devices.

   For details about the contents of the XML file, see the help topic XML File Schema (see page 49).
2. Expand the **Discovery** node in the tree view in the Unified Service Manager.

3. Hover over the **External** node in the tree and click the import icon (), or click the **External** node and choose **Discovery Import** from the **Actions** menu.
4. Navigate to the XML file in the file browser, then click **OK**.

   The device information is imported into the Nimsoft database. This can take a few moments.
5. To view imported devices, click the **External** node.

   The devices are displayed in the table to the right.

Alternative import method:

The cm_data_import probe monitors a directory for valid XML files, and if it finds one, it automatically imports the information into the database. Here is how the process works:

1. Copy the XML file you prepared to <Nimsoft install directory>\Probes\Service\cm_data_import**import** directory on the system that hosts the cm_data_import probe.
2. The cm_data_import probe scans this directory at regular intervals (the default is 60 seconds).
3. If the probe finds a valid import file, it imports the device information in the file into the Nimsoft database.
4. The probe moves the file to a timestamped subfolder in the <Nimsoft install directory>\Probes\Service\cm_data_import**processed** directory, also on the probe host, and logs the results of the process.

Viewing Discovered Systems

The **Discovery** node in the tree view of the Unified Service Manager allows you to view computers and devices that have been discovered on your network.

The Discovery section of the tree contains discovery agents, with network scopes under each discovery agent. The tree also has an Automatic and an External node.

Note: LDAP scopes are not listed in the tree.

Icons next to the tree nodes help identify the type of node and provide additional information:

 - Top-level Discovery node or discovery agent.

 - Network scope.

 - Automatic. Some probes automatically discover systems, and those systems are displayed under this node.

 - External. Systems listed under this node were imported using file-based discovery.

 - A discovery is scheduled. Hover over the icon to see the next scheduled time in the tool tip.

 - Discovery in progress. The proportion of blue indicates the progress of discovery.

 - No discovery scheduled.

Click a node in the tree to view associated systems and their properties in the table to the right. To view properties for all discovered systems, click the **Discovery** node.

A pie chart above the table displays information about discovered systems for the selected node. Choose a different criterion (**Device Type**, **Operating System,** etc.) from the pull-down menu to change the data displayed in the pie chart.

Click a slice in the pie chart or an item in the chart legend to filter for those systems. Only the systems represented in the slice are displayed in the table and reflected in the response links to the right. Click the slice or legend item again to clear the filter.

The response links to the right of the pie chart list systems according to how recently they responded to a request from the discovery agent. Click one of these links, such as **Recent (last day)**, to filter for those systems. Only those systems are displayed in the pie chart and in the table. Click the link again to clear the filter.

Note: Systems that do not respond are eventually purged from the database. By default, 30 days after the last response from a system, the system is deleted from the database. This setting is configured in the discovery_server probe GUI under **Setup** (see page 31).

A Quick Filter field below the response links allows you to filter for text in the **Name**, **IP Address**, **Domain**, **OS Name**, and **Origin** columns of the table.

Click a column header to sort the table by the column.

A key icon () in the table indicates a discovery agent was able to authenticate with the system using one of the defined authentication profiles. Hover over the key icon to view the type and name of the authentication profile used.

Click the reload icon () to refresh discovery data. This may take a few moments; the time depends on the number of systems in your environment and the speed of your network connections. After you click it, the icon is disabled until discovery is finished, then the icon is enabled again.

You can export data for a discovery agent or network scope. The data includes more columns than are displayed in the Inventory table. Data is exported to a .csv file, which is saved in a location you choose. To export data, click a discovery agent or network scope in the tree, then select **Export Group** from the **Actions** menu.

Note: When you choose **Export Group**, all systems for the selected discovery agent, or selected network scope, are exported, regardless of whether you filtered the display in the Inventory view.

Appendix A: Discovery Server Probe

This section covers the discovery_server probe.

This section contains the following topics:

discovery_server Overview

The discovery_server probe is responsible for collecting system information and storing this information into the Nimsoft Information Store (NIS) database. There is one discovery_server probe that usually runs on the primary hub.

The discovery_server probe has two major tasks:

1. Collect information about the Nimsoft infrastructure: hubs, robots, probes, packages, monitored systems or devices, monitored subsystems or items and monitored metrics.
2. Collect system information from the discovery_agent probes.

The discovery_server probe also keeps the NIS database up to date by expiring inactive systems.

The information collected by the discovery_server probe and saved into the NIS database is used by other components in the Nimsoft Monitor solution. In the Unified Server Manager (USM) portlet, the discovery_server probe enables service-oriented configuration--discovered systems are grouped into categories, then category-specific monitoring templates can be applied to deploy appropriate probe sets to each group. Once monitoring has been established, the information stored by discovery is utilized in generating Dynamic Views.

Note: Even without deploying any discovery_agent probes the discovery_server probe is still needed to generate the data required by Dynamic Views.

Database Support

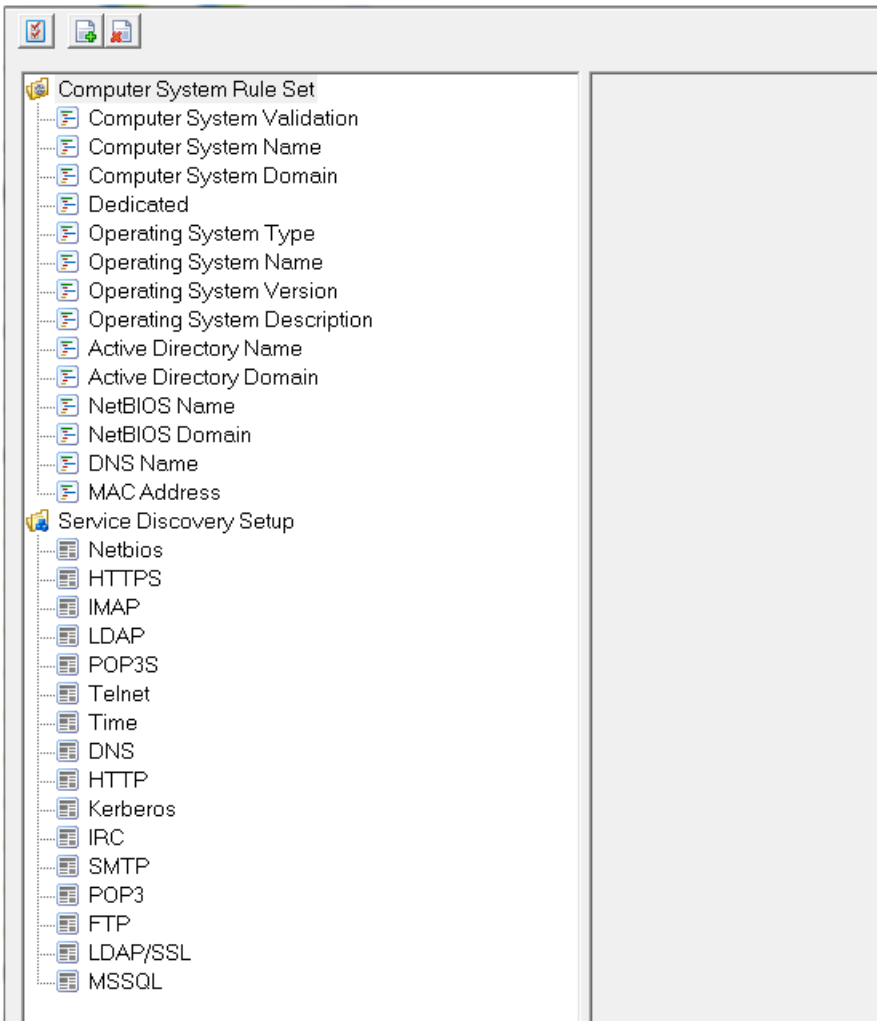
The discovery_server probe uses the database specified in the data_engine probe. The discovery_server probe supports the same set of databases as supported by the Nimsoft Server solution. Please refer to the *Nimsoft Server Installation Guide* for information on supported databases.

discovery_server Configuration

This section describes the configuration concepts and procedures for setting up the discovery_server probe.

discovery_server Configuration GUI

Double-click the icon representing the discovery_server probe in Infrastructure Manager to launch the discovery_server probe configuration interface.



The GUI contains the following sections:

- The toolbar - this contains three buttons, setup, add service, and delete service.
- The left pane - this pane contains the Computer System Rule Set and the Service Discovery Setup information.
- The right pane - this pane displays configuration information for the selected item in the left pane.

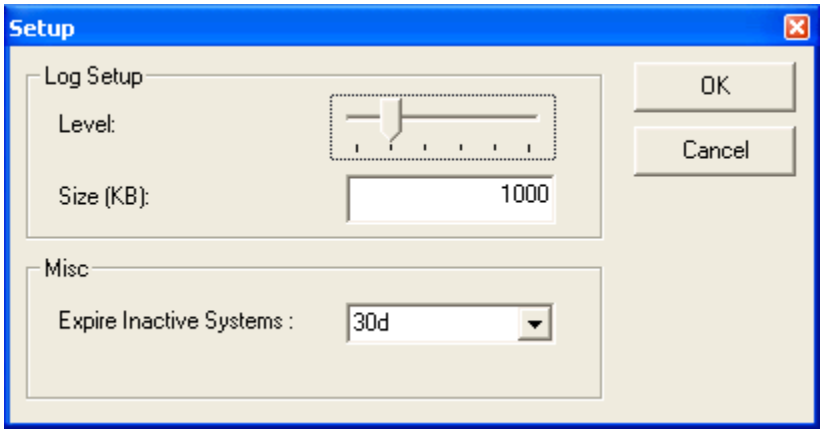
Toolbar

The toolbar contains three buttons:

- Setup (see page 31)
- Add Service
- Delete Service

Setup Button

Click the **Setup** button in the upper left corner of the main GUI to display the Setup dialog.



The Setup dialog lets you set the following parameters:

Log Setup Level

Sets the level of details written to the log file. Log as little as possible during normal operation, to minimize disk consumption.

Log Setup Size

The size of the log file in KB. Default is 1000 KB.

Misc - Expire Inactive Systems

You may configure the expiration time, which by default is set to 30 days. This means that 30 days after the last time the discovery_server has received an update on a system, the system will be deleted from the NIS. The expiration of inactive systems occurs for all systems that were not externally added via the cm_data_import probe using file-based import.

Add Service Button

The Add Service button on the toolbar allows you to add new services to your discovery_server probe configuration. Refer to Adding and Configuring a Service (see page 35) for more information.

Delete Service Button

The Delete Service button on the toolbar allows you to remove services from your discovery_server probe configuration. To delete an existing service refer to the Deleting a Service (see page 38) section.

Note: If you delete a default service, when the probe is started or restarted the discovery_server probe will reload the default service configurations.

The Left Pane

The left pane of the discovery_server probe configuration contains the Computer System Rule Set and the Service Discovery Setup information.

Computer System Rule Set

The discovery_server probe collects computer system information from all the configured discovery_agent probes. For each computer system, a discovery_agent may provide the same piece of information from multiple sources or protocols. The discovery_server probe uses the Computer System Rule Set to determine which source should be used as the provider for a particular piece of information.

Example: A discovery_agent probe may get the system name from DNS, Active Directory and SNMP. The "Computer System Name" rule specifies the precedence for choosing which name to use. Other computer system fields apply rules similar to those used for "Computer System Name".

You may override one or more of these rules and modify them to match your specific needs. You can change the ordering within a rule to change the precedence or add functions to filter or modify the data.

Note the two special rules:

- Computer system validation

  This rule allows you to exclude computer systems from being added to the database and from further processing of other rules in the rule set.

- Dedicated

  This rule is used to specify the dedicated function of a system. Some default dedicated types can be determined from SNMP (such as route, switch, and printer). You can customize this rule to define other dedicated types based on the discovery_agent probe data.

Override default rule?

The rule set consists of a number of rules. You are allowed to override one or more of these rules and modify them to match your specific needs.

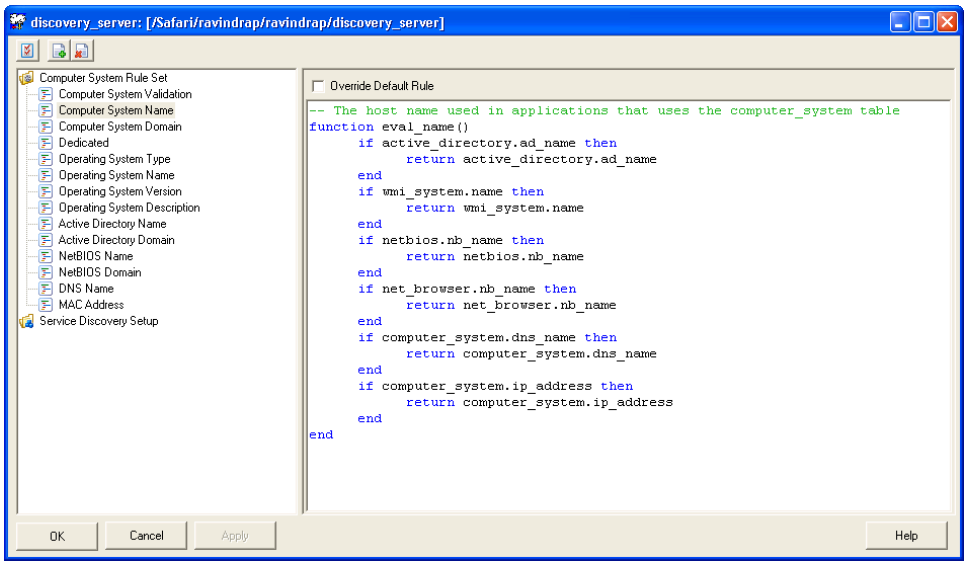
To override a rule, you select the rule in the left pane and click the *Override Default Rule* option. Then you are allowed to edit the script. This must be done individually for each of the rules you want to overrule. LUA is the scripting language used for the rules.

A rule decides the value of a given field in the computer system's record in the database. You can make the rule insert the value you want into this field, or you can modify how the discovery_agent probe data is used to determine the value for the field.

Deselecting the override option for a script, the default script will be used again.

Click **Apply** to activate any modification.

Note: A rule that is overridden will not be updated when upgrading to a newer version of the discovery_server with modified rules.



Service Discovery Setup

You can configure the service discovery using the *Service Discovery Setup* node in the discovery_server probe. You can define a custom network service to be used by discovery_agent probes to discover systems that respond to a particular network service. For example, you can define a service to find HTTP web servers in your network.

The discovery_server probe contains 16 pre-populated service discovery configurations.

The Right Pane

The right pane contains either the rule script for a selected Computer System Rule Set or the configuration settings for a selected Service Discovery Setup.

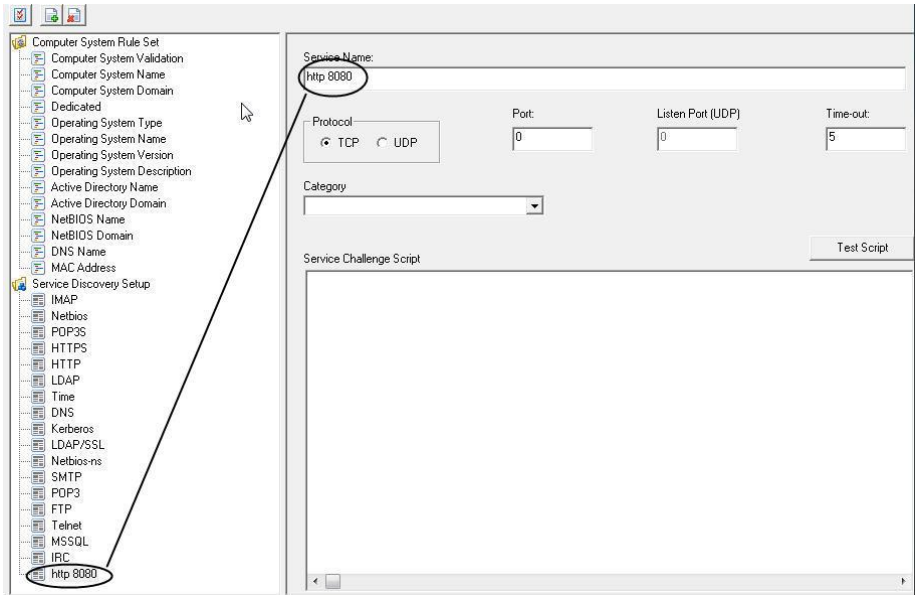
Adding and Configuring a Service

To add and configure a new service:

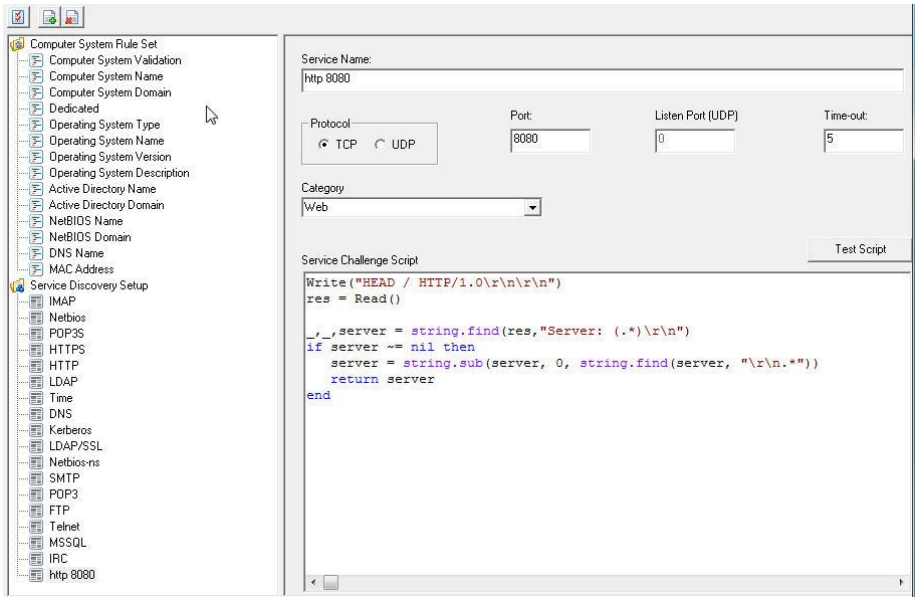
1. From the discovery_server toolbar, click the **Add Service** button.

   A new service item is added to the bottom of the list under *Service Discovery Setup*.

2. Enter a name for the service.



3. Select the protocol as either **TCP** or **UDP**.
4. Enter the port number for sending data.
5. Do not change the **Listen Port (UDP)** field. This field is currently ignored, and a default local port is used.
6. In the **Time-out** field, enter the number of seconds after which the service will time out.
7. From the **Category** drop-down, select a category for the service. If a category is not already listed, enter the required category name.
8. In the **Service Challenge Script** field, enter the script for Service.



9. Click **Test Script** to verify the script works as intended.

   See Verifying the Script (see page 37) for more information.

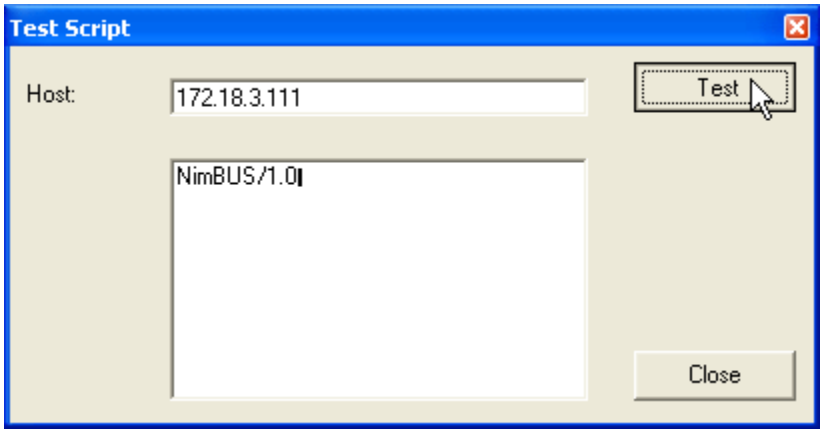
10. Click **Apply** to save the configuration changes.

Verifying the Script

To verify the script:

1. Select the service you want to verify the script.
2. In the right pane, click the **Test Script** button.

   The *Test Script* dialog opens.
3. In the *Host* field, enter the IP address of a target system running the service that you have defined.
4. Click the **Test** button.



   The return value or results of the script is displayed in the lower text box.

   Once you have verified your script is correct on a system that responds to the service you have defined, it is recommended that you also try the script on a system that is not running the service to test the non-responding case.
5. Click the **Close** button to close the Test Script dialog.

Editing a Service Discovery Configuration

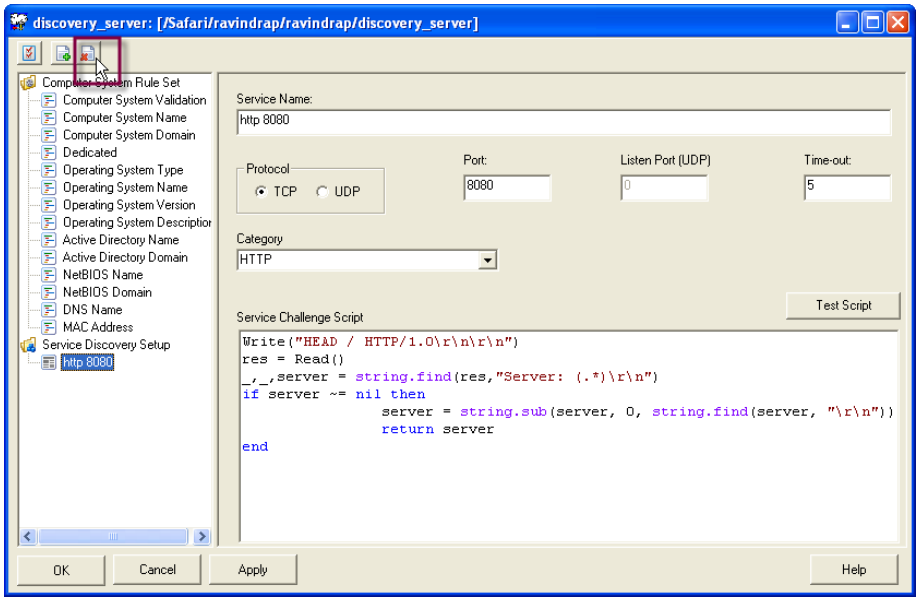
To edit an existing service discovery configuration:

1. Select the service discovery configuration you want to edit.
2. In the right pane modify the fields as appropriate.
3. Click Test Script to verify the script works as intended.

   See Verifying the Script (see page 37) for more information.
4. Click **Apply** to save the configuration changes.

Deleting a Service

1. From the tree view in the discovery_server UI, select the service to be deleted.
2. Click the **Delete Service** button.



3. Click **Ok**.

   A message appears asking for confirmation.
4. Click **Yes** to delete the service.

Advanced Configuration

This section provides information for making advanced configuration changes using the Raw Configure option for the discovery_server probe.

Java Heap Size

The default maximum Java heap size is set to 1 GB. For systems with more than 300,000 QoS objects the maximum Java heap size should be increased to 1.5 GB. For systems with more than 1,000,000 QoS objects the maximum Java heap size should be increased to 2.5 GB.

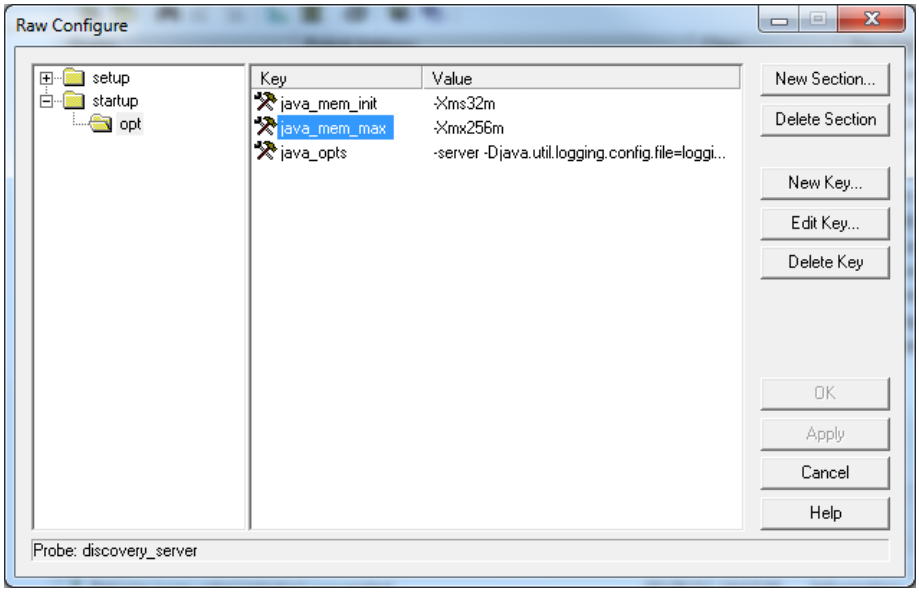
To determine the number of QoS objects, run the following query:

```
select count(*) from S_QOS_DATA;
```

To set the maximum Java heap size:

1. In Infrastructure Manager, hold the Shift key and right-click on the discovery_server probe.

2. Select **Raw Configure**.
3. In the left navigation double-click **startup**, then double-click **opt**.
4. In the content window select **java_mem_max** and click the **Edit Key** button.



5. Enter the new value using increments of 1024 MB.
   - 1 GB = -Xmx1024m
   - 2 GB = -Xmx2048m

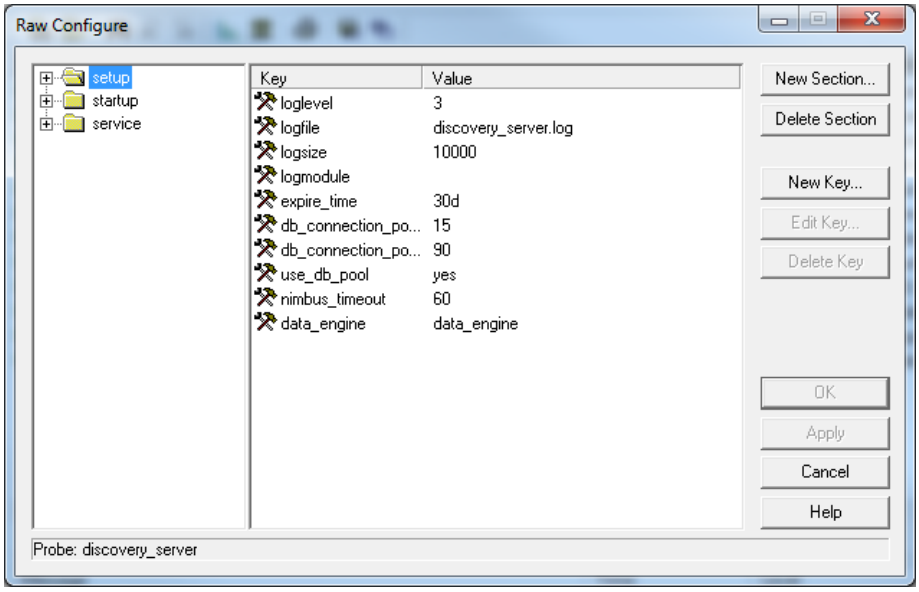
Running discovery_server on a Robot Other Than the Primary Hub

By default, the discovery server runs on the primary hub, which is the same robot where the data_engine is running. The discovery server can run on a different robot as long as the discovery server can communicate with the data_engine probe and the database server in its new location. To run the discovery server on a different robot other than the primary hub, please follow the steps below.

1. Deactivate or delete the discovery server on the primary hub. Only one instance of the discovery server should be running.
2. In Infrastructure Manager, right click on the discovery_server probe on the secondary hub.

Select Raw Configure.

In the content window select data_engine and click the Edit Key button.



1. Specify the full data_engine probe address. You can look up the data_engine address in Infrastructure Manager under the primary hub's SLM category. For example: /my_domain/my_primary_hub/my_primary_robot/data_engine.
2. Activate or restart the discovery_server in its new location.

Appendix B: Discovery Agent Probe

This section covers the discovery_agent probe.

This section contains the following topics:

discovery_agent Overview

The discovery_agent is responsible for collecting as much information as possible about the networked computer systems that it finds. This probe uses known protocols and user-defined services to accomplish this task.

The discovery_server probe collects the system information from all the discovery_agent probes in the network and stores it into the NIS database.

The discovery_agent probes can be configured in multiple locations within the Nimsoft system:

- **Nimsoft Discovery Wizard portlet:** You can define discovery network scopes and authentication credential profiles through this portlet. For more information, refer to the Discovery Wizard online help.
- **Discovery_server probe configuration:** You can configure the service discovery that is performed by the discovery agents. For more information, see the probe documentation for discovery_server.
- **Discovery_agent probe configuration:** You can configure the operation of the protocols used for the discovery_agent probe.

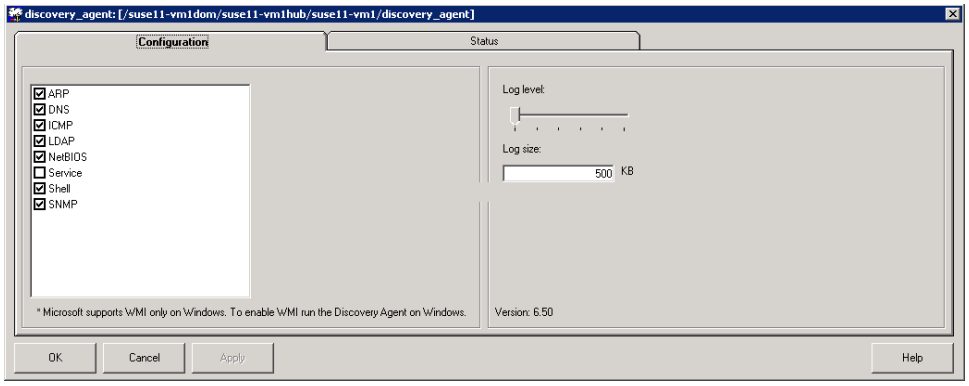
discovery_agent GUI

The Discovery configuration GUI contains the following tabs:

- Configuration (see page 42)
- Status (see page 44)

Configuration Tab

This tab defines the discovery settings and the log properties for the discovery_agent probe. The parameters listed in the center of the screen change settings for each individual protocol in the left column.



The log section of the Configuration tab contains:

Log level

Sets the level of details written to the log file. Log as little as possible during normal operation, to minimize disk consumption.

Log size

Set the size of the probe's log file to which probe-internal log messages are written. The default size is 500 KB.

When this size is reached, the contents of the file are cleared.

These protocols have no configuration options available in the GUI:

ARP

DNS

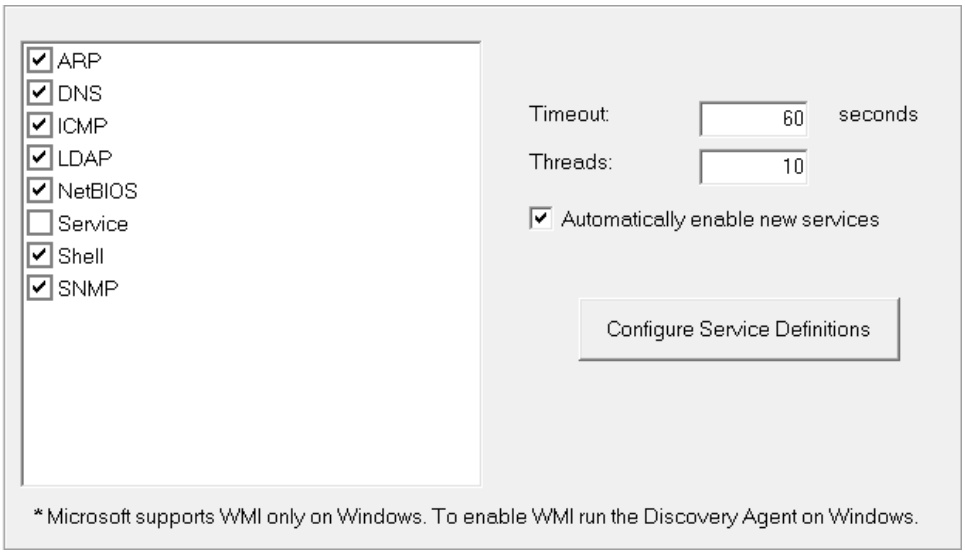
ICMP

LDAP

NetBIOS

Service

Allows you to enable or disable service definitions for this robot.



Timeout

Number of seconds a search lasts before giving up.

Threads

The maximum number of concurrent requests.

Automatically enable new services

Allows new service definitions that are defined on the discovery_server to be enabled on this discovery_agent.

Configure Service Definitions button

Allows you to enable or disable services on this discover_agent. If you want to change the service definitions you must edit the configuration from within the discovery_server probe.

Shell (telnet or SSH)

The parameters to be set for the Shell (telnet or SSH) are:

Timeout

Number of seconds a search lasts before giving up.

Threads

The maximum number of concurrent requests. Default is 10.

Note: Shell requires username and password credentials for authentication. Use the Discovery Wizard portlet in USM to view and edit the current settings.

Simple Network Management Protocol (SNMP)

The parameters to be set for the Simple Network Management Protocol (SNMP) are:

Timeout

Number of seconds a search lasts before giving up.

Threads

The maximum number of concurrent requests.

Windows Management Instrumentation (WMI)

WMI discovery can only run when the discovery_agent runs on a Windows platform.

The parameters to be set for the Windows Management Instrumentation (WMI) method are:

Timeout

Number of seconds that a search lasts before giving up.

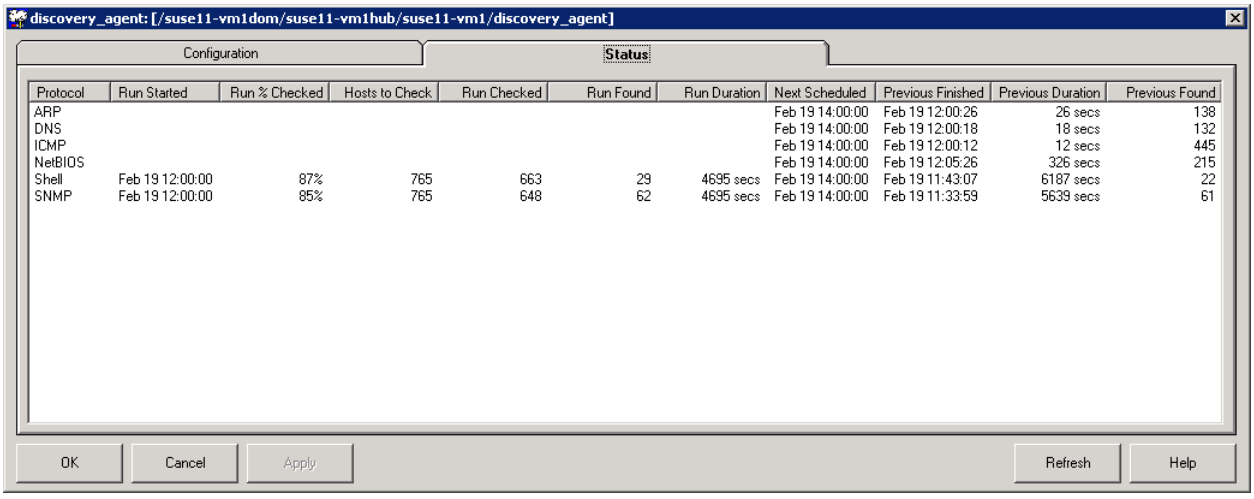
Threads

The maximum number of concurrent requests.

Note: WMI requires username and password credentials for authentication. Use the Discovery Wizard portlet in USM to view and edit the current settings.

Status Tab

This tab lists the systems discovered by the discovery_agent probe.



The count that shows up in the Checked column varies by protocol. Some of the protocols report a count that contains all possible addresses on the configured networks. Some protocols have advanced logic and only check systems which discovery has determined might potentially respond.

Appendix C: cm_data_import Probe

This section covers the cm_data_import probe.

This section contains the following topics:

cm_data_import Overview

The cm_data_import probe supports the feature of CA Nimsoft Discovery called *file-based import*. This provides a convenient way to import device description data into the discovery database. The cm_data_import probe processes device data in an XML file that your prepare. It can be initiated in two ways:

- Open a file browser from the External node of the Discovery Wizard in USM, and choose an XML file on your local file system to process
- Copy an XML file into the import directory on the machine hosting the cm_data_import probe. The cm_data_import probe scans the directory on a configurable interval--if the probe finds a valid file it:
  - Processes it
  - Publishes the devices to the Nimsoft bus--the discovery_server receives this information and adds the devices to the device database.

Compared to automated discovery, file-based import provides an alternative means to populate the discovery inventory, without the overhead of scanning the IT environment.

Devices identified to CA Nimsoft Monitor in this way are visible in the USM interface, either under Groups, or listed under the **External** branch of the Discovery tree.

Note: Devices imported via file-based import are not reflected in the Nimsoft topology function.

Features

The cm_data_import probe provides:

- A configurable interval for processing the import directory
- An "import_now" command for immediate processing.
- The equivalent of an automated gateway from an external CMDB into the Nimsoft database (NIS). Configure the CMDB to export its device information in XML to the probe's import directory.

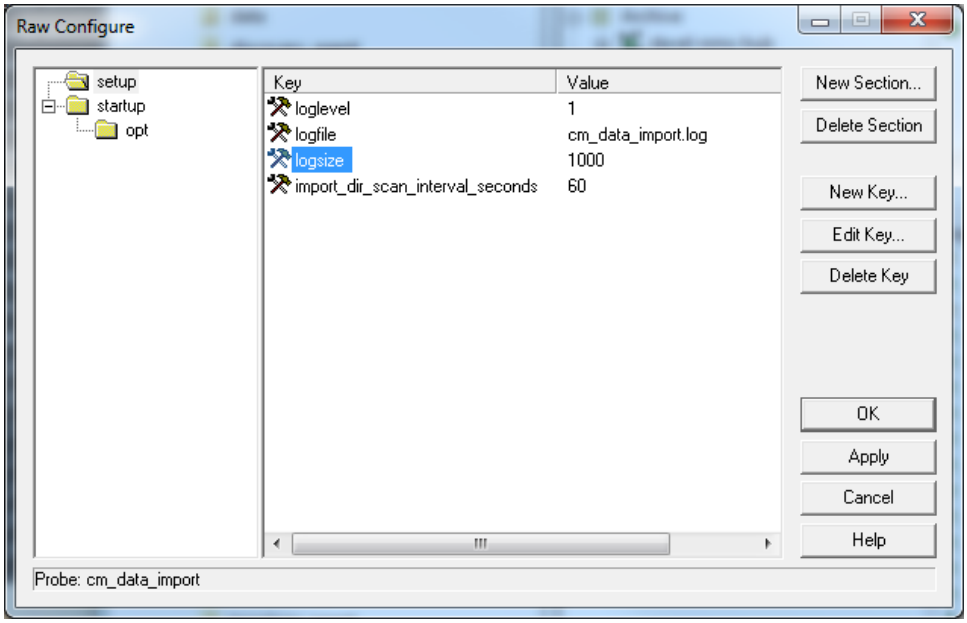
Requirements

The cm_data_import requires NMS 6.50 or higher.

Note: The cm_data_import probe must be co-located on the same hub as the discovery_server probe.

cm_data_import Configuration

The cm_data_import probe can only be configured using Raw Configure.



The key parameters are:

loglevel

Sets the level of details written to the log file. Log as little as possible during normal operation to minimize disk consumption, and increase the amount of detail when debugging. Default is 1.

logfile

Name of the log file.

logsize

The size of the log file.

import_dir_scan_interval_seconds

The amount of time between scans of the import directory. Default is 60 (seconds).

Import File Example

The cm_data_import probe scans the Nimsoft\Probes\Service\cm_data_import\import directory on regular intervals (default is 60 seconds). If it finds a file it will process it, then move it to a time-stamped subfolder in the

`Nimsoft\Probes\Service\cm_data_import\`**`processed`**

directory, logging the result of the process.

XML File Schema

To use file-based import, create an XML file with information about your computers or devices.

The XML file must include these required properties for each host or device:

- IP address - List both the IPv4 and IPv6 addresses if possible.
- Origin - Setting the origin correctly is important. See details on the Origin property in the table below.

Here is an example of XML that illustrates how to import one device with IP address 1.2.3.4 and origin "MyOrigin" in the database.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<DevicesToImport xmlns="http://nimsoft.com/2012/11/cm-data-import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <Device>
                <PrimaryIPV4Address>1.2.3.4</PrimaryIPV4Address>
                <Origin>myOrigin</Origin>
        </Device>
</DevicesToImport>
```

Additional optional properties can be included, as shown in the example below. You can also find this example file, named example1MaximalDevice.xml, in the <Nimsoft install directory>\Probes\Service\cm_data_import**schema** directory, located on the system that hosts the cm_data_import probe--typically the primary hub.

```
  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
  <DevicesToImport xmlns="http://nimsoft.com/2012/11/cm-data-import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <Device>
              <Origin>myOrigin</Origin>
              <Label>myComputer</Label>
              <Description>myComputer description goes here</Description>
              <PrimaryDnsName>myComputer.myCompany.com</PrimaryDnsName>
              <PrimaryIPV4Address>1.2.3.4</PrimaryIPV4Address>
              <PrimaryIPV6Address>fe80::223:ebff:fe06:9d40%10</PrimaryIPV6Address>
              <PrimaryMacAddress>F0-4D-A2-25-5B-7A</PrimaryMacAddress>
              <PrimaryOSType>WindowsServer-2008</PrimaryOSType>
              <PrimaryOSVersion>6.1.7601</PrimaryOSVersion>
              <ProcessorType>x86-64</ProcessorType>
              <Vendor>Dell Inc.</Vendor>
              <Model>PowerEdge T620</Model>
              <PhysSerialNumber>123-456-789-ABCD</PhysSerialNumber>
              <PrimaryDeviceRole>VirtualMachine</PrimaryDeviceRole>
              <PrimarySoftwareRole>DatabaseServer</PrimarySoftwareRole>
              <DBServerType>MSSQLServer</DBServerType>
              <WmiAuthId>3</WmiAuthId>
              <ShellAuthId>5</ShellAuthId>
              <SnmpAuthId>7</SnmpAuthId>
              <AppServerType>Unknown</AppServerType>
              <VirtualizationEnvironment>VMware</VirtualizationEnvironment>
              <MonitorFrom>monitoringRobotHostName</MonitorFrom>
       </Device>
</DevicesToImport>
```

The following table describes the XML properties. For properties that refer to open enumerations, navigate to <Nimsoft installation path>\Probes\Service\cm_data_import**schema** and open either **usm-openenums.xml** or **cm-data-import-openenums.xml** to view the defined values for each enumeration instance. It is strongly recommended you use values defined by the open enumerations, though not strictly required.

To deploy an agent or robot to an imported system using USM and ADE, some additional properties beyond IP address and origin are required. These are noted in the table below.

Property	Required?	Description
Origin	Yes	QoS data from probes are tagged with an origin name to identify the origin of the data. The origin name defaults to the Nimsoft hub name but can be overridden at the hub or robot (controller) in order to separate data in a multi-tenancy environment. To ensure that QoS data from probes is correlated to this device, the origin name specified here should match the origin name you intend to use in your Nimsoft infrastructure of hubs and robots.
Label	No	A short description or caption.
Description	No	Text description of the device.
PrimaryDnsName	No	The entity's Domain System Name, which may be used for correlation.
PrimaryIPV4Address	An IP address, either IPv4 or IPv6, is required	An IPv4 address for the entity that may be used for correlation and identity. Both this and the IPv6 address should be provided, if possible.
PrimaryIPV6Address	An IP address, either IPv4 or IPv6, is required	An IPv6 address for the entity that may be used for correlation and identity. The address is expressed using the formal, complete IPv6 notation (8 groups of up to 4 hex digits, using only uppercase where applicable, separated by colons). Both this and the IPv4 address should be provided, if possible.

Property	Required?	Description
PrimaryMacAddress	No	A MAC address for the entity that may be used for correlation and identity. The address is expressed as 6 groups of 2 hex digits (using only uppercase), separated by dashes.
PrimaryOSType	Required by ADE for robot deployment	OS type, defined by the open enumeration OSTypeEnum. For Linux, the Linux distribution name is required by ADE (for example, **Linux-RedHat**).
PrimaryOSVersion	No	OS version details.
ProcessorType	Required by ADE for robot deployment	Processor environment/type (such as "x86") as defined by the open enumeration ProcessorEnvironmentEnum.
Vendor	No	The hardware vendor/manufacturer's name, as defined by the open enumeration VendorEnum.
Model	No	The hardware model name/number.
PhysSerialNumber	No	An identifying string assigned by the hardware manufacturer and printed on a tag attached to the component. The data for this element should be input directly from the manufacturer's tag on the component (which may be an RFID tag), or read from the entPhysicalSerialNum field of SNMP's Entity-MIB. Note that a virtual entity would NOT have a PhysSerialNumber.
PrimaryDeviceRole	No	The device role as defined by the open enumeration DeviceRoleEnum.
PrimarySoftwareRole	No	The software role as defined by the open enumeration SoftwareRoleEnum.
DBServerType	No	The type of database server of which this is an instance, defined by the open enumeration DBServerTypeEnum.
AppServerType	No	The type of application server, as defined by the open enumeration AppServerTypeEnum.

Property	Required?	Description
VirtualizationEnvironment	No	Value indicating the specific virtualization environment (hypervisor manager) of a hypervisor or virtual system. Values are defined in the open enumeration VirtualizationTypeEnum.
WmiAuthId	Either WmiAuthId or ShellAuthID is required by ADE for robot deployment	A Nimsoft defined authentication profile ID to use for WMI access. This is the ID field in the WMI authentication profile.
ShellAuthId	Either WmiAuthId or ShellAuthID is required by ADE for robot deployment	A Nimsoft defined authentication profile ID to use for SSH or telnet access. This is the ID field in the Shell authentication profile.
SnmpAuthId	No	A Nimsoft defined authentication profile ID to use for SNMP access. This is the ID field in the SNMP authentication profile.
MonitorFrom	No	If the device will be remotely monitored, this specifies the system to monitor this device from. The value can be specified as an IP address, simple host name, fully qualified domain name or Nimsoft address (/NimsoftDomain/HubName/RobotName). A Nimsoft robot should be installed on the system specified here. If the robot is not installed, this device will not be imported. The origin name used by the robot should match the origin specified for this device to ensure that QoS data from probes is correlated with this device.