

Novell eDirectory™

8.7.3

March 18, 2008

INSTALLATION GUIDE

www.novell.com



Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to www.novell.com/info/exports/ for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2008 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.novell.com/company/legal/patents/> and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

Novell eDirectory 8.7.3 Installation Guide
[March 18, 2008](#)

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc. in the United States and other countries.

eDirectory is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc. in the United States and other countries.

NMAS is a trademark of Novell, Inc.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Certificate Server is a trademark of Novell, Inc.

Novell Client is a trademark of Novell, Inc.

Novell Directory Services and NDS are registered trademarks of Novell, Inc. in the United States and other countries.

Novell Support Connection is a registered trademark of Novell, Inc. in the United States and other countries.

SUSE is a registered trademark of SUSE LINUX AG, a Novell company.

Third-Party Materials

All third-party trademarks are the property of their respective owners.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org>).

About This Book	3
1 Installing or Upgrading Novell eDirectory on NetWare	5
System Requirements	5
Prerequisites	6
Hardware Requirements	6
Forcing the Backlink Process to Run	7
Updating the eDirectory Schema for NetWare	7
Schema Extension in a Mixed Tree	9
Installing or Upgrading Novell eDirectory on NetWare	9
Installing or Upgrading Novell eDirectory 8.7.3 on NetWare	9
Installing NMAS Server Software	10
Installing NMAS Client Software	10
Installing into a Tree with Dotted Name Containers	10
2 Installing or Upgrading Novell eDirectory on Windows	13
System Requirements	13
Prerequisites	14
Hardware Requirements	14
Forcing the Backlink Process to Run	15
Updating the eDirectory Schema for Windows	15
Installing Novell eDirectory on Windows	16
Installing or Updating Novell eDirectory 8.7.3 on Windows NT, 2000, or Server 2003	16
Communicating with eDirectory through LDAP	18
Installing NMAS Server Software	21
Installing NMAS Client Software	21
Installing into a Tree with Dotted Name Containers	21
3 Installing or Upgrading Novell eDirectory on Linux	23
System Requirements	23
Prerequisites	24
Hardware Requirements	25
Forcing the Backlink Process to Run	25
Upgrading eDirectory	25
Installing eDirectory	26
Using SLP with eDirectory	26
Using the nds-install Utility to Install eDirectory Components	26
Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server	28
Using ndsconfig to Install a Linux Server into a Tree with Dotted Name Containers	30
Using the nmasinst Utility to Configure NMAS	31
4 Installing or Upgrading Novell eDirectory on Solaris	33
System Requirements	33
Prerequisites	33
Hardware Requirements	34
Forcing the Backlink Process to Run	34
Upgrading eDirectory	35
Installing eDirectory	35
Using SLP with eDirectory	35
Using the nds-install Utility to Install eDirectory Components	35
Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server	38
Using ndsconfig to Install a Solaris Server into a Tree with Dotted Name Containers	40
Using the nmasinst Utility to Configure NMAS	40
5 Installing or Upgrading Novell eDirectory on AIX	43
System Requirements	43
Prerequisites	43

Hardware Requirements	44
Forcing the Backlink Process to Run	44
Upgrading eDirectory	45
Installing eDirectory	45
Using SLP with eDirectory	45
Using the nds-install Utility to Install eDirectory Components	45
Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server	48
Using ndsconfig to Install an AIX Server into a Tree with Dotted Name Containers.	50
Using the nmasinst Utility to Configure NMAS	50
6 Migrating to eDirectory 8.7.3.10	53
Migrating to eDirectory 8.7.3 SP10 While Upgrading the Operating System	54
Migrating to eDirectory 8.7.3 SP10 Without Upgrading the Operating System	54
7 Uninstalling Novell eDirectory	57
Uninstalling eDirectory on NetWare	57
Reinstalling eDirectory	57
Uninstalling eDirectory on Windows.	57
Uninstalling eDirectory, ConsoleOne, and SLP DA	58
Uninstalling an Upgraded Version of eDirectory.	58
Uninstalling NICI	58
Uninstalling eDirectory on Linux, Solaris, or AIX	59
8 Configuring Novell eDirectory on Linux, Solaris, or AIX Systems	61
Configuration Utilities	61
The ndsconfig Utility	61
Using the Idapconfig Utility to Configure the LDAP Server and LDAP Group Objects.	61
Using the nmasinst Utility to Configure Novell Modular Authentication Service	61
Configuration Parameters	62
A Linux, Solaris, and AIX Packages for Novell eDirectory	67
B Configuring OpenSLP for eDirectory	71
Service Location Protocol	71
SLP Fundamentals	71
Novell Service Location Providers	72
User Agents	72
Service Agents	73
Configuration Parameters	73

About This Book

This Installation Guide describes how to install Novell® eDirectory™ 8.7.3. It is intended for network administrators, and contains the following sections:

- ◆ Chapter 1, “Installing or Upgrading Novell eDirectory on NetWare,” on page 5
- ◆ Chapter 2, “Installing or Upgrading Novell eDirectory on Windows,” on page 13
- ◆ Chapter 3, “Installing or Upgrading Novell eDirectory on Linux,” on page 23
- ◆ Chapter 4, “Installing or Upgrading Novell eDirectory on Solaris,” on page 33
- ◆ Chapter 5, “Installing or Updating Novell eDirectory on AIX,” on page 43
- ◆ Chapter 6, “Migrating to eDirectory 8.7.3.10,” on page 53
- ◆ Chapter 7, “Uninstalling Novell eDirectory,” on page 57
- ◆ Chapter 8, “Configuring Novell eDirectory on Linux, Solaris, or AIX Systems,” on page 61
- ◆ Appendix A, “Linux, Solaris, and AIX Packages for Novell eDirectory,” on page 67
- ◆ Appendix B, “Configuring OpenSLP for eDirectory,” on page 71

Additional Documentation

For documentation on managing and administering eDirectory, see the *Novell eDirectory 8.7.3 Administration Guide* (<http://www.novell.com/documentation/lg/edir873/index.html>).

Documentation Updates

For the most recent version of the *Novell eDirectory 8.7.3 Installation Guide*, see the [Novell eDirectory 8.7.3 Documentation](http://www.novell.com/documentation/lg/edir873/index.html) (<http://www.novell.com/documentation/lg/edir873/index.html>) Web site.

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items within a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as UNIX*, should use forward slashes as required by your software.

1

Installing or Upgrading Novell eDirectory on NetWare

Use the following information to install or upgrade Novell® eDirectory™ 8.7.3 on a NetWare® server:

- ◆ “System Requirements” on page 5
- ◆ “Prerequisites” on page 6
- ◆ “Hardware Requirements” on page 6
- ◆ “Forcing the Backlink Process to Run” on page 7
- ◆ “Updating the eDirectory Schema for NetWare” on page 7
- ◆ “Installing or Upgrading Novell eDirectory on NetWare” on page 9

System Requirements

- You can upgrade to eDirectory 8.7.3 on the following versions of NetWare:
 - ◆ NetWare 5.1 with [Support Pack 6](http://support.novell.com/filefinder/9331/index.html) (http://support.novell.com/filefinder/9331/index.html) or later
 - ◆ NetWare 6 with [Support Pack 3](http://support.novell.com/filefinder/13659/index.html) (http://support.novell.com/filefinder/13659/index.html) or later
 - ◆ NetWare 6.5 with [Support Pack 1](http://support.novell.com/filefinder/18197/index.html) (http://support.novell.com/filefinder/18197/index.html)

IMPORTANT: On NetWare 6.5, eDirectory 8.7.3 is only supported through the NetWare 6.5 SP 1 installation. You cannot install a standalone version of eDirectory 8.7.3 on NetWare 6.5 or NetWare 6.5 SP1.
- If you are using RCONSOLE, you will need a ConsoleOne® administrator workstation with the following:
 - ◆ 200 MHz or faster processor
 - ◆ 64 MB RAM minimum (128 MB recommended)
 - ◆ Novell Client™ for Windows NT/2000/XP version 4.9 or Novell Client for Windows 95/98 version 3.4
- Administrative rights to the eDirectory tree so you can modify the schema

For information on hardware requirements, see “Hardware Requirements” on page 6.

Prerequisites

- ❑ If you are installing into an eDirectory tree that has NetWare and Windows servers, each NetWare server must be running one of the following:
 - ◆ NetWare 4.2 with Support Pack 9 or later and NDS[®] 6.21 or later
NDS 6.21 can be downloaded from the [Novell Support \(http://support.novell.com/produpdate/patchlist.html#nds\)](http://support.novell.com/produpdate/patchlist.html#nds) Web site. The filename is ds621.exe.
 - ◆ NetWare 5.0 with [Support Pack 6a or later \(http://support.novell.com/filefinder/5611/index.html\)](http://support.novell.com/filefinder/5611/index.html)
 - ◆ NetWare 5.1 with [Support Pack 5 \(http://support.novell.com/filefinder/9331/index.html\)](http://support.novell.com/filefinder/9331/index.html) or later
 - ◆ NetWare 6 with [Support Pack 2 \(http://support.novell.com/filefinder/13659/index.html\)](http://support.novell.com/filefinder/13659/index.html) or later
 - ◆ NetWare 6.5

Each Windows server must be running NDS eDirectory 8.0 or later.

IMPORTANT: There is an issue when installing NetWare 6.5 into a replica ring that contains NDS 7.x which results in a failed install with the error “-609 Missing Mandatory.” This issue is resolved with NDS 7.62b. NDS 7.62b has only been tested on NetWare 5.1. Because NetWare 5.0 is a discontinued product (see [Novell Products - Support Life Cycle \(http://support.novell.com/lifecycle\)](http://support.novell.com/lifecycle)), NDS 7.62b has not been thoroughly tested on NetWare 5.0. Novell has performed very limited testing on NDS 7.62b running NetWare 5.0 for upgrade purposes only. Novell will support, on a limited basis, NDS 7.62b running on NetWare 5.0 when upgrading to NetWare 6.5. If issue outside of the upgrade arise that are specific to the NetWare 5.0 operating system, upgrading from NetWare 5.0 to NetWare 5.1 will be required in order to resolve the issue.

- ❑ Before installing eDirectory 8.7.3 into an existing tree, NCI 2.4.2 or later must be installed on every server in the tree. This version of NCI is not in the latest NetWare Support Packs, and must be downloaded and applied after the Support Packs are installed. You can download the latest version of NCI (Novell International Cryptographic Infrastructure) from [Novell Product Downloads \(http://download.novell.com\)](http://download.novell.com).

Hardware Requirements

Hardware requirements depend on the specific implementation of eDirectory.

For example, a base installation of eDirectory with the standard schema requires about 74 MB of disk space for every 50,000 users. However, if you add a new set of attributes or completely fill in every existing attribute, the object size grows. These additions affect the disk space, processor, and memory needed.

Two factors increase performance: more cache memory and faster processors.

For best results, cache as much of the DIB Set as the hardware allows.

eDirectory scales well on a single processor. However, Novell eDirectory 8.7 takes advantage of multiple processors. Adding processors improves performance in some areas—for example, logins and having multiple threads active on multiple processors. eDirectory itself is not processor intensive, but it is I/O intensive.

The following table illustrates typical system requirements for eDirectory for NetWare:

Objects	Processor	Memory	Hard Disk
100,000	Pentium* III 450-700 MHz (single)	384 MB	144 MB
1 million	Pentium III 450-700 MHz (dual)	2 GB	1.5 GB
10 million	Pentium III 450-700 MHz (2 to 4)	2+ GB	15 GB

Requirements for processors might be greater than the table indicates, depending upon additional services available on the computer as well as the number of authentications, reads, and writes that the computer is handling. Processes such as encryption and indexing can be processor intensive.

Of course, faster processors improve performance. Additional memory also improves performance because eDirectory can then cache more of the directory into memory.

Forcing the Backlink Process to Run

Because the internal eDirectory identifiers change when upgrading to Novell eDirectory, the backlink process must update backlinked objects for them to be consistent.

Backlinks keep track of external references to objects on other servers. For each external reference on a server, the backlink process ensures that the real object exists in the correct location and verifies all backlink attributes on the master of the replica. The backlink process occurs two hours after the database is open and then every 780 minutes (13 hours). The interval is configurable from 2 minutes to 10,080 minutes (7 days).

After migrating to eDirectory, we recommend that you force the backlink to run by issuing the following commands from the server console. Running the backlink process is especially important on servers that do not contain a replica.

- 1** At the server console, enter `set dstrace=on`.
- 2** Enter `set dstrace+=blink`.
- 3** Enter `set dstrace=*b`.
- 4** When the process is complete, enter `set dstrace=off`.

Updating the eDirectory Schema for NetWare

When upgrading a NetWare server to eDirectory 8.7.3, you might need to update the eDirectory schema by running DSRepair on the server that has the master replica of the root partition.

IMPORTANT: If the master replica of the root partition resides on a Windows server, follow the instructions in [“Updating the eDirectory Schema for Windows” on page 15](#).

If one or both of the following conditions exist, you must run dsrepair.nlm before installing the first eDirectory server in your tree:

- ◆ Any NetWare 5 server in your eDirectory tree is running eDirectory 8.
- ◆ Your first installation of eDirectory is on a NetWare 5.1 or later server that does not hold a writable replica of the eDirectory 8.7.3 root partition.

To update the schema:

- 1 Copy the appropriate dsrepair.nlm file from the product CD (or downloaded and expanded file) to the sys:\system directory of the server that contains the master replica of the Tree partition.

For This Version of NetWare	With This Version of NDS	Copy
4.11 or 4.2	6.17 or later	patches\dsrepair\ nw4x\dsrepair.nlm
5.0 or later	NDS 7, version 7.47 or later	patches\dsrepair\ nw5x\dsrepair.nlm
5.0 or later	8.11 or 8.17	(Not supported)
5.0 or later	NDS eDirectory 8, version 8.51 or later	patches\dsrepair\ nwnds8\dsrepair.nlm
	IMPORTANT: You don't need to run this version of DSRepair with Novell eDirectory 8.6, version 103xx.xx, or Novell eDirectory 8.7, version 104xx.xx.	

- 2 At the server console of the master replica of the root partition, load dsrepair.nlm.
- 3 Select Advanced Options Menu > Global Schema Operations.
- 4 Enter the Administrator's name (for example, Admin.VMP) and password.
- 5 Select Post NetWare 5 Schema Update > Yes.

dsrepair.nlm updates the schema and posts the results to the dsrepair.log file.

Ignore errors associated with adding object classes. dsrepair.nlm is simply applying the Post NetWare 5 Schema Update changes to each object.

- 6 Copy the appropriate patch version of dsrepair.nlm to each NetWare server in the eDirectory tree.

Use the table in [Step 1](#) as a reference. Having a correct version on each server ensures that the schema needed for eDirectory is properly maintained when dsrepair.nlm is run in the future.

If you use an earlier version of dsrepair.nlm and select Rebuild Operational Schema, schema enhancements made by the Post NetWare 5 Schema Update will be lost. To resolve lost schema enhancements, run dsrepair.nlm according to the following table.

If You Are Running DSREPAIR.NLM From Here	Then
A server that holds a writable replica of the root partition	Reapply the Post NetWare 5 Schema Update to your eDirectory tree.
From any other server	Select Advanced Options > Global Schema Operations > Request Schema from Tree.

This action resynchronizes the schema from the root of the tree.

- 7 Close dsrepair.nlm before installing eDirectory on the server.
If dsrepair.nlm is loaded, the server might not restart.

Schema Extension in a Mixed Tree

On NetWare, the schema for the native HTTP stack is not extended at the time of installation. But on Windows NT and UNIX platforms, schema extension is done during the installation using `httpstk.sch`.

If the tree contains NetWare servers and other platforms, use NWConfig on the NetWare server to extend the schema, using the `\nt\I386\NDSonNT\ndsnt\nds\httpstk.sch` file.

- 1 At the server console, load `nwconfig.nlm`.
- 2 Select Directory Options > Extend Schema.
- 3 Enter an administrator name and password.
- 4 Press F3 (F4 if you're using RCONSOLE) and specify the path to the `\nt\I386\NDSonNT\ndsnt\nds\httpstk.sch` file (on CD, or downloaded from the Web).
- 5 Press Enter.

Installing or Upgrading Novell eDirectory on NetWare

This section contains the following information:

- ♦ “Installing or Upgrading Novell eDirectory 8.7.3 on NetWare” on page 9
- ♦ “Installing NMAS Server Software” on page 10
- ♦ “Installing NMAS Client Software” on page 10
- ♦ “Installing into a Tree with Dotted Name Containers” on page 10

Installing or Upgrading Novell eDirectory 8.7.3 on NetWare

- 1 At the server console, enter `nwconfig.nlm`.
- 2 Select Product Options > Install a Product Not Listed.
- 3 Press F3 (F4 if you're using RCONSOLE) and specify the path to the NW directory where the installation program can find the `nds8.ips` file.
 - ♦ If you downloaded eDirectory from the Web, enter the path to the NW directory you extracted from the downloaded file (for example, `sys:\edir\nw`).
 - ♦ If you are installing from a CD, mount the CD as a volume and enter `volume_name:NW` (for example, `edir_871:NW`).

For information on mounting a CD as a volume, see “CD-ROMs as Logical Volumes” (http://www.novell.com/documentation/lg/nw6p/nss_enu/data/htxx7fd6.html) in the *Novell Storage Services Administration Guide*.

- 4 Follow the on-screen prompts concerning license agreements, the Readme file, and tips.
- 5 Enter the administrator’s login name (for example, Admin.VMP) and password.

IMPORTANT: This window might close before you enter this information. If it does, toggle (Alt+Esc) to the screen and enter the information. Otherwise, the installation will not be complete.
- 6 In the LDAP Configuration screen, specify which LDAP ports to use, then click Next.

For more information, see “Communicating with eDirectory through LDAP” on page 18.
- 7 Select the NMAS™ login method you want to install, then click Next.

See “Installing NMAS Server Software” on page 10 and “Installing NMAS Client Software” on page 10 for more information.

- 8** Select a language for the installation, then click Next.
- 9** Select the ConsoleOne components you want to install, then click Next.
- 10** Click Finish to start the eDirectory installation.
ConsoleOne 1.3.6 is installed as part of the eDirectory installation.
- 11** To complete the installation, remove any diskettes or CDs when prompted, then click Yes to restart the server.

Installing NMAS Server Software

Novell Modular Authentication Service™ (NMAS) server components are installed automatically when you run the eDirectory installation program. You will need to select the login methods you want to install.

Select the login methods that you want to install into eDirectory by checking the appropriate check boxes. When you select a login method, a description of the component appears in the Description box. For more information on login methods, see “Managing Login and Post-Login Methods and Sequences” (<http://www.novell.com/documentation/lg/nmas23/admin/data/a53vj9a.html>) in the *Novell Modular Authentication Service Administration Guide*.

Click Select All if you want to install all the login methods into eDirectory. Click Clear All if you want to clear all selections.

The NDS login method is installed by default.

Installing NMAS Client Software

The NMAS client software must be installed on each client workstation where you want to use the NMAS login methods.

- 1** At a Windows client workstation, insert the *Novell eDirectory 8.7.3 CD*.
- 2** From the NMAS directory, run `nmasinstall.exe`.
- 3** Select the NMAS Client Components checkbox.
Optionally, you can select the NICI checkbox if you want to install this component.
- 4** Click OK and follow the on-screen instructions.
- 5** Reboot the client workstation after the installation completes.

Installing into a Tree with Dotted Name Containers

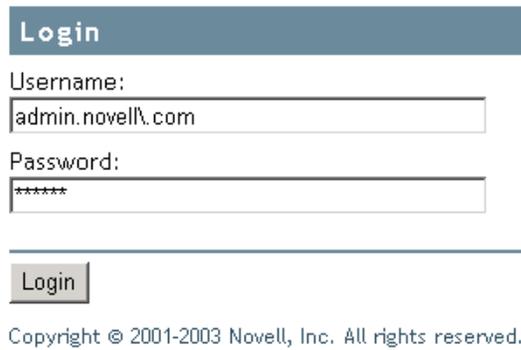
You can install a NetWare server into an eDirectory tree that has containers with dots in the names (for example, O=novell.com or C=u.s.a). Using containers with dotted names requires that those dots be escaped with the backslash character. To escape a dot, simply put a backslash in front of any dot in a container name. For example:

```
O=novell\.com
```

You cannot start a name with a dot. For example, you cannot create a container named “.novell” because it starts with a dot (‘.’).

IMPORTANT: If your tree has containers with dotted names, you must escape those names when logging into utilities such as iMonitor, iManager, and DHost iConsole. For example, if your tree has “novell.com” as the name of the O, enter *username.novell\.*com in the Username field when logging in to iMonitor (see [Figure 1](#)).

Figure 1 iMonitor Login Screen



Login

Username:
admin.novell\.

Password:

Login

Copyright © 2001-2003 Novell, Inc. All rights reserved.

2

Installing or Upgrading Novell eDirectory on Windows

Use the following information to install or upgrade Novell® eDirectory™ 8.7.3 on a Windows* NT*, Windows 2000, or Windows Server 2003:

- ♦ “System Requirements” on page 13
- ♦ “Prerequisites” on page 14
- ♦ “Hardware Requirements” on page 14
- ♦ “Forcing the Backlink Process to Run” on page 15
- ♦ “Updating the eDirectory Schema for Windows” on page 15
- ♦ “Installing Novell eDirectory on Windows” on page 16

IMPORTANT: Novell eDirectory 8.7.3 lets you install eDirectory for Windows without the Novell Client™. If you install eDirectory 8.7.3 on a machine already containing the Novell Client, eDirectory will use the existing Client. For more information, see “Installing or Updating Novell eDirectory 8.7.3 on Windows NT, 2000, or Server 2003” on page 16.

System Requirements

- One of the following:
 - ♦ Windows NT Server 4.0 with Service Pack 6 or later
 - ♦ Windows 2000 Server with Service Pack 4 or later
 - ♦ Windows Server 2003
- IMPORTANT:** Windows XP is not a supported Novell eDirectory 8.7.3 platform.
- An assigned IP address.
- A Pentium 200 with a minimum of 64 MB RAM (128 MB recommended) and a monitor color palette set to a number higher than 16.
- (Optional) One or more workstations running one of the following:
 - ♦ Novell Client for Windows 95/98 version 3.4
 - ♦ Novell Client for Windows NT/2000/XP version 4.9
- Administrative rights to the Windows server and to all portions of the eDirectory tree that contain domain-enabled User objects. For an installation into an existing tree, you need administrative rights to the Tree object so that you can extend the schema and create objects.

Prerequisites

- ❑ Because NTFS provides a safer transaction process than a FAT file system provides, you can install eDirectory only on an NTFS partition. Therefore, if you have only FAT file systems, do one of the following:
 - ◆ Create a new partition and format it as NTFS.
Use Disk Administrator. Refer to *Windows NT Server User Guide* for more information.
 - ◆ Convert an existing FAT file system to NTFS, using the CONVERT command.
 - If your server only has a FAT file system and you forget or overlook this process, the installation program prompts you to provide an NTFS partition.
 - ❑ If you are upgrading to eDirectory 8.7.3, make sure you have the latest NDS and eDirectory patches installed on all non-eDirectory 8.7.3 servers in the tree. You can get NDS and eDirectory patches from the [Novell Support \(http://support.novell.com\)](http://support.novell.com) Web site.
 - ❑ Make sure you have the latest Windows NT, 2000, or 2003 Server Service Packs installed. The latest updated Windows Service Pack needs to be installed after the installation of the Windows SNMP service.
 - ❑ If you are installing into an eDirectory tree that has NetWare and Windows servers, each NetWare server must be running one of the following:
 - ◆ NetWare 4.2 with Support Pack 9 or later and NDS[®] 6.21 or later
NDS 6.21 can be downloaded from the [Novell Support \(http://support.novell.com/produpdate/patchlist.html#nds\)](http://support.novell.com/produpdate/patchlist.html#nds) Web site. The filename is ds621.exe.
 - ◆ NetWare 5.0 with [Support Pack 6a or later \(http://support.novell.com/filefinder/5611/index.html\)](http://support.novell.com/filefinder/5611/index.html)
 - ◆ NetWare 5.1 with [Support Pack 5 \(http://support.novell.com/filefinder/9331/index.html\)](http://support.novell.com/filefinder/9331/index.html) or later
 - ◆ NetWare 6 with [Support Pack 2 \(http://support.novell.com/filefinder/13659/index.html\)](http://support.novell.com/filefinder/13659/index.html) or later
 - ◆ NetWare 6.5
- Each Windows server must be running NDS eDirectory 8.0 or later.
- ❑ If you are upgrading from a previous version of eDirectory, it must be eDirectory 8.35 or later.

Hardware Requirements

Hardware requirements depend on the specific implementation of eDirectory.

For example, a base installation of eDirectory with the standard schema requires about 74 MB of disk space for every 50,000 users. However, if you add a new set of attributes or completely fill in every existing attribute, the object size grows. These additions affect the disk space, processor, and memory needed.

Two factors increase performance: more cache memory and faster processors.

For best results, cache as much of the DIB Set as the hardware allows.

eDirectory scales well on a single processor. However, Novell eDirectory 8.7.3 takes advantage of multiple processors. Adding processors improves performance in some areas—for example,

logins and having multiple threads active on multiple processors. eDirectory itself is not processor intensive, but it is I/O intensive.

The following table illustrates typical system requirements for Novell eDirectory for Windows NT and Windows 2000:

Objects	Processor	Memory	Hard Disk
10,000	Pentium III 450-700 MHz (single)	384 MB	144 MB
1 million	Pentium III 450-700 MHz (dual)	2 GB	1.5 GB
10 million	Pentium III 450-700 MHz (2 to 4)	2+ GB	15 GB

Requirements for processors might be greater than the table indicates, depending upon additional services available on the computer as well as the number of authentications, reads, and writes that the computer is handling. Processes such as encryption and indexing can be processor intensive.

Forcing the Backlink Process to Run

Because the internal eDirectory identifiers change when upgrading to eDirectory, the backlink process must update backlinked objects for them to be consistent.

Backlinks keep track of external references to objects on other servers. For each external reference on a server, the backlink process ensures that the real object exists in the correct location and verifies all backlink attributes on the master of the replica. The backlink process occurs two hours after the database is open and then every 780 minutes (13 hours). The interval is configurable from 2 minutes to 10,080 minutes (7 days).

After migrating to eDirectory, we recommend that you force the backlink to run by issuing the following commands from the server console. Running the backlink process is especially important on servers that do not contain a replica.

- 1** At the server command prompt, enter `set dstrace=on`.
- 2** Enter `set dstrace+=blink`.
- 3** Enter `set dstrace=*b`.
- 4** When the process is complete, enter `set dstrace=off`.

Updating the eDirectory Schema for Windows

To install eDirectory 8.7.3 into an existing tree, you might need to update the eDirectory schema by running DSRepair on the server that contains the master replica of the root partition.

IMPORTANT: If the master replica of the root partition resides on a NetWare server, follow the instructions in [“Updating the eDirectory Schema for NetWare” on page 7](#).

The eDirectory installation program checks the existing schema’s version. If the schema has not been upgraded, the installation program instructs you to run DSRepair and then discontinues.

- 1** Copy `patches\dsrepair\ntnds8\dsrepair.dll` from the product CD to the directory where you installed eDirectory (for example, `c:\novell\nds`).

This file is version 8.35.

- 2** Click Start > Settings > Control Panel > Novell eDirectory Services.

- 3** Select dsrepair.dlm in the Service list.
- 4** Enter `-ins` in the Startup Parameters field, then click Start.
After the schema has been updated, the Status field next to the dsrepair.dlm service will be blank.
- 5** To see the results of the schema update, select dsrepair.dlm, then click Start.
- 6** Click File > Open Log File > Open.
The last entry in the log file will contain the results of the schema update.

Installing Novell eDirectory on Windows

This section contains the following information:

- ♦ [“Installing or Updating Novell eDirectory 8.7.3 on Windows NT, 2000, or Server 2003” on page 16](#)
- ♦ [“Communicating with eDirectory through LDAP” on page 18](#)
- ♦ [“Installing NMAS Server Software” on page 21](#)
- ♦ [“Installing NMAS Client Software” on page 21](#)
- ♦ [“Installing into a Tree with Dotted Name Containers” on page 21](#)

Installing or Updating Novell eDirectory 8.7.3 on Windows NT, 2000, or Server 2003

You can install eDirectory 8.7.3 for Windows without the Novell Client. If you install eDirectory 8.7.3 on a machine already containing the Novell Client, eDirectory will use the existing Client, or update it if it is not the latest version.

- 1** At the Windows server, log in as Administrator or as a user with administrative privileges.
- 2** To resolve tree names, make sure that SLP is correctly configured on your network and that SLP DAs are stable.

For more information, see one of the following:

- ♦ [Appendix B, “Configuring OpenSLP for eDirectory,” on page 71](#)
 - ♦ [DHCP Options for Service Location Protocol \(http://www.openslp.org/doc/rfc/rfc2610.txt\)](http://www.openslp.org/doc/rfc/rfc2610.txt)
 - ♦ [OpenSLP Documentation \(http://www.openslp.org/#Documentation\)](http://www.openslp.org/#Documentation)
- 3** If you have Autorun turned off, run setup.exe from the NT directory on the *Novell eDirectory 8.7.3* CD or from the downloaded file.
 - 4** Select the components you want to install or upgrade.

You can install the following components separately or together.

- ♦ Install Novell eDirectory
Installs or upgrades eDirectory in a Windows-only or mixed server environment.
- ♦ Install Novell Client
Installs the Novell Client for Windows, or updates an existing version of the Novell Client.

5 Click Install.

The installation program checks for the following components before it installs eDirectory. If a component is missing or is an incorrect version, the installation program automatically launches an installation for that component.

- ◆ Novell eDirectory License

You can obtain an evaluation license file from the [Novell eDirectory Eval License Download \(http://www.novell.com/products/edirectory/licenses/eval_87.html\)](http://www.novell.com/products/edirectory/licenses/eval_87.html) Web site.

To purchase eDirectory licenses, see the [Novell eDirectory How To Buy \(http://www.novell.com/products/edirectory/howtobuy.html\)](http://www.novell.com/products/edirectory/howtobuy.html) Web site.

- ◆ NCI 2.6.4

For more information on the Novell International Cryptographic Infrastructure (NICI), see the [NICI Administration Guide \(http://www.novell.com/documentation/lg/nici20/index.html\)](http://www.novell.com/documentation/lg/nici20/index.html).

You might have to reboot the server after the NICI installation. The eDirectory installation will continue after the reboot.

- ◆ Novell Client for Windows NT/2000/XP.

IMPORTANT: The Novell Client is updated automatically if you have an older version of the Client already installed on the machine. For more information on the Client, see the [Novell Client for Windows \(http://www.novell.com/documentation/lg/nocienu/index.html\)](http://www.novell.com/documentation/lg/nocienu/index.html) online documentation.

6 Click Next to start the eDirectory installation.**7** View the license agreement, then click I Accept.**8** Select a language for the installation, then click Next.**9** Specify or confirm the installation path, then click Next.**10** (New installations only) Select an eDirectory installation type, then click Next.

- ◆ **Install eDirectory into an Existing Tree** incorporates this server into your eDirectory network. The server can be installed into any level of your tree.
- ◆ **Create a New eDirectory Tree** creates a new tree. Use this option if this is the first server to go into the tree or if this server requires a separate tree. The resources available on the new tree will not be available to users logged in to a different tree.

11 Provide information in the eDirectory Installation screen, then click Next.

- ◆ If you are installing a new eDirectory server, specify a Tree name, Server object context, and Admin name and password for the new tree.
- ◆ If you are installing into an existing tree, specify the Tree name, Server object context, and Admin name and password of the existing tree.
- ◆ If you are upgrading an eDirectory server, specify the Admin password.

For information on using dots in container names, see [“Installing into a Tree with Dotted Name Containers” on page 21](#).

12 (New installations only) In the HTTP Server Port Configuration page, specify the ports to use for the eDirectory administrative HTTP server, then click Next.

IMPORTANT: Make sure that the HTTP stack ports you set during the eDirectory installation are different than the HTTP stack ports you have used or will use for Novell iManager. For more information, see the [Novell iManager 2.0.x Administration Guide \(http://www.novell.com/documentation/lg/imanager20/index.html\)](http://www.novell.com/documentation/lg/imanager20/index.html).

- 13** (New installations only) In the LDAP Configuration page, specify which LDAP ports to use, then click Next.
- For more information, see [“Communicating with eDirectory through LDAP” on page 18](#).
- 14** Select the NMAS™ login methods you want to install, then click Next.
- See [“Installing NMAS Server Software” on page 21](#) and [“Installing NMAS Client Software” on page 21](#) for more information.
- 15** Click Finish to complete the eDirectory installation.

Communicating with eDirectory through LDAP

When you install eDirectory, you must select a port that the LDAP server monitors so that it can service LDAP requests. The following table lists options for various installations:

Installation	Option	Result
eDirectory 8.7.3	Clear text (port 389)	Selects port 389.
eDirectory 8.7.3	Encrypted (port 636)	Selects port 636.
eDirectory 8.7.3	Require TLS for simple bind	Keeps (on the LDAP Group object) a parameter asked about during installation.

Port 389, the Industry-Standard LDAP Clear-Text Port

The connection through port 389 is not encrypted. All data sent on a connection made to this port is clear. Therefore, a security risk exists. For example, LDAP passwords can be viewed on a simple bind request.

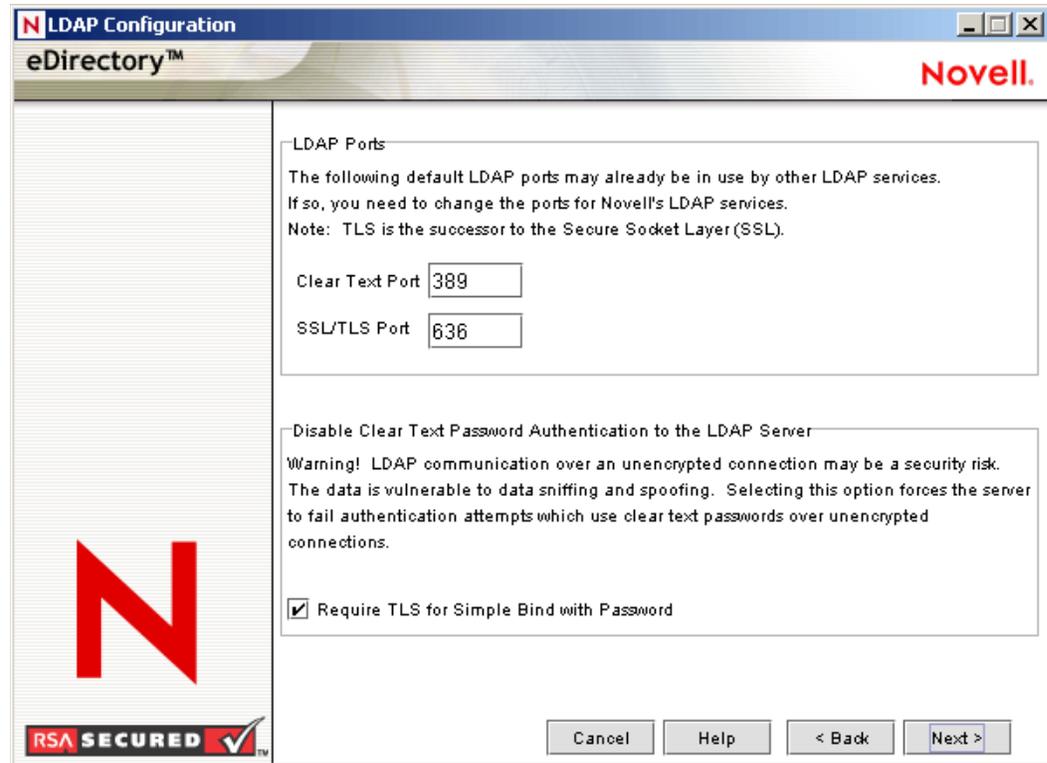
An LDAP Simple Bind requires only a DN and a password. The password is in clear text. If you use port 389, the entire packet is in clear text. By default, this option is disabled during the eDirectory installation.

Because port 389 allows clear text, the LDAP server services Read and Write requests to the Directory through this port. This openness is adequate for environments of trust, where spoofing doesn't occur and no one inappropriately captures packets.

To disallow clear passwords and other data, select the Require TLS for Simple Bind with Password option during installation.

As the following figure illustrates, the page gives defaults of 389, 636, and Require TLS for Simple Bind with Password.

Figure 2 Defaults for the LDAP Configuration Screen



Scenario: Require TLS for Simple Bind Is Enabled: Olga is using a client that asks for a password. After Olga enters a password, the client connects to the server. However, the LDAP server does not allow the connection to bind to the server over the clear-text port. Everyone is able to view Olga's password, but Olga is unable to get a bound connection.

The Require TLS for Simple Bind discourages users from sending observable passwords. If this setting is disabled (that is, not checked), users are unaware that others can observe their passwords. This option, which does not allow the connection, only applies to the clear-text port.

If you make a secure connection to port 636 and have a simple bind, the connection is already encrypted. No one can view passwords, data packets, or bind requests.

Port 636, the Industry-Standard Secure Port

The connection through port 636 is encrypted. TLS (formerly SSL) manages the encryption. By default, the eDirectory installation selects this port.

The following figure illustrates the selected port.

Figure 3 LDAP Server Connections Page in iManager

The screenshot shows the 'LDAP Server Connections Page in iManager'. At the top, there is a 'General' tab and a navigation bar with links for 'Information', 'Connections', 'Searches', 'Events', 'Tracing', and 'Referrals'. Below this is the 'Transport Layer Security (TLS / SSL)' section, which includes fields for 'Server Certificate' (set to 'SSL CertificateDNS'), 'Client Certificate' (set to 'Not Requested'), and 'Trusted Root Containers'. There are also two checkboxes: 'Require TLS for all operations' (unchecked) and 'Enable and require mutual authentication' (checked). Below this is the 'Ports' section, which has two checkboxes: 'Enable Encrypted Port' (checked) and 'Enable Non-Encrypted Port' (checked). The 'Port' field for the encrypted port is set to '636'.

A connection to port 636 automatically instantiates a handshake. If the handshake fails, the connection is denied.

IMPORTANT: This default selection might cause a problem for your LDAP server. If a service already loaded on the host server (before eDirectory was installed) uses port 636, you must specify another port.

Installations earlier than eDirectory 8.7 treated this conflict as a fatal error and unloaded nldap.nlm. The eDirectory 8.7.3 installation loads nldap.nlm, places an error message in the dstrace.log file, and runs without the secure port.

Scenario: Port 636 Is Already Used: Your server is running Active Directory*. Active Directory is running an LDAP program, which uses port 636. You install eDirectory. The installation program detects that port 636 is already used and doesn't assign a port number for the Novell LDAP server. The LDAP server loads and appears to run. However, because the LDAP server does not duplicate or use a port that is already open, the LDAP server does not service requests on any duplicated port.

If you are not certain that port 389 or 636 is assigned to the Novell LDAP server, run the ICE utility. If the Vendor Version field does not specify Novell, you must reconfigure LDAP Server for eDirectory and select a different port. See [“Verifying That the LDAP Server Is Running”](#) in the *Novell eDirectory 8.7.3 Administration Guide* for more information.

Scenario: Active Directory Is Running: Active Directory is running. Clear-text port 389 is open. You run the ICE command to port 389 and ask for the vendor version. The report displays Microsoft*. You then reconfigure the Novell LDAP server by selecting another port, so that the eDirectory LDAP server can service LDAP requests.

Novell iMonitor can also report that port 389 or 636 is already open. If the LDAP server isn't working, use Novell iMonitor to identify details. See [“Verifying That the LDAP Server Is Running”](#) in the *Novell eDirectory 8.7.3 Administration Guide* for more information.

Installing NMAS Server Software

Novell Modular Authentication Service™ (NMAS) server components are installed automatically when you run the eDirectory installation program. You will need to select the login methods you want to install.

Select the login methods that you want to install into eDirectory by checking the appropriate check boxes. When you select a login method, a description of the component appears in the Description box. For more information on login methods, see “[Managing Login and Post-Login Methods and Sequences](http://www.novell.com/documentation/lg/nmas23/admin/data/a53vj9a.html)” (<http://www.novell.com/documentation/lg/nmas23/admin/data/a53vj9a.html>) in the *Novell Modular Authentication Service Administration Guide*.

Click Select All if you want to install all the login methods into eDirectory. Click Clear All if you want to clear all selections.

The NDS login method is installed by default.

Installing NMAS Client Software

The NMAS client software must be installed on each client workstation where you want to use the NMAS login methods.

- 1** At a Windows client workstation, insert the *Novell eDirectory 8.7.3 CD*.
- 2** From the NMAS directory, run `nmasinstall.exe`.
- 3** Select the NMAS Client Components check box.
Optionally, you can select the NICI check box if you want to install this component.
- 4** Click OK, then follow the on-screen instructions.
- 5** Reboot the client workstation after the installation completes.

Installing into a Tree with Dotted Name Containers

You can install a Windows server into an eDirectory tree that has containers with dots in the names (for example, O=novell.com or C=u.s.a). Using containers with dotted names requires that those dots be escaped with the backslash character. To escape a dot, simply put a backslash in front of any dot in a container name. See [Figure 4](#) for an example.

You cannot start a name with a dot. For example, you cannot create a container named “.novell” because it starts with a dot (‘.’).

Figure 4 eDirectory Installation Information Screen

eDirectory Installation

Novell.

Enter eDirectory information to create a new tree.

eDirectory Information

Tree Name
ELEVEN

New server object context (e.g. thisServer-NDS.Novell)
Server1-2000-NDS.novell.com

Administrator Information

Admin Name
Admin

Admin Context
novell.com

Password

Retype Password

Cancel Help < Back Next >

RSA SECURED

IMPORTANT: If your tree has containers with dotted names, you must escape those names when logging into utilities such as iMonitor, iManager, and DHost iConsole. For example, if your tree has “novell.com” as the name of the O, enter *username.novell.com* in the Username field when logging in to iMonitor (see [Figure 5](#)).

Figure 5 iMonitor Login Screen

Login

Username:
admin.novell.com

Password:

Login

Copyright © 2001-2003 Novell, Inc. All rights reserved.

3

Installing or Upgrading Novell eDirectory on Linux

Use the following information to install or upgrade Novell® eDirectory™ 8.7.3 on a Linux* server:

- ◆ “System Requirements” on page 23
- ◆ “Prerequisites” on page 24
- ◆ “Hardware Requirements” on page 25
- ◆ “Forcing the Backlink Process to Run” on page 25
- ◆ “Upgrading eDirectory” on page 25
- ◆ “Installing eDirectory” on page 26

IMPORTANT: The instructions in this guide do not apply when installing eDirectory with Novell Nterprise™ Linux Services. Please follow the prerequisites and installation instructions provided in the *Novell Nterprise Linux Services Installation Guide* (<http://www.novell.com/documentation/lg/npls/install/data/front.html>).

System Requirements

- One of the following:
 - ◆ OES Linux SP2 32 bit
 - ◆ SUSE® Linux Enterprise Server 8.x 32 bit
 - ◆ SUSE® Linux Enterprise Server 9 32 bit (SP1, SP2 & SP3) and 64 bit (SP3) or later
 - ◆ SUSE® Linux Enterprise Server 10 32 bit and 64 bit
 - NOTE:** To determine the version of SUSE Linux you are running, see the `/etc/SuSE-release` file.
 - ◆ SUSE® Linux Enterprise Server 10 32 bit and 64 bit
 - ◆ Red Hat Enterprise Linux AS 2.1 32 bit
 - ◆ Red Hat Enterprise Linux ES & AS 3.0 32 bit
 - ◆ Red Hat Enterprise Linux AS 4.0 32 and 64-bit
 - ◆ Ensure that the latest glibc patches are applied from [Red Hat Errata \(http://rhn.redhat.com/errata\)](http://rhn.redhat.com/errata) on Red Hat systems. The minimum required version of the glibc library is version 2.1.
 - ◆ Red Hat* Enterprise Linux AS Release 4 x86_64
 - ◆ Red Hat* Enterprise Linux ES Release 4 x86_64
 - IMPORTANT:** To install eDirectory 8.7.3 on SuSE Linux Enterprise Server 9, you must be running eDirectory 8.7.3 IR3 or later.
- 128 MB RAM minimum

- ❑ 90 MB of disk space for the eDirectory server
- ❑ 25 MB of disk space for the eDirectory administration utilities
- ❑ 74 MB of disk space for every 50,000 users
- ❑ Ensure that gettext is installed

To see if gettext is installed, run the following command:

```
rpm -q gettext
```

This displays the package and the version (if it is installed).

If you need to install gettext, see <http://www.gnu.org/software/gettext/> (<http://www.gnu.org/software/gettext/>).

Prerequisites

- ❑ Enable the Linux host for multicast routing.

To check if the host is enabled for multicast routing, enter the following command:

```
/bin/netstat -nr
```

The following entry should be present in the routing table:

```
224.0.0.0 0.0.0.0
```

If the entry is not present, log in as root and enter the following command to enable multicast routing:

```
route add -net 224.0.0.0 netmask 240.0.0.0 dev -interface
```

The *-interface* could be a value such as eth0, hme0, hme1, or hme2, depending on the NIC that is installed and used.

- ❑ Ensure that NICI 2.6.4 is installed.

eDirectory prompts for the installation of NICI 2.6.4 during installation if it is not already installed. The package containing NICI 2.6.4 is named `nici-2.6.4-u0.i386.rpm` on Linux.

- ❑ For secure Novell eDirectory operations, you will need the NICI Foundation Key file.

You can obtain an evaluation file from the [Novell eDirectory Eval License Download \(http://www.novell.com/products/edirectory/licenses/eval_87.html\)](http://www.novell.com/products/edirectory/licenses/eval_87.html) Web site. If you do not use the NICI Foundation Key, you will not be able to create Certificate Authority and Key Material objects.

- ❑ If you have more than one server in the tree, the time on all the network servers should be synchronized.

Use Network Time Protocol's (NTP) `xntpd` to synchronize time. If you want to synchronize time on Linux, Solaris, or AIX with NetWare[®] servers, use `timesync.nlm` 5.09 or later.

- ❑ If you are installing a secondary server, all the replicas in the partition that you install the product on should be in the On state.

- ❑ If you are going to install ConsoleOne[®], make sure your file system supports symbolic links.

Hardware Requirements

Hardware requirements depend on the specific implementation of eDirectory. Two factors increase performance: more cache memory and faster processors. For best results, cache as much of the DIB Set as the hardware allows.

eDirectory scales well on a single processor. However, Novell eDirectory 8.7.3 takes advantage of multiple processors. Adding processors improves performance in some areas—for example, logins and having multiple threads active on multiple processors. eDirectory itself is not processor intensive, but it is I/O intensive.

The following table illustrates typical system requirements for eDirectory for Linux:

Objects	Processor	Memory	Hard Disk
100,000	Pentium III 450-700 MHz (single)	384 MB	144 MB
1 million	Pentium III 450-700 MHz (dual)	2 GB	1.5 GB
10 million	Pentium III 450-700 MHz (2 to 4)	2+ GB	15 GB

Requirements for processors might be greater than the table indicates, depending upon additional services available on the computer as well as the number of authentications, reads, and writes that the computer is handling. Processes such as encryption and indexing can be processor intensive.

Forcing the Backlink Process to Run

Because the internal eDirectory identifiers change when upgrading to Novell eDirectory, the backlink process must update backlinked objects for them to be consistent.

Backlinks keep track of external references to objects on other servers. For each external reference on a server, the backlink process ensures that the real object exists in the correct location and verifies all backlink attributes on the master of the replica. The backlink process occurs two hours after the database is open, and then every 780 minutes (13 hours). The interval is configurable from 2 minutes to 10,080 minutes (7 days).

After migrating to eDirectory, start the `ndstrace` process by issuing the `ndstrace -l>log&` command, which runs the process at the background. You can force the backlink to run by issuing the `ndstrace -c set ndstrace=*B` command from the `ndstrace` command prompt. Then you can unload the `ndstrace` process by issuing the `ndstrace -u` command. Running the backlink process is especially important on servers that do not contain a replica.

Upgrading eDirectory

To upgrade to eDirectory 8.7.3 from eDirectory 8.5.x, 8.6.x, 8.7, or 8.7.1, enter the following:

```
nds-install
```

NOTE: Upgrade ConsoleOne to 1.3.6 if an older version is installed on the system. Upgrade NAM to 2.1.2 if an older version is installed on the system.

Installing eDirectory

The following sections provide information about installing Novell eDirectory on Linux:

- ◆ [“Using SLP with eDirectory” on page 26](#)
- ◆ [“Using the nds-install Utility to Install eDirectory Components” on page 26](#)
- ◆ [“Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server” on page 28](#)
- ◆ [“Using ndsconfig to Install a Linux Server into a Tree with Dotted Name Containers” on page 30](#)
- ◆ [“Using the nmasinst Utility to Configure NMAS” on page 31](#)

Using SLP with eDirectory

If you plan to use SLP to resolve tree names, it should have been properly configured and SLP DAs should be stable. If you don't want to (or cannot) use SLP, you can use the flat file `hosts.nds` to resolve tree names to server referrals. The `hosts.nds` file can be used to avoid SLP multicast delays when a SLP DA is not present in the network.

`hosts.nds` is a static lookup table used by eDirectory applications to search eDirectory partition and servers. See the `hosts.nds` man page for more details.

NOTE: If you decide to use SLP to resolve the tree name to determine if the eDirectory tree is advertised, after eDirectory and SLP are installed, enter the following:

```
/usr/bin/slpinfo -s "ndap.novell///(svcname-ws==[treename or *])"
```

For more information, see [Appendix B, “Configuring OpenSLP for eDirectory,” on page 71](#).

Using the nds-install Utility to Install eDirectory Components

Use the `nds-install` utility to install eDirectory components on Linux systems. This utility is located in the `Setup` directory on the CD for the Linux platform. The utility adds the required packages based on what components you choose to install.

- 1 Log in as root on the host.
- 2 Enter the following command at the `setup` directory:

```
./nds-install
```

To install eDirectory components, use the following syntax:

```
nds-install [-c component1 [-c component2]...] [-h]
[-n License file path] [-i]
```

If you do not provide the required parameters in the command line, the `nds-install` utility will prompt you for the parameters.

The following table provides a description of the `nds-install` utility parameters:

nds-install Parameter	Description
-c	Specifies the component to be installed based on the packages available. You can install more than one component by using the <code>-c</code> option multiple times.
-h	Displays help for <code>nds-install</code> .

nds-install Parameter	Description
-n	Specifies the path to the license file.
-i	Prevents the nds-install script from invoking ndsconfig upgrade if a DIB is detected at the time of the upgrade.

For example, to install Novell eDirectory Server packages, you would enter the following command:

```
./nds-install -c server -n /var
```

```
nds-install -c server -n /var
```

- 3 When prompted, accept the license agreement.

The installation program displays a list of eDirectory components that you can install.

- 4 Specify the option for the component you want to install.

Based on the component you choose to install, the installation program proceeds to add the appropriate RPMs or packages into the Linux system. The following table lists the packages installed for each eDirectory component.

eDirectory Component	Packages Installed	Description
eDirectory Server	NDSbase NDScommon NDSmasv NDSserv NDSimon NDSrepair NDSslp NDSdexvnt NOVSubag NOVsnmp NOVpkit NOVpkis NOVpkia NOVembox NOVimgnt NOVstlog NOVxis NLDAPsdk NLDAPbase NOVsas NOVntls NOVnmas	The eDirectory replica server is installed on the specified server.
Administration Utilities	NOVLice NDSbase NLDAPbase NLDAPsdk NOVpkia NOVxis NOVimgnt	The Novell Import Conversion Export and LDAP Tools administration utilities are installed on the specified workstation.

eDirectory Component	Packages Installed	Description
Management Console for eDirectory	NDSbase NDSslp NOVLC1 C1JRE NDS set of packages	The management console for eDirectory is installed on the specified workstation.

- 5** If you are prompted, enter the complete path to the license file.

You will be prompted to enter the complete path to the license file only if the installation program cannot locate the file in the default location (/var, a mounted license diskette, or the current directory).

If the path you entered is not valid, you will be prompted to enter the correct path.

You can use the ndsconfig utility to configure eDirectory Server after installation. However, to do so, you need to ensure that the License file has been copied to the /var directory.

Novell Modular Authentication Service™ (NMASTM) is installed as part of the server component. By default, ndsconfig configures NMASTM. You can also use the nmasinst utility to configure NMASTM server after installation. This must be done after configuring eDirectory with ndsconfig.

For more information on the ndsconfig utility, see [“The ndsconfig Utility” on page 61](#).

For more information on the nmasinst utility, see [“Using the nmasinst Utility to Configure NMASTM” on page 31](#).

Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server

You must have Administrator rights to use the ndsconfig utility. When this utility is used with arguments, it validates all arguments and prompts for the password of the user having Administrator rights. If the utility is used without arguments, ndsconfig displays a description of the utility and available options. This utility can also be used to remove the eDirectory Replica Server and change the current configuration of eDirectory Server. For more information, see [“The ndsconfig Utility” on page 61](#).

Creating A New Tree

Use the following syntax:

```
ndsconfig new -t treename -n server context -a admin FDN [-i] [-S server name]
[-d path for dib] [-m module] [e] [-L ldap port] [-l SSL port] [-o http port]
-O https port]
```

A new tree is installed with the specified tree name and context.

There is a limitation on the number of characters in the *tree_name*, *admin FDN* and *server context* variables. The maximum number of characters allowed for these variables is as follows:

- ◆ *tree_name*: 32 characters
- ◆ *any FDN*: 256 characters

If the parameters are not specified in the command line, ndsconfig prompts you to enter values for each of the missing parameters.

Or, you can also use the following syntax:

```
ndsconfig def -t treeName -n server context -a admin FDN [-i] [-S server name]
[-d path for dib] [-m module] [-e] [-L ldap port] [-l SSL port] [-o http port]
-o https port]
```

A new tree is installed with the specified tree name and context. If the parameters are not specified in the command line, ndsconfig takes the default value for each of the missing parameters.

For example, to create a new tree, you could enter the following command:

```
ndsconfig new -t corp-tree -n o=company -a cn=admin.o=company
```

Adding a Server into an Existing Tree

Use the following syntax:

```
ndsconfig add -t treeName -n server context -a admin FDN [-e] [-L ldap port]
[-l SSL port] [-o http port] -O https port] [-S server name] [-d path for dib]
[-p IP address] [-m module]
```

A server is added to an existing tree in the specified context. If the context that the user wants to add the Server object to does not exist, ndsconfig creates the context and adds the server.

LDAP and security services can also be added after eDirectory has been installed into the existing tree.

For example, to add a server into an existing tree, you could enter the following command:

```
ndsconfig add -t corp-tree -n o=company -a cn=admin.o=company
```

Removing a Server Object And Directory Services From a Tree

Use the following syntax:

```
ndsconfig rm -a admin FDN
```

eDirectory and its database are removed from the server.

NOTE: The HTML files created using iMonitor will not be removed. You must manually remove these files before removing eDirectory.

For example, to remove the eDirectory Server object and directory services from a tree, you could enter the following command:

```
ndsconfig rm -a cn=admin.o=company
```

ndsconfig Utility Parameters

ndsconfig Parameter	Description
new	Creates a new eDirectory tree. If the parameters are not specified in the command line, ndsconfig prompts you to enter values for each of the missing parameters.
def	Creates a new eDirectory tree. If the parameters are not specified in the command line, ndsconfig takes the default value for each of the missing parameters.
add	Adds a server into an existing tree.
rm	Removes the Server object and directory services from a tree.

ndsconfig Parameter	Description
-i	Ignores a tree of the same name, while installing a new tree. This option is generally not recommended for use.
-S	Specifies the server name. The default server name is <i>host name</i> .
-t	The tree name to which the server has to be added. If not specified, ndsconfig uses the tree name from the n4u.base.tree-name parameter specified in the etc/nds.conf file.
-n	The context of the server into which the Server object is added. If not specified, ndsconfig uses the context from the n4u.nds.server-context parameter specified in the /etc/nds.conf file.
-d	The directory path where the database files will be stored.
-L	The TCP port number on the LDAP server.
-l	The SSL port number on the LDAP server.
-a	Distinguished name of the User object that has Supervisor rights to the context in which the Server object and directory services will be created.
-e	Enables clear text passwords for LDAP objects.
-p	Installs eDirectory Server into an existing tree by specifying the IP address of a server hosting the tree. If this option is used, SLP is not used for tree lookup.
-m	Specifies the module name to install. While installing a new tree, you can install only the ds module. After installing the ds module, you can add the NMAS, LDAP, SAS, HTTP and SNMP services using the add command. If the module name is not specified, by default, all the five modules are installed.
-o	Specifies the HTTP clear port number.
-O	Specifies the HTTP secure port number.
set	Sets the value for the specified eDirectory configurable parameters. If the parameter list is not specified, ndsconfig lists all the eDirectory configurable parameters.
get	Lets you view the current value of the eDirectory configurable parameters.
get help	Lets you view the help strings for the eDirectory configurable parameters.

Using ndsconfig to Install a Linux Server into a Tree with Dotted Name Containers

You can use ndsconfig to install a Linux server into an eDirectory tree that has containers using dotted names (for example, novell.com).

Because ndsconfig is a command line utility, using containers with dotted names requires that those dots be escaped out, and the parameters containing these contexts must be enclosed in double quotes. For example, to install a new eDirectory tree on a Linux server using “O=novell.com” as the name of the O, use the following command:

```
ndsconfig new -a "admin.novell\.com" -t novell_tree -n "OU=servers.O=novell\.com"
```

The Admin name and context and the server context parameters are enclosed in double quotes, and only the dot (.) in novell.com is escaped using the \ (backslash) character.

You can also use this format when installing a server into an existing tree.

NOTE: You should use this format when entering dotted admin name and context while using utilities such as ndsrepair, ndsbackup, ndsmerge, ndslogin, and ldapconfig.

Using the nmasinst Utility to Configure NMAS

For eDirectory 8.7.3, by default, ndsconfig configures NMAS. You can also use nmasinst on Linux, Solaris, and AIX systems to configure NMAS.

ndsconfig only configures NMAS and does not install the login methods. To install these login methods, you can use nmasinst.

IMPORTANT: You must configure eDirectory with ndsconfig before you install the NMAS login methods. You must also have administrative rights to the tree.

- ◆ “Configuring NMAS” on page 31
- ◆ “Installing Login Methods” on page 31

Configuring NMAS

By default, ndsconfig configures NMAS. You can also use nmasinst for the same.

To configure NMAS and create NMAS objects in eDirectory, enter the following at the server console command line:

```
nmasinst -i admin.context tree_name
```

nmasinst will prompt you for a password.

This command creates the objects in the Security container that NMAS needs, and installs the LDAP extensions for NMAS on the LDAP Server object in eDirectory.

The first time NMAS is installed in a tree, it must be installed by a user with enough rights to create objects in the Security container. However, subsequent installs can be done by container administrators with read-only rights to the Security container. nmasinst will verify that the NMAS objects exist in the Security container before it tries to create them.

nmasinst does not extend the schema. The NMAS schema is installed as part of the base eDirectory schema.

Installing Login Methods

To install login methods using nmasinst, enter the following at the server console command line:

```
nmasinst -addmethod admin.context tree_name config.txt_path
```

The last parameter specifies the config.txt file for the login method that is to be installed. A config.txt file is provided with each login method.

Here is an example of the -addmethod command:

```
nmasinst -addmethod admin.novell MY_TREE ./nmas-methods/novell/Simple  
Password/config.txt
```

If the login method already exists, nmasinst will update it.

For more information, see “Managing Login and Post-Login Methods and Sequences” (<http://www.novell.com/documentation/lg/nmas23/admin/data/a53vj9a.html>) in the *Novell Modular Authentication Service Administration Guide*.

4

Installing or Upgrading Novell eDirectory on Solaris

Use the following information to install or upgrade Novell® eDirectory™ 8.7.3 on a Solaris* server:

- ♦ “System Requirements” on page 33
- ♦ “Prerequisites” on page 33
- ♦ “Hardware Requirements” on page 34
- ♦ “Forcing the Backlink Process to Run” on page 34
- ♦ “Upgrading eDirectory” on page 35
- ♦ “Installing eDirectory” on page 35

System Requirements

- One of the following:
 - ♦ Solaris 8 on Sun SPARC (with patch 108827-20 or later)
 - ♦ Solaris 9 on Sun SPARC
- All latest recommended set of patches available on the [SunSolve* Web page \(http://sunsolve.sun.com\)](http://sunsolve.sun.com). If you do not update your system with the latest patches before installing eDirectory, you will get the patchadd error.
- 128 MB RAM minimum
- 120 MB of disk space for the eDirectory server
- 32 MB of disk space for the eDirectory administration utilities
- 74 MB of disk space for every 50,000 users

Prerequisites

- Enable the Solaris host for multicast routing.

To check if the host is enabled for multicast routing, enter the following command:

```
/usr/bin/netstat -nr
```

The following entry should be present in the routing table:

```
224.0.0.0 host_IP_address
```

If the entry is not present, log in as root, and enter the following command to enable multicast routing:

```
route add -net 224.0.0.0 -net 224.0.0.0 netmask 240.0.0.0 hme0
```

- Ensure that NCI 2.6.4 is installed.

eDirectory prompts for the installation of NCI 2.6.4 during installation if it is not already installed. The package containing NCI 2.6.4 is named NOVLniu0-2.6.4 on Solaris.

- For secure Novell eDirectory operations, you will need the NCI Foundation Key file.

You can obtain an evaluation file from the [Novell eDirectory Eval License Download \(http://www.novell.com/products/edirectory/licenses/eval_87.html\)](http://www.novell.com/products/edirectory/licenses/eval_87.html) Web site. If you do not use the NCI Foundation Key, you will not be able to create Certificate Authority and Key Material objects.

- If you have more than one server in the tree, the time on all the network servers should be synchronized.

Use Network Time Protocol's (NTP) xntpd to synchronize time. If you want to synchronize time on Linux, Solaris, or AIX systems with NetWare[®] servers, use timesync.nlm 5.09 or later.

- If you are installing a secondary server, all the replicas in the partition that you install the product on should be in the On state.

Hardware Requirements

Hardware requirements depend on the specific implementation of eDirectory. Two factors increase performance: more cache memory and faster processors. For best results, cache as much of the DIB Set as the hardware allows.

eDirectory scales well on a single processor. However, Novell eDirectory 8.7.3 takes advantage of multiple processors. Adding processors improves performance in some areas—for example, logins and having multiple threads active on multiple processors. eDirectory itself is not processor intensive, but it is I/O intensive.

The following table illustrates typical system requirements for Novell eDirectory for Solaris.

Objects	Processor	Memory	Hard Disk
100,000	Sun* Enterprise 220	384 MB	144 MB
1 million	Sun Enterprise 450	2 GB	1.5 GB
10 million	Sun Enterprise 4500 with multiple processors	2+ GB	15 GB

Requirements for processors might be greater than the table indicates, depending upon additional services available on the computer as well as the number of authentications, reads, and writes that the computer is handling. Processes such as encryption and indexing can be processor intensive.

Forcing the Backlink Process to Run

Because the internal eDirectory identifiers change when upgrading to Novell eDirectory, the backlink process must update backlinked objects for them to be consistent.

Backlinks keep track of external references to objects on other servers. For each external reference on a server, the backlink process ensures that the real object exists in the correct location and

verifies all backlink attributes on the master of the replica. The backlink process occurs two hours after the database is open, and then every 780 minutes (13 hours). The interval is configurable from 2 minutes to 10,080 minutes (7 days).

After migrating to eDirectory, start the ndstrace process by issuing the `ndstrace -l>log&` command, which runs the process at the background. You can force the backlink to run by issuing the `ndstrace -c set ndstrace=*B` command from the ndstrace command prompt. Then you can unload the ndstrace process by issuing the `ndstrace -u` command. Running the backlink process is especially important on servers that do not contain a replica.

Upgrading eDirectory

To upgrade to eDirectory 8.7.3 from eDirectory 8.5.x, 8.6.x, 8.7, or 8.7.1, enter the following:

```
nds-install
```

NOTE: Upgrade ConsoleOne to 1.3.6 if an older version is installed on the system. Upgrade NAM to 2.1.2 if an older version is installed on the system.

Installing eDirectory

The following sections provide information about installing Novell eDirectory on Solaris:

- ♦ [“Using SLP with eDirectory” on page 35](#)
- ♦ [“Using the nds-install Utility to Install eDirectory Components” on page 35](#)
- ♦ [“Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server” on page 38](#)
- ♦ [“Using ndsconfig to Install a Solaris Server into a Tree with Dotted Name Containers” on page 40](#)
- ♦ [“Using the nmasinst Utility to Configure NMAS” on page 40](#)

Using SLP with eDirectory

If you plan to use SLP to resolve tree names, it should have been properly configured and SLP DAs should be stable. If you don't want to (or cannot) use SLP, you can use the flat file `hosts.nds` to resolve tree names to server referrals. The `hosts.nds` file can be used to avoid SLP multicast delays when a SLP DA is not present in the network.

`hosts.nds` is a static lookup table used by eDirectory applications to search eDirectory partition and servers. See the `hosts.nds` man page for more details.

NOTE: If you decide to use SLP to resolve the tree name to determine if the eDirectory tree is advertised, after eDirectory and SLP are installed, enter the following:

```
/usr/bin/slpinfo -s "ndap.novell//(svcname-ws==[treename or *])"
```

For more information, see [Appendix B, “Configuring OpenSLP for eDirectory,” on page 71](#).

Using the nds-install Utility to Install eDirectory Components

Use the `nds-install` utility to install eDirectory components on Solaris systems. This utility is located in the `Setup` directory on the CD for the Solaris platform. The utility adds the required packages based on what components you choose to install.

- 1 Log in as root on the host.

- 2** Enter the following command from the setup directory:

```
./nds-install
```

To install eDirectory components, use the following syntax:

```
nds-install [-c component1 [-c component2]...] [-h]
[-n License file path] [-i]
```

If you do not provide the required parameters in the command line, the nds-install utility will prompt you for the parameters.

The following table provides a description of the nds-install utility parameters:

nds-install Parameter	Description
-c	Specifies the component to be installed based on the packages available. You can install more than one component by using the -c option multiple times.
-h	Displays help for nds-install.
-n	Specifies the path to the license file.
-i	Prevents the nds-install script from invoking ndsconfig upgrade if a DIB is detected at the time of the upgrade.

For example, to install Novell eDirectory Server packages, you would enter the following command:

```
./nds-install -c server -n /var
```

- 3** When prompted, accept the license agreement.

The installation program displays a list of eDirectory components that you can install.

- 4** Specify the option for the component you want to install.

Based on the component you choose to install, the installation program proceeds to add the appropriate RPMs or packages into the Solaris system. The following table lists the packages installed for each eDirectory component.

eDirectory Component	Packages Installed	Description
eDirectory Server	NDSbase NDScommon NDSmasv NDSserv NDSimon NDSrepair NDSslp NDSdexvnt NOVLsubag NOVLsnmp NOVLpkit NOVLpkis NOVLpkia NOVLembox NOVLimgnt NOVLstlog NOVLxis NLDAPsdk NLDAPbase NOVLsas NOVLntls NOVLnmas	The eDirectory replica server is installed on the specified server.
Administration Utilities	NOVLice NDSbase NLDAPbase NLDAPsdk NOVLpkia NOVLxis NOVLimgnt	The Novell Import Conversion Export and LDAP Tools administration utilities are installed on the specified workstation.
Management Console for eDirectory	NDSbase NDSslp NOVLC1 C1JRE NDS set of packages	The management console for eDirectory is installed on the specified workstation.

5 If you are prompted, enter the complete path to the license file.

You will be prompted to enter the complete path to the license file only if the installation program cannot locate the file in the default location (/var, a mounted license diskette, or the current directory).

If the path you entered is not valid, you will be prompted to enter the correct path.

You can use the ndsconfig utility to configure eDirectory Server after installation. However, to do so, you need to ensure that the License file has been copied to the /var directory.

Novell Modular Authentication Service™ (NMAS™) is installed as part of the server component. By default, ndsconfig configures NMAS. You can also use the nmasinst utility to configure NMAS server after installation. This must be done after configuring eDirectory with ndsconfig.

For more information on the ndsconfig utility, see [“The ndsconfig Utility” on page 61](#).

For more information on the nmasinst utility, see [“Using the nmasinst Utility to Configure NMAS” on page 40](#).

Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server

You must have Administrator rights to use the ndsconfig utility. When this utility is used with arguments, it validates all arguments and prompts for the password of the user having Administrator rights. If the utility is used without arguments, ndsconfig displays a description of the utility and available options. This utility can also be used to remove the eDirectory Replica Server and change the current configuration of eDirectory Server. For more information, see [“The ndsconfig Utility” on page 61](#).

Creating a New Tree

Use the following syntax:

```
ndsconfig new -t tree_name -n server context -a admin FDN [-i] [-S server name]
[-d path for dib] [-m module] [-e] [-L ldap port] [-l SSL port] [-o http port]
-O https port]
```

A new tree is installed with the specified tree name and context.

There is a limitation on the number of characters in the *tree_name*, *admin FDN* and *server context* variables. The maximum number of characters allowed for these variables is as follows:

- ◆ *tree_name*: 32 characters
- ◆ *any FDN*: 256 characters

If the parameters are not specified in the command line, ndsconfig prompts you to enter values for each of the missing parameters.

Or, you can also use the following syntax:

```
ndsconfig def -t tree_name -n server context -a admin FDN [-i] [-S server name]
[-d path for dib] [-m module] [-e] [-L ldap port] [-l SSL port] [-o http port]
-O https port]
```

A new tree is installed with the specified tree name and context. If the parameters are not specified in the command line, ndsconfig takes the default value for each of the missing parameters.

For example, to create a new tree, you could enter the following command:

```
ndsconfig new -t corp-tree -n o=company -a cn=admin.o=company
```

Adding a Server into an Existing Tree

Use the following syntax:

```
ndsconfig add -t tree_name -n server context -a admin FDN [-e] [-L ldap port]
[-l SSL port] [-o http port] -O https port] [-S server name] [-d path for dib]
[-p IP address] [-m module]
```

A server is added to an existing tree in the specified context. If the context that the user wants to add the Server object to does not exist, ndsconfig creates the context and adds the server.

LDAP and security services can also be added after eDirectory has been installed into the existing tree.

For example, to add a server into an existing tree, you could enter the following command:

```
ndsconfig add -t corp-tree -n o=company -a cn=admin.o=company
```

Removing a Server Object and Directory Services from a Tree

Use the following syntax:

```
ndsconfig rm -a admin FDN
```

eDirectory and its database are removed from the server.

NOTE: The HTML files created using iMonitor will not be removed. You must manually remove these files before removing eDirectory.

For example, to remove the eDirectory Server object and directory services from a tree, you could enter the following command:

```
ndsconfig rm -a cn=admin.o=company
```

ndsconfig Utility Parameters

ndsconfig Parameter	Description
new	Creates a new eDirectory tree. If the parameters are not specified in the command line, ndsconfig prompts you to enter values for each of the missing parameters.
def	Creates a new eDirectory tree. If the parameters are not specified in the command line, ndsconfig takes the default value for each of the missing parameters.
add	Adds a server into an existing tree.
rm	Removes the Server object and directory services from a tree.
-i	Ignores a tree of the same name, while installing a new tree. This option is generally not recommended for use.
-S	Specifies the server name. The default server name is <i>host name</i> .
-t	The tree name to which the server has to be added. If not specified, ndsconfig uses the tree name from the <code>n4u.base.tree-name</code> parameter specified in the <code>etc/nds.conf</code> file.
-n	The context of the server into which the Server object is added. If not specified, ndsconfig uses the context from the <code>n4u.nds.server-context</code> parameter specified in the <code>/etc/nds.conf</code> file.
-d	The directory path where the database files will be stored.
-L	The TCP port number on the LDAP server.
-l	The SSL port number on the LDAP server.
-a	Distinguished name of the User object that has Supervisor rights to the context in which the Server object and directory services will be created.
-e	Enables clear text passwords for LDAP objects.
-p	Installs eDirectory Server into an existing tree by specifying the IP address of a server hosting the tree. If this option is used, SLP is not used for tree lookup.

ndsconfig Parameter	Description
-m	Specifies the module name to install. While installing a new tree, you can install only the ds module. After installing the ds module, you can add the NMAS, LDAP, SAS, HTTP and SNMP services using the add command. If the module name is not specified, by default, all the five modules are installed.
-o	Specifies the HTTP clear port number.
-O	Specifies the HTTP secure port number.
set	Sets the value for the specified eDirectory configurable parameters. If the parameter list is not specified, ndsconfig lists all the eDirectory configurable parameters.
get	Lets you view the current value of the eDirectory configurable parameters.
get help	Lets you view the help strings for the eDirectory configurable parameters.

Using ndsconfig to Install a Solaris Server into a Tree with Dotted Name Containers

You can use ndsconfig to install a Solaris server into an eDirectory tree that has containers using dotted names (for example, novell.com).

Because ndsconfig is a command line utility, using containers with dotted names requires that those dots be escaped out, and the parameters containing these contexts must be enclosed in double quotes. For example, to install a new eDirectory tree on a Solaris server using “O=novell.com” as the name of the O, use the following command:

```
ndsconfig new -a "admin.novell\.com" -t novell_tree -n "OU=servers.O=novell\.com"
```

The Admin name and context and the server context parameters are enclosed in double quotes, and only the dot (.) in novell.com is escaped using the \ (backslash) character.

You can also use this format when installing a server into an existing tree.

NOTE: You should use this format when entering dotted admin name and context while using utilities such as ndsrepair, ndsbackup, ndsmerge, ndslogin, and ldapconfig.

Using the nmasinst Utility to Configure NMAS

For eDirectory 8.7.3, by default, ndsconfig configures NMAS. You can also use nmasinst on Linux, Solaris, and AIX systems to configure NMAS.

ndsconfig only configures NMAS and does not install the login methods. To install these login methods, you can use nmasinst.

IMPORTANT: You must configure eDirectory with ndsconfig before you install the NMAS login methods. You must also have administrative rights to the tree.

- ◆ [“Configuring NMAS” on page 41](#)
- ◆ [“Installing Login Methods” on page 41](#)

Configuring NMAS

By default, ndsconfig configures NMAS. You can also use nmasinst for the same.

To configure NMAS and create NMAS objects in eDirectory, enter the following at the server console command line:

```
nmasinst -i admin.context tree_name
```

nmasinst will prompt you for a password.

This command creates the objects in the Security container that NMAS needs, and installs the LDAP extensions for NMAS on the LDAP Server object in eDirectory.

The first time NMAS is installed in a tree, it must be installed by a user with enough rights to create objects in the Security container. However, subsequent installs can be done by container administrators with read-only rights to the Security container. nmasinst will verify that the NMAS objects exist in the Security container before it tries to create them.

nmasinst does not extend the schema. The NMAS schema is installed as part of the base eDirectory schema.

Installing Login Methods

To install login methods using nmasinst, enter the following at the server console command line:

```
nmasinst -addmethod admin.context tree_name config.txt_path
```

The last parameter specifies the config.txt file for the login method that is to be installed. A config.txt file is provided with each login method.

Here is an example of the -addmethod command:

```
nmasinst -addmethod admin.novell MY_TREE ./nmas-methods/novell/Simple  
Password/config.txt
```

If the login method already exists, nmasinst will update it.

For more information, see “Managing Login and Post-Login Methods and Sequences” (<http://www.novell.com/documentation/lg/nmas23/admin/data/a53vj9a.html>) in the *Novell Modular Authentication Service Administration Guide*.

5

Installing or Updating Novell eDirectory on AIX

Use the following information to install or upgrade Novell® eDirectory™ 8.7.3 on an AIX* server:

- ♦ “System Requirements” on page 43
- ♦ “Prerequisites” on page 43
- ♦ “Hardware Requirements” on page 44
- ♦ “Forcing the Backlink Process to Run” on page 44
- ♦ “Upgrading eDirectory” on page 45
- ♦ “Installing eDirectory” on page 45

System Requirements

- One of the following:
 - ♦ AIX 5L Version 5.1
 - ♦ AIX 5L Version 5.2
- All recommended AIX OS patches, available at the [IBM* Tech Support \(https://techsupport.services.ibm.com/server/fixes\)](https://techsupport.services.ibm.com/server/fixes) Web site
- 128 MB RAM minimum
- 190 MB of disk space for the eDirectory server
- 12 MB of disk space for the eDirectory administration utilities
- 74 MB of disk space for every 50,000 users

Prerequisites

- Enable the AIX host for multicast routing.

See if the multicast routing daemon mrouterd is running.

If it is not running, configure and start the multicast daemon mrouterd.

See the “mrouterd.conf File” section in the *Files Reference* book in [AIX Documentation \(http://www16.boulder.ibm.com/pseries/en_US/infocenter/base/aix.htm\)](http://www16.boulder.ibm.com/pseries/en_US/infocenter/base/aix.htm) for an example configuration file.
- Ensure that NICI 2.6.4 is installed.

eDirectory prompts for the installation of NICI 2.6.4 during installation if it is not already installed. The package containing NICI 2.6.4 is named NOVLniu0-2.6.4 on AIX.
- For secure Novell eDirectory operations, you will need the NICI Foundation Key file.

You can obtain an evaluation file from the [Novell eDirectory Eval License Download \(http://www.novell.com/products/edirectory/licenses/eval_87.html\)](http://www.novell.com/products/edirectory/licenses/eval_87.html) Web site. If you do not use the NICI Foundation Key, you will not be able to create Certificate Authority and Key Material objects.

- If you have more than one server in the tree, the time on all the network servers should be synchronized.

Use Network Time Protocol's (NTP) `xntpd.nlm` to synchronize time. If you want to synchronize time on Linux, Solaris, or AIX systems with NetWare® servers, use `timesync.nlm` 5.09 or later.

- If you are installing a secondary server, all the replicas in the partition that you install the product on should be in the On state.

Hardware Requirements

Hardware requirements depend on the specific implementation of eDirectory.

For example, a base installation of Novell eDirectory with the standard schema requires about 74 MB of disk space for every 50,000 users. However, if you add a new set of attributes or completely fill in every existing attribute, the object size grows. These additions affect the disk space, processor, and memory needed.

Two factors increase performance: more cache memory and faster processors.

For best results, cache as much of the DIB Set as the hardware allows.

eDirectory scales well on a single processor. However, eDirectory 8.7.3 takes advantage of multiple processors. Adding processors improves performance in some areas—for example, logins and having multiple threads active on multiple processors. eDirectory itself is not processor intensive, but it is I/O intensive.

The following table illustrates typical system requirements for Novell eDirectory for AIX.

Objects	Processor	Memory	Hard Disk
100,000	RS/6000	344 MB	144 MB
1 Million	RS/6000	2 GB	1.5 GB
10 Million	RS/6000	2+ GB	15 GB

Requirements for processors might be greater than the table indicates, depending upon additional services available on the computer as well as the number of authentications, reads, and writes that the computer is handling. Processes such as encryption and indexing can be processor intensive.

Forcing the Backlink Process to Run

Because the internal eDirectory identifiers change when upgrading to Novell eDirectory, the backlink process must update backlinked objects for them to be consistent.

Backlinks keep track of external references to objects on other servers. For each external reference on a server, the backlink process ensures that the real object exists in the correct location and verifies all backlink attributes on the master of the replica. The backlink process occurs two hours

after the database is open, and then every 780 minutes (13 hours). The interval is configurable from 2 minutes to 10,080 minutes (7 days).

After migrating to eDirectory, start the `ndstrace` process by issuing the `ndstrace -l>log&` command, which runs the process at the background. You can force the backlink to run by issuing the `ndstrace -c set ndstrace=*B` command from the `ndstrace` command prompt. Then you can unload the `ndstrace` process by issuing the `ndstrace -u` command. Running the backlink process is especially important on servers that do not contain a replica.

Upgrading eDirectory

To upgrade to eDirectory 8.7.3 from eDirectory 8.7 or 8.7.1, enter the following:

```
nds-install
```

Installing eDirectory

The following sections provide information about installing Novell eDirectory on AIX:

- ♦ [“Using SLP with eDirectory” on page 45](#)
- ♦ [“Using the nds-install Utility to Install eDirectory Components” on page 45](#)
- ♦ [“Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server” on page 48](#)
- ♦ [“Using ndsconfig to Install an AIX Server into a Tree with Dotted Name Containers” on page 50](#)
- ♦ [“Using the nmasinst Utility to Configure NMAS” on page 50](#)

Using SLP with eDirectory

If you plan to use SLP to resolve tree names, it should have been properly configured and SLP DAs should be stable. If you don't want to (or cannot) use SLP, you can use the flat file `hosts.nds` to resolve tree names to server referrals. The `hosts.nds` file can be used to avoid SLP multicast delays when a SLP DA is not present in the network.

`hosts.nds` is a static lookup table used by eDirectory applications to search eDirectory partition and servers. See the `hosts.nds` man page for more details.

NOTE: If you decide to use SLP to resolve the tree name to determine if the eDirectory tree is advertised, after eDirectory and SLP are installed, enter the following:

```
/usr/bin/slpinfo -s "ndap.novell///(svcname-ws==[treename or *])"
```

For more information, see [Appendix B, “Configuring OpenSLP for eDirectory,” on page 71](#).

Using the nds-install Utility to Install eDirectory Components

Use the `nds-install` utility to install eDirectory components on AIX systems. This utility is located in the `Setup` directory on the CD for the AIX platform. The utility adds the required packages based on what components you choose to install.

- 1 Log in as root on the host.
- 2 Enter the following command from the `setup` directory:

```
./nds-install
```

To install eDirectory components, use the following syntax:

```
nds-install [-c component1 [-c component2]...] [-h]
[-n License file path] [-i]
```

If you do not provide the required parameters in the command line, the nds-install utility will prompt you for the parameters.

The following table provides a description of the nds-install utility parameters:

nds-install Parameter	Description
-c	Specifies the component to be installed based on the packages available. You can install more than one component by using the -c option multiple times.
-h	Displays help for nds-install.
-n	Specifies the path to the license file.
-i	Prevents the nds-install script from invoking ndsconfig upgrade if a DIB is detected at the time of the upgrade.

For example, to install Novell eDirectory Server packages, you would enter the following command:

```
./nds-install -c server -n /var
```

- 3** When prompted, accept the license agreement.

The installation program displays a list of eDirectory components that you can install.

- 4** Specify the option for the component you want to install.

Based on the component you choose to install, the installation program proceeds to add the appropriate RPMs or packages into the AIX system. The following table lists the packages installed for each eDirectory component.

eDirectory Component	Packages Installed	Description
eDirectory Server	NDSbase NDScommon NDSmasv NDSserv NDSimon NDSrepair NDSslp NDSdexvnt NOVLsubag NOVLsnmp NOVLpkit NOVLpkis NOVLpkia NOVLembox NOVLimgnt NOVLstlog NOVLxis NLDAPsdk NLDAPbase NOVLsas NOVLntls NOVLnmas	The eDirectory replica server is installed on the specified server.
Administration Utilities	NOVLice NDSbase NLDAPbase NLDAPsdk NOVLpkia NOVLxis NOVLimgnt	The Novell Import Conversion Export and LDAP Tools administration utilities are installed on the specified workstation.
Management Console for eDirectory	NDSbase NDSslp	The management console for eDirectory is installed on the specified workstation.

5 If you are prompted, enter the complete path to the license file.

You will be prompted to enter the complete path to the license file only if the installation program cannot locate the file in the default location (/var, a mounted license diskette, or the current directory).

If the path you entered is not valid, you will be prompted to enter the correct path.

You can use the ndsconfig utility to configure eDirectory Server after installation. However, to do so, you need to ensure that the License file has been copied to the /var directory.

Novell Modular Authentication Service™ (NMASTM) is installed as part of the server component. By default ndsconfig configures NMASTM. You can also use the nmasinst utility to configure NMASTM server after installation. This must be done after configuring eDirectory with ndsconfig.

For more information on the ndsconfig utility, see [“The ndsconfig Utility” on page 61](#).

For more information on the nmasinst utility, see [“Using the nmasinst Utility to Configure NMASTM” on page 50](#).

Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server

You must have Administrator rights to use the ndsconfig utility. When this utility is used with arguments, it validates all arguments and prompts for the password of the user having Administrator rights. If the utility is used without arguments, ndsconfig displays a description of the utility and available options. This utility can also be used to remove the eDirectory Replica Server and change the current configuration of eDirectory Server. For more information, see [“The ndsconfig Utility” on page 61](#).

Creating a New Tree

Use the following syntax:

```
ndsconfig new -t treename -n server context -a admin FDN [-i] [-S server name]
[-d path for dib] [-m module] [-e] [-L ldap port] [-l SSL port] [-o http port]
-O https port]
```

A new tree is installed with the specified tree name and context.

There is a limitation on the number of characters in the *tree_name*, *admin FDN* and *server context* variables. The maximum number of characters allowed for these variables is as follows:

- ◆ *tree_name*: 32 characters
- ◆ *any FDN*: 256 characters

If the parameters are not specified in the command line, ndsconfig prompts you to enter values for each of the missing parameters.

Or, you can also use the following syntax:

```
ndsconfig def -t treename -n server context -a admin FDN [-i] [-S server name]
[-d path for dib] [-m module] [-e] [-L ldap port] [-l SSL port] [-o http port]
-O https port]
```

A new tree is installed with the specified tree name and context. If the parameters are not specified in the command line, ndsconfig takes the default value for each of the missing parameters.

For example, to create a new tree, you could enter the following command:

```
ndsconfig new -t corp-tree -n o=company -a cn=admin.o=company
```

Adding a Server into an Existing Tree

Use the following syntax:

```
ndsconfig add -t treename -n server context -a admin FDN [-e] [-L ldap port]
[-l SSL port] [-o http port] -O https port] [-S server name] [-d path for dib]
[-p IP address] [-m module]
```

A server is added to an existing tree in the specified context. If the context that the user wants to add the Server object to does not exist, ndsconfig creates the context and adds the server.

LDAP and security services can also be added after eDirectory has been installed into the existing tree.

For example, to add a server into an existing tree, you could enter the following command:

```
ndsconfig add -t corp-tree -n o=company -a cn=admin.o=company
```

Removing a Server Object and Directory Services from a Tree

Use the following syntax:

```
ndsconfig rm -a admin FDN
```

eDirectory and its database are removed from the server.

NOTE: The HTML files created using iMonitor will not be removed. You must manually remove these files before removing eDirectory.

For example, to remove the eDirectory Server object and directory services from a tree, you could enter the following command:

```
ndsconfig rm -a cn=admin.o=company
```

ndsconfig Utility Parameters

ndsconfig Parameter	Description
new	Creates a new eDirectory tree. If the parameters are not specified in the command line, ndsconfig prompts you to enter values for each of the missing parameters.
def	Creates a new eDirectory tree. If the parameters are not specified in the command line, ndsconfig takes the default value for each of the missing parameters.
add	Adds a server into an existing tree.
rm	Removes the Server object and directory services from a tree.
-i	Ignores a tree of the same name, while installing a new tree. This option is generally not recommended for use.
-S	Specifies the server name. The default server name is <i>host name</i> .
-t	The tree name to which the server has to be added. If not specified, ndsconfig uses the tree name from the <code>n4u.base.tree-name</code> parameter specified in the <code>etc/nds.conf</code> file.
-n	The context of the server into which the Server object is added. If not specified, ndsconfig uses the context from the <code>n4u.nds.server-context</code> parameter specified in the <code>/etc/nds.conf</code> file.
-d	The directory path where the database files will be stored.
-L	The TCP port number on the LDAP server.
-I	The SSL port number on the LDAP server.
-a	Distinguished name of the User object that has Supervisor rights to the context in which the Server object and directory services will be created.
-e	Enables clear text passwords for LDAP objects.
-p	Installs eDirectory Server into an existing tree by specifying the IP address of a server hosting the tree. If this option is used, SLP is not used for tree lookup.

ndsconfig Parameter	Description
-m	Specifies the module name to install. While installing a new tree, you can install only the ds module. After installing the ds module, you can add the NMAS, LDAP, SAS, HTTP and SNMP services using the add command. If the module name is not specified, by default, all the five modules are installed.
-o	Specifies the HTTP clear port number.
-O	Specifies the HTTP secure port number.
set	Sets the value for the specified eDirectory configurable parameters. If the parameter list is not specified, ndsconfig lists all the eDirectory configurable parameters.
get	Lets you view the current value of the eDirectory configurable parameters.
get help	Lets you view the help strings for the eDirectory configurable parameters.

Using ndsconfig to Install an AIX Server into a Tree with Dotted Name Containers

You can use ndsconfig to install an AIX server into an eDirectory tree that has containers using dotted names (for example, novell.com).

Because ndsconfig is a command line utility, using containers with dotted names requires that those dots be escaped out, and the parameters containing these contexts must be enclosed in double quotes. For example, to install a new eDirectory tree on an AIX server using “O=novell.com” as the name of the O, use the following command:

```
ndsconfig new -a "admin.novell\com" -t novell_tree -n "OU=servers.O=novell\com"
```

The Admin name and context and the server context parameters are enclosed in double quotes, and only the dot ('.') in novell.com is escaped using the '\' (backslash) character.

You can also use this format when installing a server into an existing tree.

NOTE: You should use this format when entering dotted admin name and context while using utilities such as ndsrepair, ndsbackup, ndsmerge, ndslogin, and ldapconfig.

Using the nmasinst Utility to Configure NMAS

For eDirectory 8.7.3, by default, ndsconfig configures NMAS. You can also use nmasinst on Linux, Solaris, and AIX systems to configure NMAS.

Ndsconfig only configures NMAS and does not install the login methods. To install these login methods, you can use nmasinst.

IMPORTANT: You must configure eDirectory with ndsconfig before you install the NMAS login methods. You must also have administrative rights to the tree.

- ◆ [“Configuring NMAS” on page 50](#)
- ◆ [“Installing Login Methods” on page 51](#)

Configuring NMAS

By default, ndsconfig configures NMAS. You can also use nmasinst for the same.

To configure NMAS and create NMAS objects in eDirectory, enter the following at the server console command line:

```
nmasinst -i admin.context tree_name
```

nmasinst will prompt you for a password.

This command creates the objects in the Security container that NMAS needs, and installs the LDAP extensions for NMAS on the LDAP Server object in eDirectory.

The first time NMAS is installed in a tree, it must be installed by a user with enough rights to create objects in the Security container. However, subsequent installs can be done by container administrators with the Read-only right to the Security container. nmasinst will verify that the NMAS objects exist in the Security container before it tries to create them.

nmasinst does not extend the schema. The NMAS schema is installed as part of the base eDirectory schema.

Installing Login Methods

To install login methods using nmasinst, enter the following at the server console command line:

```
nmasinst -addmethod admin.context tree_name config.txt_path
```

The last parameter specifies the config.txt file for the login method that is to be installed. A config.txt file is provided with each login method.

Here is an example of the -addmethod command:

```
nmasinst -addmethod admin.novell MY_TREE ./nmas-methods/novell/Simple  
Password/config.txt
```

If the login method already exists, nmasinst will update it.

For more information, see “Managing Login and Post-Login Methods and Sequences” (<http://www.novell.com/documentation/lg/nmas23/admin/data/a53vj9a.html>) in the *Novell Modular Authentication Service Administration Guide*.

6 Migrating to eDirectory 8.7.3.10

This document guides you to migrate your Novell® eDirectory™ servers to eDirectory 8.7.3 SP10 when you have to upgrade your operating system also.

eDirectory 8.7.3 SP10 supports the following platforms:

Platform	Supported Versions
Linux*	<ul style="list-style-type: none"> ◆ OES Linux SP2 ◆ SUSE Linux Enterprise Server 10 x86_64 and SUSE Linux Enterprise Server 9 x86_64 ◆ SUSE Linux Enterprise Server 10, SUSE® Linux Enterprise Server 9 and SUSE Linux Enterprise Server 8.x ◆ Red Hat* Advanced Server 4.0 x86_64 ◆ Red Hat* Enterprise Server 3.0 ◆ Red Hat* Advanced Server 3.0 and Red Hat* Advanced Server 4.0
Solaris	<ul style="list-style-type: none"> ◆ Solaris 8 and 9 on Sun* SPARC
AIX	<ul style="list-style-type: none"> ◆ AIX 5L Version 5.2
NetWare®	<ul style="list-style-type: none"> ◆ NetWare 6.5 (OES) with Support Pack 6 and NetWare 6.5 Support Pack 7
Windows*	<ul style="list-style-type: none"> ◆ Windows Server 2003 with Service Pack 1

With the change in the operating systems supported in eDirectory 8.7.3 SP10, there are certain versions that eDirectory 8.7.3 SP10 does not support that were earlier supported with eDirectory 8.7.3.x. It is also advisable that you upgrade your older versions of eDirectory/NDS to eDirectory 8.7.3 before trying to migrate to eDirectory 8.7.3 SP10.

There are two scenarios while migrating to eDirectory 8.7.3 SP10:

- ◆ Migrating to eDirectory 8.7.3 SP10 when platform upgrade is possible.

Here, you upgrade your operating system to a supported version and then upgrade eDirectory to eDirectory 8.7.3 SP10.

- ◆ Migrating to eDirectory 8.7.3 SP10 when platform upgrade is not possible.

Here, you cannot upgrade your operating system to a supported version as the operating system migration path is not possible.

Migrating to eDirectory 8.7.3 SP10 While Upgrading the Operating System

In this scenario, you can migrate to eDirectory 8.7.3 SP10 after upgrading the operating system. The table below describes the migration path.

Table 1 Migration Path

Operating System	Starting State	Intermediate State	Desired State
NetWare	NetWare 5.1 SP6	NetWare 6.5 SP6	eDirectory 8.7.3 SP10
	NetWare 6 SP3	NetWare 6.5 SP6	eDirectory 8.7.3 SP10
Windows	Windows NT 4.0 SP6 + eDirectory 8.7.3	Windows 2003 + eDirectory 8.7.3	Windows 2003 + eDirectory 8.7.3 SP10
Linux	SuSE ES 8.1 + eDirectory 8.7.3	OES SP2 + eDirectory 8.7.3	OES SP2 + eDirectory 8.7.3 SP10
	SLES 9 + eDirectory 8.7.3	SLES 9 SP3 + eDirectory 8.7.3	SLES 9 SP3 + eDirectory 8.7.3 SP10
	Red Hat 9.0 + eDirectory 8.7.3	Red Hat AS 4.0 + eDirectory 8.7.3	Red Hat AS 4.0 + eDirectory 8.7.3 SP10
AIX	AIX 5.1 + eDirectory 8.7.3	AIX 5.2 + eDirectory 8.7.3	AIX 5.2 + eDirectory 8.7.3 SP10

Precautions: Before upgrading eDirectory on UNIX and Linux, ensure that the hostname is configured to a valid IP address and not to loopback address in `/etc/hosts`.

Recommendations

1. Backup your eDirectory 8.7.3 files before upgrading the operating system. Stop eDirectory and backup the following files:
 - ◆ `nds.rfl` directory (by default this directory is present under the `dib` directory)
 - ◆ `nds.conf` file
 - ◆ `nici` directory
 - ◆ log files
2. Do not perform any operations on the intermediate state other than upgrading eDirectory or the operating system, if the eDirectory version is not supported on a particular operating system in the intermediate state.

Migrating to eDirectory 8.7.3 SP10 Without Upgrading the Operating System

This method is used in such migration scenarios where there is no operating system upgrade path to support eDirectory 8.7.3 SP10 version.

For example, eDirectory 8.7.3 is installed on Red Hat 7.3. A customer using Red Hat 7.3 wants to upgrade to eDirectory 8.7.3 SP10. eDirectory 8.7.3 SP10 is supported on Red Hat AS 3.0 and there is no upgrade path from Red Hat 7.3 to Red Hat AS 3.0.

Complete the following steps to migrate to eDirectory 8.7.3 SP10:

- 1** Stop the eDirectory server.
- 2** Take a backup of the following eDirectory 8.7.3 files:
 - ♦ `dib` directory
 - ♦ `nds.rfl` directory (by default, this directory is present under the `dib` directory)
 - ♦ `nds.conf` file
 - ♦ `nici` directory
 - ♦ log files
- 3** Install the new operating system.
- 4** Restore the `nici` folder to the `/var/novell` folder from backup performed before installing the new operating system.
- 5** Install eDirectory 8.7.3 on the server (a new install) and upgrade to 8.7.3 SP10.
- 6** Restore the `dib` and `nds.rfl` directories.
- 7** Restore the `nds.conf` in `/etc` folder.
- 8** Edit `nds.conf` file and add the following:

```
nds4u.nds.dibdir=dib_file_location
```
- 9** By default, the `lib` and `var` are defined. But if you optionally prefer to change the locations, edit the following in `nds.conf` file:

```
n4u.server.libdir=lib_directory  
n4u.server.vardir=var_directory
```
- 10** You can also store the `nds.conf` in a user defined location instead of the default `/etc` folder. If you prefer to do so, provide the `nds.conf` file location in the environment variable `$NDS_CONF`.
- 11** Run `ndsconfig upgrade` after restoring the DIB and configuration files to upgrade the instance for 8.7.3 SP10.

7

Uninstalling Novell eDirectory

This chapter contains the following information:

- ◆ “Uninstalling eDirectory on NetWare” on page 57
- ◆ “Uninstalling eDirectory on Windows” on page 57
- ◆ “Uninstalling eDirectory on Linux, Solaris, or AIX” on page 59

Uninstalling eDirectory on NetWare

If necessary, you can remove eDirectory™ from a NetWare® server.

IMPORTANT: Removing eDirectory from a NetWare server makes the NetWare volumes and file system inaccessible.

Removing eDirectory also removes the roll-forward log directory and all the logs in it. If you want to be able to use the logs for restoring eDirectory on this server in the future, before removing eDirectory you must first copy the roll-forward logs to another location. For information about roll-forward logs, see “Using Roll-Forward Logs” in the *Novell eDirectory 8.7.3 Administration Guide*.

- 1 At the server console, run NWCONFIG.
- 2 Select Directory Options > Remove Directory Services from This Server.
- 3 Follow the online instructions.

Reinstalling eDirectory

If you used NWCONFIG to uninstall eDirectory, follow these steps to reinstall eDirectory:

- 1 Edit the sys:system\schema\schema.cfg file to uncomment the following entries:
 - ◆ ndps100.sch
 - ◆ ndps200.sch
 - ◆ ndps201.sch
- 2 From the NetWare console, run NWCONFIG.
- 3 Select Product Options > Install a Product Not Listed.
- 4 Specify the location containing the Novell eDirectory 8.7.3 installation package.
See “Installing or Upgrading Novell eDirectory 8.7.3 on NetWare” on page 9 for more information.

Uninstalling eDirectory on Windows

Use the Windows Control Panel to remove eDirectory, ConsoleOne, SLP DA, and NICI from Windows servers.

IMPORTANT: Removing eDirectory also removes the roll-forward log directory and all the logs in it. If you want to be able to use the logs for restoring eDirectory on this server in the future, before removing eDirectory you must first copy the roll-forward logs to another location. For information about roll-forward logs, see “Using Roll-Forward Logs” in the *Novell eDirectory 8.7.3 Administration Guide*.

- ◆ “Uninstalling eDirectory, ConsoleOne, and SLP DA” on page 58
- ◆ “Uninstalling an Upgraded Version of eDirectory” on page 58
- ◆ “Uninstalling NICI” on page 58

Uninstalling eDirectory, ConsoleOne, and SLP DA

- 1** On the Windows server where eDirectory is installed, click Start > Settings > Control Panel > Add/Remove Programs.
- 2** Select eDirectory, ConsoleOne, or the SLP Directory Agent from the list, then click Add/Remove.
- 3** Confirm that you want to remove your selection by clicking Yes.
The Installation Wizard removes the program from the server.

Uninstalling an Upgraded Version of eDirectory

When uninstalling eDirectory 8.7.3, you might receive the following error if the installation of eDirectory 8.7.3 was an upgrade from NDS eDirectory or NDS eDirectory 8.5:

```
Incompatible JClient/DClient Package  
JClient Revision 1.0.19  
DClient Revision 1.1.1095
```

This error occurs only when the previous eDirectory installation was performed on a date later than the dates of the eDirectory 8.7.3 files located in the \nt\i386\ndsonnt\nt\lib directory on the Novell eDirectory 8.7.3 CD. If the previous installation was performed prior to those dates, this error will not occur.

To solve this issue, copy the .jar files from the \nt\i386\ndsonnt\nt\lib directory on the Novell eDirectory 8.7.3 CD to the \program files\common files\novell\nt\lib directory on the Windows server before performing the eDirectory 8.7.3 uninstall.

Uninstalling NICI

- 1** On the Windows server where eDirectory is installed, click Start > Settings > Control Panel > Add/Remove Programs.
- 2** Select NICI from the list, then click Add/Remove.
- 3** Confirm that you want to remove NICI by clicking Yes.
The Installation Wizard removes NICI from the server.

After uninstalling NICI, if you want to completely remove NICI from your system, delete the C:\winnt\system32\novell\nici subdirectory. You might need to take ownership of some of the files and directories to delete them.

WARNING: After the NICI subdirectory has been removed, any data or information that was previously encrypted with NICI will be lost.

Uninstalling eDirectory on Linux, Solaris, or AIX

Use the `nds-uninstall` utility to uninstall eDirectory components from Linux, Solaris, or AIX systems. This utility uninstalls eDirectory from the local host.

IMPORTANT: Removing eDirectory also removes the roll-forward log directory and all the logs in it. If you want to be able to use the logs for restoring eDirectory on this server in the future, before removing eDirectory you must first copy the roll-forward logs to another location. For information about roll-forward logs, see ["Using Roll-Forward Logs"](#) in the *Novell eDirectory 8.7.3 Administration Guide*.

- 1 Execute the `nds-uninstall` command.

The utility lists the installed components.

- 2 Select the desired component.

Use the following syntax:

```
nds-uninstall -c component1 [[-c component2]...] [-h]
```

If you do not provide the required parameters in the command line, the `nds-uninstall` utility will prompt for the parameters.

Parameter	Description
-h	Displays the help strings.
-c	Specifies the component that is to be uninstalled. More than one component can be uninstalled by using the <code>-c</code> option multiple times.

NOTE: Make sure you deconfigure the server on the machine where eDirectory is installed before attempting to run `nds-uninstall`.

For example, to uninstall Novell eDirectory Server packages, enter the following command:

```
nds-uninstall -c server
```


8

Configuring Novell eDirectory on Linux, Solaris, or AIX Systems

Novell® eDirectory™ includes configuration utilities that simplify the configuration of various eDirectory components on Linux, Solaris, and AIX systems. The following sections provide information about functionality and usage of eDirectory configuration components:

- ♦ “Configuration Utilities” on page 61
- ♦ “Configuration Parameters” on page 62

Configuration Utilities

This section provides information about using the following eDirectory configuration utilities:

- ♦ “The ndsconfig Utility” on page 61
- ♦ “Using the ldapconfig Utility to Configure the LDAP Server and LDAP Group Objects” on page 61
- ♦ “Using the nmasinst Utility to Configure Novell Modular Authentication Service” on page 61

The ndsconfig Utility

You can use the ndsconfig utility to configure eDirectory. This utility can also be used to add the eDirectory Replica Server into an existing tree or to create a new tree. For more information, see “Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server” on page 28.

NOTE: Ensure that the NCP™ server name is unique in the network.

To change the current configuration of the installed components, use the following syntax:

```
ndsconfig {set value_list | get [parameter_list] | get help [parameter_list]}
```

Refer to “ndsconfig Utility Parameters” on page 29 for a description of ndsconfig parameters.

Using the ldapconfig Utility to Configure the LDAP Server and LDAP Group Objects

You can use the LDAP configuration utility, ldapconfig, on Linux, Solaris, and AIX systems to modify, view, and refresh the attributes of LDAP Server and Group objects.

For more information, see “Using the ldapconfig Utility on UNIX” in the *Novell eDirectory 8.7.3 Administration Guide*.

Using the nmasinst Utility to Configure Novell Modular Authentication Service

For eDirectory 8.7.3, by default, ndsconfig configures NMAS. You can also use nmasinst on Linux, Solaris, and AIX systems to configure NMAS.

ndsconfig only configures NMAS and does not install the login methods. To install these login methods, you can use nmasinst. For more information, see [“Using the nmasinst Utility to Configure NMAS” on page 31](#).

Configuration Parameters

The eDirectory configuration parameters are stored in the nds.conf file.

When configuration parameters are changed, ndsd needs to be restarted for the new value to take effect.

However, for some configuration parameters, ndsd need not be restarted. These parameters are listed below:

- ◆ n4u.nds.inactivity-synchronization-interval
- ◆ n4u.nds.synchronization-restrictions
- ◆ n4u.nds.janitor-interval
- ◆ n4u.nds.backlink-interval
- ◆ n4u.nds.drl-interval
- ◆ n4u.nds.flatcleaning-interval
- ◆ n4u.nds.server-state-up-threshold
- ◆ n4u.nds.heartbeat-schema
- ◆ n4u.nds.heartbeat-data

The following table provides a description of all the configuration parameters.

Parameter	Description
n4u.nds.preferred-server	The host name of the machine that hosts the eDirectory service. Default=null
n4u.base.tree-name	The tree name that Account Management uses. This is a mandatory parameter set by the Account Management installer. This parameter cannot be set or changed by the administrator.
n4u.base.dclient.use-udp	The Directory User Agent can use UDP in addition to TCP for communicating with eDirectory servers. This parameter enables the UDP transport. Default=0 Range=0, 1
n4u.base.slp.max-wait	The Service Location Protocol (SLP) API calls timeout. Default=30 Range=3 to 100

Parameter	Description
n4u.nds.advertise-life-time	eDirectory reregisters itself with the Directory Agent after this time period. Default=3600 Range=1 to 65535
n4u.server.signature-level	Determines the level of enhanced security support. Increasing this value increases security, but decreases performance. Default=1 Range=0 to 3
n4u.nds.dibdir	The eDirectory directory information database. Default=/var/nds/dib This parameter is set during installation and cannot be modified later.
n4u.nds.server-guid	A globally unique identifier for eDirectory server. Default=null
n4u.nds.server-name	The name of the eDirectory Server. Default=null
n4u.nds.bindery-context	The Bindery context string. Default=null
n4u.nds.server-context	The context that the eDirectory server is added to. This parameter cannot be set or changed.
n4u.nds.external-reference-life-span	The number of hours unused external references are allowed to exist before being removed. Default=192 Range=1 to 384
n4u.nds.inactivity-synchronization-interval	The interval (in minutes) after which full synchronization of the replicas is performed, following a period of no change to the information held in eDirectory on the server. Default=60 Range=2 to 1440
n4u.nds.synchronization-restrictions	The Off value allows synchronization with any version of eDirectory. The On value restricts synchronization to version numbers you specify as parameters (for example, ON,420,421). Default=Off
n4u.nds.janitor-interval	The interval (in minutes) after which the eDirectory Janitor process is executed. Default=2 Range=1 to 10080

Parameter	Description
n4u.nds.backlink-interval	The interval (in minutes) after which eDirectory backlink consistency is checked. Default=780 Range=2 to 10080
n4u.nds.flatcleaning-interval	The interval (in minutes) after which the flatcleaner process automatically begins purging and deleting entries from the database. Default=720 Range=1 to 720
n4u.nds.server-state-up-threshold	The server state up threshold, in minutes. This is the time after which eDirectory checks the server state before returning -625 errors. Default=30 Range=1 to 720
n4u.nds.heartbeat-schema	The heartbeat base schema synchronization interval in minutes. Default=240 Range=2 to 1440
n4u.nds.heartbeat-data	The heartbeat synchronization interval in minutes. Default=60 Range=2 to 1440
n4u.nds.drl-interval	The interval (in minutes) after which eDirectory distributed reference link consistency is checked. Default=780 Range=2 to 10080
n4u.server.tcp-port	The default port used if the port number is not specified in the n4u.server.interfaces parameter.
n4u.server.max-interfaces	This parameter specifies maximum number of interfaces that eDirectory will use. This value can range from 1 to 2048. Default value is 128.
n4u.server.max-openfiles	This parameter specifies the maximum number of file descriptors that eDirectory can use. Default=maximum allowed by the administrator
n4u.ldap.lburp.transize	Number of records that are sent from the Novell Import/Export client to the LDAP server in a single LBURP packet. You can increase the transaction size to ensure that multiple add operations can be performed in a single request. Default=25 Range=1 to 250

Parameter	Description
n4u.server.sid-caching	Enables SSL session ID caching. Refer to the SSL v3.0 RFC for more details about session ID caching in SSL.
n4u.server.max-threads	The maximum number of threads that will be started by the eDirectory server. This is the number of concurrent operations that can be done within the eDirectory server. Default=64 Range=32 to 512
n4u.server.idle-threads	The maximum number of idle threads that are allowed in the eDirectory server. Default=8 Range=1 to 128
n4u.nds.dofsync	Setting this parameter to 0 increases update performance significantly for large databases, but there is a risk of database corruption if the system crashes.
n4u.server.configdir	The eDirectory configuration files are placed here. Default=/etc
n4u.server.vardir	The eDirectory and utilities log files are placed here. Default=/var/nds
n4u.server.libdir	The eDirectory specific libraries are placed here in the nds-modules directory. Default=/usr/lib
n4u.server.start-threads	Initial number of threads to be started up. Default=8
http.server.interfaces	Comma-separated list of interfaces that HTTP server should use.
https.server.interfaces	Comma-separated list of interfaces that HTTPS should use.
http.server.request-io-buffer-size	Default IO buffer size.
http.server.request_timeout-seconds	Server request timeout.
http.server.keep-timeout-seconds	Number of seconds to wait for the next request from the same client on the same connection.
http.server.threads-per-processor	HTTP thread pool size per processor.
http.server.session-exp-seconds	Session expiration time in seconds.
http.server.sadmin-passwd	Session administrator password.
http.server.module-base	HTTP server webroot.
https.server.cached-cert-dn	HTTPS server cached certificate DN.

Parameter	Description
https.server.cached-server-dn	HTTPS server cached DN.
http.server.trace-level	Diagnostic trace level of HTTP server.
http.server.auth-req-tls	HTTP server authentication requires TLS.
http.server.clear-port	Server port for the HTTP protocol.
http.server.tls-port	Server port for the HTTPS protocol.

A

Linux, Solaris, and AIX Packages for Novell eDirectory

Novell® eDirectory™ includes a Linux, Solaris, and AIX package system, which is a collection of tools that simplify the installation and uninstallation of various eDirectory components. Packages contain makefiles that describe the requirements to build a certain component of eDirectory. Packages also include configuration files, utilities, libraries, daemons, and man pages that use the standard Linux, Solaris, or AIX tools installed with the OS.

The following table provides information about the Linux, Solaris, and AIX packages that are included with Novell eDirectory.

Package	Description
NOVLice	Contains the Novell Import Convert Export utility and is dependent on the NOVLMgmt, NOVLxis and NLDAPbase packages.
NDSbase	Represents the Directory User Agent. This package is dependent on the NICI package. The NDSbase package contains the following: <ul style="list-style-type: none"> ♦ Authentication toolbox containing the RSA authentication needed for eDirectory ♦ Platform-independent system abstraction library, a library containing all the defined Directory User Agent functions, and the schema extension library ♦ Combined configuration utility and the Directory User Agent test utility ♦ eDirectory configuration file and manual pages
NDScommon	Contains the man pages for the eDirectory configuration file, install, and uninstall utilities. This package is dependent on the NDSbase package.
NDSmasv	Contains the libraries required for mandatory access control (MASV).

Package	Description
NDSserv	<p>Contains all the binaries and libraries needed by the eDirectory Server. It also contains the utilities to manage the eDirectory Server on the system. This package is dependent on the NDSbase, NDScommon, NDSmasv, NLDAPsdk, NOVLPkia and NOVLPkit packages.</p> <p>The NDSserv package contains the following:</p> <ul style="list-style-type: none"> ♦ NDS install library, FLAIM library, trace library, NDS library, LDAP server library, LDAP install library, index editor library, DNS library, merge library, and LDAP extension library for LDAP SDK ♦ eDirectory Server daemon ♦ Binary for DNS and a binary to load or unload LDAP ♦ The utility needed to create the MAC address, the utility to trace the server and change some of the global variables of the server, the utility to back up and restore eDirectory, and the utility to merge eDirectory trees ♦ Startup scripts for DNS, NDS, and NLDAP ♦ Man pages
NDSimon	<p>Contains the runtime libraries and utilities used to search and retrieve data from eDirectory services. This package is dependent on the NDSbase package.</p>
NDSrepair	<p>Contains the runtime libraries and the utility that corrects problems in the eDirectory database. This package is dependent on the NDSbase package.</p>
NDSslp	<p>The NDSslp package contains the following:</p> <ul style="list-style-type: none"> ♦ SLP User Agent/Service Agent daemon and the SLP libraries to access SLP ♦ Transport library, utility library, and configuration library that the SLP daemon uses ♦ Unicode* library that the SLP daemon and API library use.
NLDAPbase	<p>Contains LDAP libraries, extensions to LDAP libraries, and the following LDAP tools:</p> <ul style="list-style-type: none"> ♦ Idapdelete ♦ Idapmodify ♦ Idapmodrtn ♦ Idapsearch <p>This package is dependent on the NLDAPsdk package.</p>
NDS set of packages	<p>Contains a set of ConsoleOne snap-ins.</p>
NOVLC1	<p>Contains Linux and Solaris packages for the ConsoleOne management utility.</p>
C1JRE	<p>Contains the Java runtime files and libraries that are required to run ConsoleOne on Linux or Solaris systems.</p>

Package	Description
NOVLnmas	Contains all the NMAS libraries and the nmasinst binaries needed for NMAS server. This package is dependent on the NICI and NDSmasv packages.
NLDAPsdk	Contains Novell extensions to LDAP runtime and Security libraries (Client NICI).
NOVLsubag	Contains the runtime libraries and utilities for the eDirectory SNMP subagent. This package is dependent on the NICI, NDSbase, and NLDAPbase packages.
NOVLpkit	Provides PKI Services which do not require eDirectory. This package is dependent on the NICI and NLDAPsdk packages.
NOVLpkis	Provides PKI Server Service. This package is dependent on the NICI, NDSbase, and NLDAPsdk packages.
NOVLsnmp	The runtime libraries and utilities for SNMP. This package is dependent on the NICI package.
NDSdexvnt	Contains the library that manages events generated in Novell eDirectory to other databases.
NOVLpkia	Provides PKI services. This package is dependent on the NICI, NDSbase, and NLDAPsdk packages.
NOVLembox	Provides the eMBox infrastructure and eMTools.
NOVLimgnt	Contains runtime libraries for Novell Language Management.
NOVLstlog	Contains the Novell status logger.
NOVLxis	Contains the runtime libraries for Novell XIS.
NOVLsas	Contains the Novell SAS libraries.
NOVLntls	Contains Novell TLS library. This package is identified as: <ul style="list-style-type: none"> ◆ NOVLntls on Solaris, and AIX. ◆ ntlsl on Linux

B

Configuring OpenSLP for eDirectory

This appendix provides information for network administrators on the proper configuration of OpenSLP for Novell® eDirectory™ installations without the Novell Client™.

- ♦ “Service Location Protocol” on page 71
- ♦ “SLP Fundamentals” on page 71
- ♦ “Configuration Parameters” on page 73

Service Location Protocol

OpenSLP is an open-source implementation of the IETF Service Location Protocol Version 2.0 standard, which is documented in [IETF Request-For-Comments \(RFC\) 2608](http://www.ietf.org/rfc/rfc2608.txt?number=2608) (<http://www.ietf.org/rfc/rfc2608.txt?number=2608>).

In addition to implementing the SLP v2 protocol, the interface provided by OpenSLP source code is an implementation of another IETF standard for programmatically accessing SLP functionality, documented in [RFC 2614](http://www.ietf.org/rfc/rfc2614.txt?number=2614) (<http://www.ietf.org/rfc/rfc2614.txt?number=2614>).

To fully understand the workings of SLP, we recommend that you read these two documents and internalize them. They are not necessarily light reading, but they are essential to the proper configuration of SLP on an intranet.

For more information on the OpenSLP project, see the [OpenSLP](http://www.OpenSLP.org) (<http://www.OpenSLP.org>) Web site and the [SourceForge](http://sourceforge.net/projects/openslp) (<http://sourceforge.net/projects/openslp>) Web site. The OpenSLP Web site provides several documents that contain valuable configuration tips. Many of these are incomplete at the time of this writing.

SLP Fundamentals

Service Location Protocol specifies three components:

- ♦ The user agent (UA)
- ♦ The service agent (SA)
- ♦ The directory agent (DA)

The user agent's job is to provide a programmatic interface for clients to query for services, and for services to advertise themselves. A user agent contacts a directory agent to query for registered services of a specified service class and within a specified scope.

The service agent's job is to provide persistent storage and maintenance points for local services that have registered themselves with SLP. The service agent essentially maintains an in-memory database of registered local services. In fact, a service cannot register with SLP unless a local SA is present. Clients can discover services with only a UA library, but registration requires an SA,

primarily because an SA must reassert the existence of registered services periodically in order to maintain the registration with listening directory agents.

The directory agent's job is to provide a long-term persistent cache for advertised services, and to provide a point of access for user agents to look up services. As a cache, the DA listens for SAs to advertise new services, and caches those notifications. Over a short time, a DA's cache will become more complete. Directory agents use an expiration algorithm to expire cache entries. When a directory agent comes up, it reads its cache from persistent storage (generally a hard drive), and then begins to expire entries according to the algorithm. When a new DA comes up, or when a cache has been deleted, the DA detects this condition and sends out a special notification to all listening SAs to dump their local databases so the DA can quickly build its cache.

In the absence of any directory agents, the UA will resort to a general multicast query that SAs can respond to, building a list of the requested services in much the same manner that DAs use to build their cache. The list of services returned by such a query is an incomplete and much more localized list than that provided by a DA, especially in the presence of multicast filtering, which is done by many network administrators, limiting broadcasts and multicasts to only the local subnet.

In summary, everything hinges on the directory agent that a user agent finds for a given scope.

Novell Service Location Providers

The Novell version of SLP takes certain liberties with the SLP standard in order to provide a more robust service advertising environment, but it does so at the expense of some scalability.

For example, in order to improve scalability for a service advertising framework, we want to limit the number of packets that are broadcast or multicast on a subnet. The SLP specification manages this by imposing restrictions on service agents and user agents regarding directory agent queries. The first directory agent discovered that services the desired scope is the one that a service agent (and consequently, local user agents) will use for all future requests on that scope.

The Novell SLP implementation actually scans all of the directory agents it knows about looking for query information. It assumes a 300-millisecond round trip time is too long, so it can scan 10 servers in about 3 to 5 seconds. This doesn't need to be done if SLP is configured correctly on the network, and OpenSLP assumes the network is in fact configured correctly for SLP traffic. OpenSLP's response timeout values are greater than that of Novell's SLP service provider, and it limits the number of directory agents to the first one that responds, whether or not that agent's information is accurate and complete.

User Agents

A user agent takes the physical form of a static or dynamic library that is linked into an application. It allows the application to query for SLP services.

User agents follow an algorithm to obtain the address of a directory agent to which queries will be sent. Once they obtain a DA address for a specified scope, they continue to use that address for that scope until it no longer responds, at which time they obtain another DA address for that scope. User agents locate a directory agent address for a specified scope by:

1. Checking to see if the socket handle on the current request is connected to a DA for the specified scope. (If the request happens to be a multipart request, there may already be a cached connection present on the request.)
2. Checking its local known DA cache for a DA matching the specified scope.

3. Checking with the local SA for a DA with the specified scope (and adding new addresses to the cache).
4. Querying DHCP for network-configured DA addresses that match the specified scope (and adding new addresses to the cache).
5. Multicasting a DA discovery request on a well-known port (and adding new addresses to the cache).

The specified scope is “default” if not specified. That is, if no scope is statically defined in the SLP configuration file, and no scope is specified in the query, then the scope used is the word “default”. It should also be noted that eDirectory never specifies a scope in its registrations. That's not to say the scope always used with eDirectory is “default.” In fact, if there is a statically configured scope, that scope becomes the default scope for all local UA requests and SA registrations in the absence of a specified scope.

Service Agents

Service agents take the physical form of a separate process on the host machine. In the case of Win32, `slpd.exe` runs as a service on the local machine. User agents query the local service agent by sending messages to the loop-back address on a well-known port.

A service agent locates and caches directory agents and their supported scope list by sending a DA discovery request directly to potential DA addresses by:

1. Checking all statically configured DA addresses (and adding new ones to the SA's known DA cache).
2. Requesting a list of DA's and scopes from DHCP (and adding new ones to the SA's known DA cache).
3. Multicasting a DA discovery request on a well-known port (and adding new ones to the SA's known DA cache).
4. Receiving DA advertising packets that are periodically broadcast by DAs (and adding new ones to the SA's known DA cache).

Since a user agent always queries the local service agent first, this is important, as the local service agent's response will determine whether or not the user agent continues to the next stage of discovery (in this case DHCP-- see steps 3 and 4 in “[User Agents](#)” on page 72).

Configuration Parameters

The SLP configuration parameters are stored in `slp.conf` file located in `/etc` on UNIX and Linux platforms, `sys:\etc` on NetWare, and `%systemroot%/slp.conf` on Windows platform. These parameters can be modified to tune the network operations.

For example, the following parameters control the DA discovery.

```
net.slp.useScopes = <comma delimited scope list>
net.slp.DAAddresses = <comma delimited address list>
net.slp.passiveDADetection = <"true" or "false">
net.slp.activeDADetection = <"true" or "false">
net.slp.DAActiveDiscoveryInterval = <0, 1, or a number of seconds>
```

The `useScopes` option indicates which scopes the SA will advertise into, and which scopes queries will be made to in the absence of a specific scope on the registration or query made by the service

or client application. Because eDirectory always advertises into and queries from the default scope, this list will become the default scope list for all eDirectory registrations and queries.

The DAAddresses option is a comma-delimited list of dotted decimal IP addresses of DAs that should be preferred to all others. If this list of configured DAs does not support the scope of a registration or query, then SAs and UAs will resort to multicast DA discovery, unless such discovery is disabled.

The passiveDADetection option is True by default. Directory agents will periodically broadcast their existence on the subnet on a well-known port if configured to do so. These packets are termed DAAdvert packets. If this option is set to False, all broadcast DAAdvert packets are ignored by the SA.

The activeDADetection option is also True by default. This allows the SA to periodically broadcast a request for all DAs to respond with a directed DAAdvert packet. A directed packet is not broadcast, but sent directly to the SA in response to these requests. If this option is set to False, no periodic DA discovery request is broadcast by the SA.

The DAActiveDiscoveryInterval option is a try-state parameter. The default value is 1, which is a special value meaning that the SA should only send out one DA discovery request upon initialization. Setting this option to 0 has the same effect as setting the activeDADetection option to "false." Any other value is a number of seconds between discovery broadcasts.

These options, when used properly, can ensure an appropriate use of network bandwidth for service advertising. In fact, the default settings are designed to optimize scalability on an average network.