

Novell eDirectory™

8.8

www.novell.com

INSTALLATION GUIDE

September 30, 2005



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 © 2003-2005 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 8.8 Installation Guide
September 30, 2005

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

Novell Trademarks

Client32 is a trademark of Novell, Inc.

eDirectory is a trademark of Novell, Inc.

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

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

NMAS is a trademark of Novell, Inc.

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

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.

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

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

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

This Installation Guide describes how to install Novell® eDirectory™ 8.8. It is intended for network administrators, and contains the following sections:

- ♦ Chapter 1, “Installing or Upgrading Novell eDirectory on NetWare,” on page 7
- ♦ 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 47
- ♦ Chapter 5, “Installing or Updating Novell eDirectory on AIX,” on page 63
- ♦ Chapter 6, “Installing or Upgrading Novell eDirectory on HP-UX,” on page 77
- ♦ Chapter 7, “Relocating the DIB,” on page 91
- ♦ Chapter 8, “Configuring Novell eDirectory on Linux, Solaris, AIX, or HP-UX Systems,” on page 93
- ♦ Chapter 9, “Installing iManager Plug-ins,” on page 99
- ♦ Chapter 10, “Uninstalling Novell eDirectory,” on page 101
- ♦ Appendix A, “Linux, Solaris, AIX, and HP-UX Packages for Novell eDirectory,” on page 105
- ♦ Appendix B, “Server Health Checks,” on page 109
- ♦ Appendix C, “Configuring OpenSLP for eDirectory,” on page 115

Additional Documentation

For documentation on managing and administering eDirectory, see the *Novell eDirectory 8.8 Administration Guide* (<http://www.novell.com/documentation/edir88/index.html>).

Documentation Updates

For the most recent version of the *Novell eDirectory 8.8 Installation Guide*, see the Novell eDirectory 8.8 Documentation (<http://www.novell.com/documentation/edir88/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 Linux* and 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™ 8.8 on a NetWare® server:

- ♦ “System Requirements” on page 7
- ♦ “Prerequisites” on page 7
- ♦ “Hardware Requirements” on page 8
- ♦ “Forcing the Backlink Process to Run” on page 9
- ♦ “Updating the eDirectory Schema for NetWare” on page 9
- ♦ “Installing or Upgrading Novell eDirectory on NetWare” on page 10

System Requirements

- ☐ You can upgrade to eDirectory 8.8 on the following version of NetWare:
 - ♦ NetWare 6.5 with Support Pack 3 or later (<http://support.novell.com/filefinder/18197/index.html>)
- ☐ Administrative rights to the eDirectory tree so you can modify the schema.

For information on hardware requirements, see “Hardware Requirements” on page 8.

Prerequisites

- ☐ If you are installing into an eDirectory tree that has NetWare and Windows servers, each NetWare server must be running:
 - ♦ NetWare 5.1 with Support Pack 8 (<http://support.novell.com/filefinder/9331/index.html>) or later
 - ♦ NetWare 6.0 with Support Pack 5 (<http://support.novell.com/filefinder/13659/index.html>) or later
 - ♦ NetWare 6.5 with Support Pack 3 (<http://support.novell.com/filefinder/18197/index.html>) or later

Each Windows server must be running eDirectory 8.7.3 or later.

- ☐ (Conditional) NCI 2.7 and eDirectory 8.8 support key sizes up to 4096 bits. If you want to use a 4 KB key size, every server must be upgraded to eDirectory 8.8. In addition, every workstation using the management utilities, for example, iManager and ConsoleOne, must have NCI 2.7 installed on it.

When you upgrade your Certificate Authority (CA) server to eDirectory 8.8, the key size will not change; it will be 2 KB. The only way to create a 4 KB key size is recreate the CA on an eDirectory 8.8 server. In addition, you would have to change the default from 2 KB to 4 KB for the key size, during the CA creation.

- ❑ (Conditional) (to verify) If you are upgrading a NetWare server as a nonadministrator user, ensure that you have met the following prerequisites:

- ♦ A NetWare server in the eDirectory 8.8 tree installed as the tree admin

Ensure that you have the following rights:

- ♦ Supervisor rights to the container the server is being installed into.
- ♦ All Attributes rights: read, compare, and write rights over the W0.KAP.Security object.
- ♦ Entry rights: browse rights over Security container object.
- ♦ All Attributes rights: read and compare rights over Security container object.

As a nonadministrator user, you can only upgrade a NetWare server.

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 took 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 8.8, 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.

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.
- 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.

NOTE: In eDirectory 8.8 and later, you can have case sensitive passwords for all the utilities. Refer to *Novell eDirectory 8.8 What's New Guide* (<http://www.novell.com/documentation/edir88/index.html>) for more information.

- 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 dsreapir.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.

Installing or Upgrading Novell eDirectory on NetWare

This section contains the following information:

- ♦ “Installing or Upgrading Novell eDirectory 8.8 on NetWare” on page 10
- ♦ “Server Health Checks” on page 11
- ♦ “Installing NMAS Server Software” on page 11
- ♦ “Installing NMAS Client Software” on page 12
- ♦ “Installing into a Tree with Dotted Name Containers” on page 12

Installing or Upgrading Novell eDirectory 8.8 on NetWare

- 1** At the server console, enter **nwconfig.nlm**.
- 2** Select Product Options > Install a Product Not Listed.
- 3** Press F3 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_88: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.

NOTE: In eDirectory 8.8 and later, you can have case sensitive passwords for all the utilities. Refer to *Novell eDirectory 8.8 What's New Guide* (<http://www.novell.com/documentation/edir88/index.html>) for more information.

- 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 11 and “Installing NMAS Client Software” on page 12 for more information.
- 8** Click Finish to start the eDirectory installation.
- 9** To complete the installation, remove any diskettes or CDs when prompted, then click Yes to restart the server.

Server Health Checks

With eDirectory 8.8, when you upgrade eDirectory, two server health checks are conducted by default to ensure that the server is safe for the upgrade:

- ♦ “Basic Server Health” on page 110
- ♦ “Partitions and Replica Health” on page 110

Based on the results obtained from the health checks, the upgrade will either continue or exit as follows:

- ♦ If all the health checks are successful, the upgrade will continue.
- ♦ If there are minor errors, the upgrade will prompt you to continue or exit.
- ♦ If there are critical errors, the upgrade will exit.

See Appendix B, “Server Health Checks,” on page 109 for a list of minor and critical error conditions.

Skipping Server Health Checks

To skip server health checks, enter No when you prompted to perform the health check.

For more information, see Appendix B, “Server Health Checks,” on page 109.

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 8.8* 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

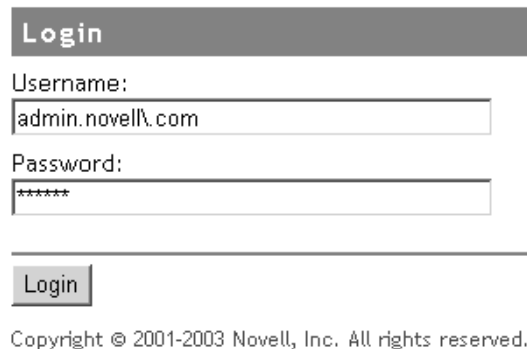
You can install a NetWare server into an eDirectory tree that has containers with dots in the names (for example, `O=novell.com` or `C=u.s.a`). Using containers with dotted names requires that those dots be escaped with the backslash character. To escape a dot, simply put a backslash in front of any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



The image shows a login window titled "Login". It contains two text input fields: "Username:" with the text "admin.novell\\.com" and "Password:" with masked characters "*****". Below the fields is a "Login" button. At the bottom of the window is a copyright notice: "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™ 8.8 on a 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 8.8 lets you install eDirectory for Windows without the Novell Client™. If you install eDirectory 8.8 on a machine already containing the Novell Client, eDirectory will use the existing Client. For more information, see “Installing or Updating Novell eDirectory 8.8 on Windows 2000 or Server 2003” on page 16.

System Requirements

- ☐ One of the following:
 - ♦ Windows 2000 Server with Service Pack 4 or later, Windows 2000 Advanced Server with Service Pack 4 or later
 - ♦ Windows Server 2003
- IMPORTANT:** Windows XP is not a supported Novell eDirectory 8.8 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 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 Server User Guide* for more information.

- ♦ Convert an existing FAT file system to NTFS, using the CONVERT command.

Refer to *Windows Server User Guide* for more information.

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.

- ❑ (Conditional) NCI 2.7 and eDirectory 8.8 support key sizes up to 4096 bits. If you want to use a 4 KB key size, every server must be upgraded to eDirectory 8.8. In addition, every workstation using the management utilities, for example, iManager and ConsoleOne, must have NCI 2.7 installed on it.

When you upgrade your Certificate Authority (CA) server to eDirectory 8.8, the key size will not change; it will be 2 KB. The only way to create a 4 KB key size is recreate the CA on an eDirectory 8.8 server. In addition, you would have to change the default from 2 KB to 4 KB for the key size, during the CA creation.

- ❑ If you are upgrading to eDirectory 8.8, make sure you have the latest NDS and eDirectory patches installed on all non-eDirectory 8.8 servers in the tree. You can get NDS and eDirectory patches from the Novell Support (<http://support.novell.com>) Web site.
- ❑ Make sure you have the latest Windows 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 upgrading from a previous version of eDirectory, it must be eDirectory 8.7 or later.
- ❑ (Conditional) (to verify) If you are installing a secondary server into an existing tree as a nonadministrator user, ensure that you have the following rights:
 - ♦ Supervisor rights to the container the server is being installed into.
 - ♦ Supervisor rights to the partition where you want to add the server.

NOTE: This is required for adding the replica when the replica count is less than 3.
 - ♦ All Attributes rights: read, compare, and write rights over the W0.KAP.Security object.
 - ♦ Entry rights: browse rights over Security container object.
 - ♦ All Attributes rights: read and compare rights over Security container object.

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 8.8 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 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 completing the following procedure. Running the backlink process is especially important on servers that do not contain a replica.

- 1** Click Start > Settings > Control Panel > Novell eDirectory Services
- 2** In the Services tab, select ds.dlm.
- 3** Click Configure.
- 4** In the Trigger tab, click Backlinker.

For more information about the backlink process, refer to the *Novell eDirectory 8.8 Administration Guide* (<http://www.novell.com/documentation/edir88/edir88/data/h0000005.html>).

Updating the eDirectory Schema for Windows

To install eDirectory 8.8 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 9.

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).
- 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 8.8 on Windows 2000 or Server 2003” on page 16
- ♦ “Server Health Checks” on page 18
- ♦ “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 8.8 on Windows 2000 or Server 2003

You can install eDirectory 8.8 for Windows without the Novell Client. If you install eDirectory 8.8 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 C, “Configuring OpenSLP for eDirectory,” on page 115
 - ♦ DHCP Options for Service Location Protocol (<http://www.openslp.org/doc/rfc/rfc2610.txt>)
 - ♦ OpenSLP Documentation (<http://www.openslp.org/#Documentation>)
- 3** If you have Autorun turned off, run setup.bat from the *Novell eDirectory 8.8* CD or from the downloaded file.

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.

- ♦ NCI 2.7

For more information on the Novell International Cryptographic Infrastructure (NICI), see the *NICI 2.7 Administration Guide* (<http://www.novell.com/documentation/beta/nici27x/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 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/noclienu/index.html>) online documentation.

4 View the license agreement, then click I Accept.

5 Select a language for the installation, then click Next.

6 Specify or confirm the installation path, then click Next.

7 Specify or confirm the DIB path, then click Next.

8 (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.

9 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.

NOTE: In eDirectory 8.8 and later, you can have case sensitive passwords for all the utilities. Refer to *Novell eDirectory 8.8 What's New Guide* (<http://www.novell.com/documentation/edir88/index.html>) for more information.

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

10 (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 2.5 Administration Guide* (<http://www.novell.com/documentation/imanager25/index.html>).

11 (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.

12 Select the NMASTM login methods you want to install, then click Next.

See “Installing NMASTM Server Software” on page 21 and “Installing NMASTM Client Software” on page 21 for more information.

13 Click Finish to complete the eDirectory installation.

Server Health Checks

With eDirectory 8.8, when you upgrade eDirectory, two server health checks are conducted by default to ensure that the server is safe for the upgrade.

- ♦ “Basic Server Health” on page 110
- ♦ “Partitions and Replica Health” on page 110

Based on the results obtained from the health checks, the upgrade will either continue or exit as follows:

- ♦ If all the health checks are successful, the upgrade will continue.
- ♦ If there are minor errors, the upgrade will prompt you to continue or exit.
- ♦ If there are critical errors, the upgrade will exit.

See Appendix B, “Server Health Checks,” on page 109 for a list of minor and critical error conditions.

Skiping Server Health Checks

To skip server health checks, disable server health checks when prompted in the installation Wizard

For more information, see Appendix B, “Server Health Checks,” on page 109.

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 8.8	Clear text (port 389)	Selects port 389.
eDirectory 8.8	Encrypted (port 636)	Selects port 636.
eDirectory 8.8	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.

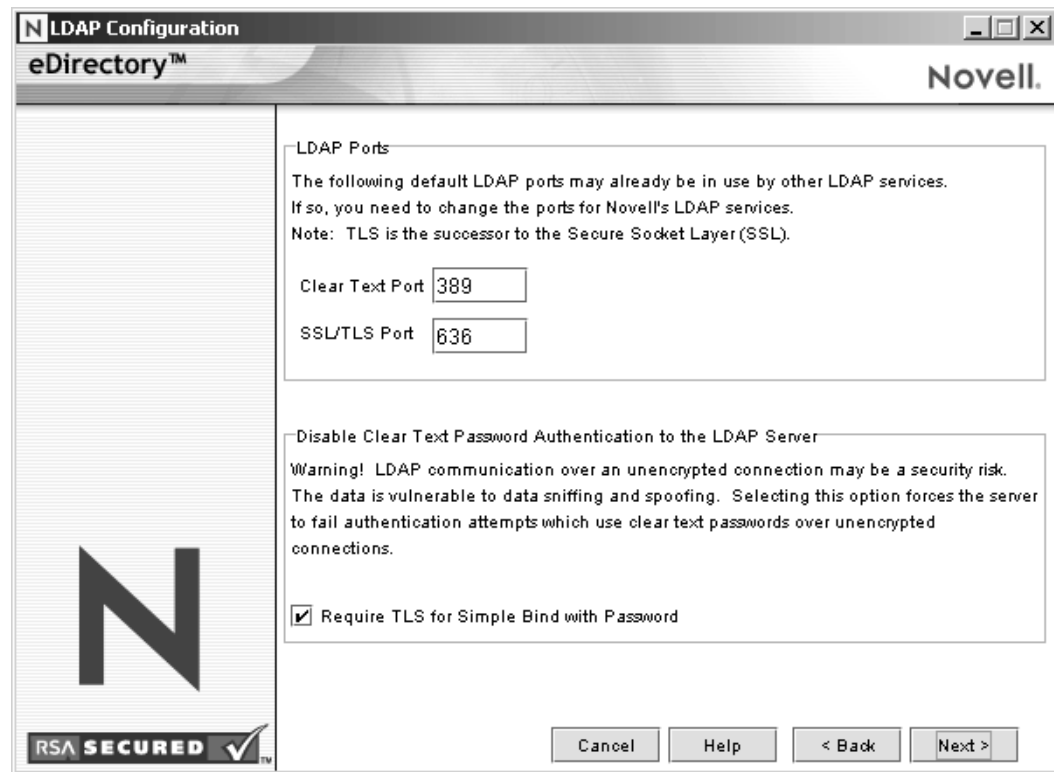
An LDAP Simple Bind requires only a DN and a password. The password is in clear text. If you use port 389, the entire packet is in clear text. By default, this option is disabled during the eDirectory installation.

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

General

Information | **Connections** | Searches | Events | Tracing | Referrals

Transport Layer Security (TLS / SSL)

Server Certificate:

Client Certificate:

Trusted Root Containers:

☐ Require TLS for all operations

☒ Enable and require mutual authentication

Ports

☒ Enable Encrypted Port

Port:

☒ Enable Non-Encrypted Port

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 onwards 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 8.8 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 8.8 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/beta/nmas30/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.

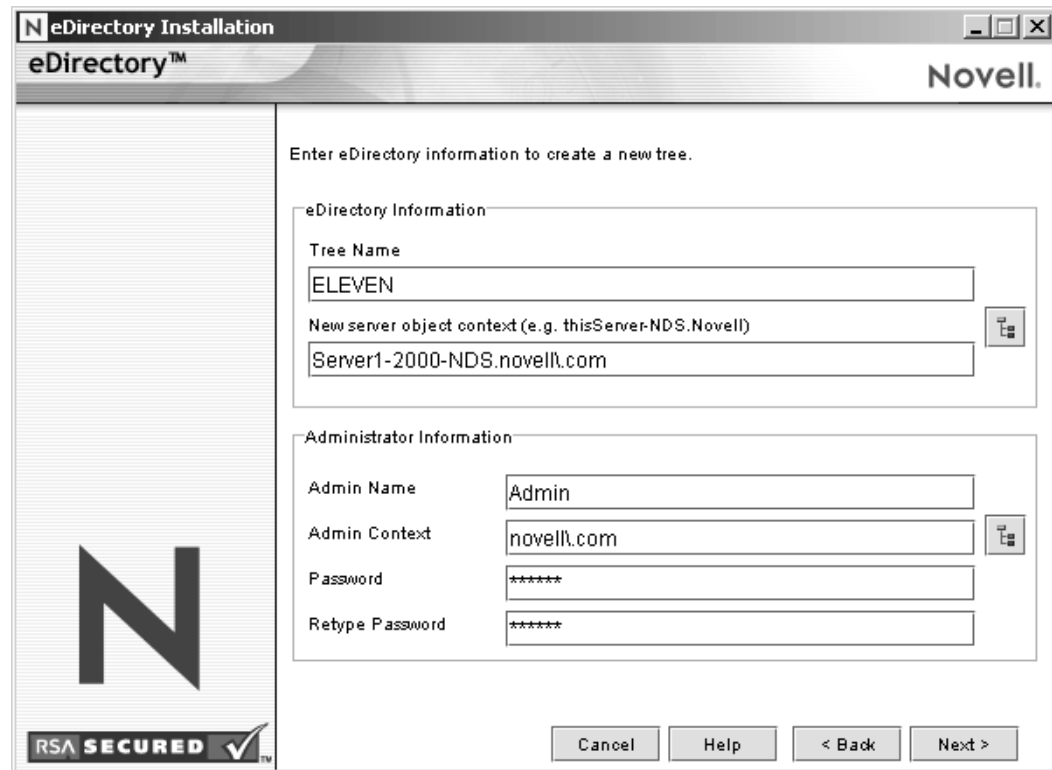
- 1** At a Windows client workstation, insert the *Novell eDirectory 8.8 CD*.
- 2** From the NMAS directory, run `nmasinstall.exe`.
- 3** Select the NMAS Client Components check box.
Optionally, you can select the NICI check box if you want to install this component.
- 4** Click OK, then follow the on-screen 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 (‘.’).

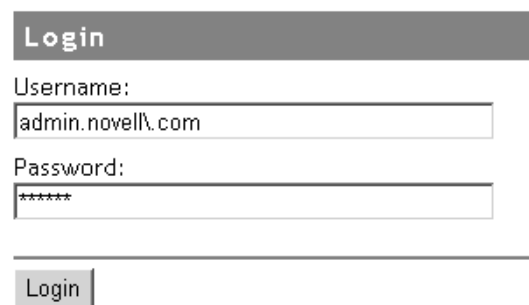
Figure 4 eDirectory Installation Information Screen



The screenshot shows the 'eDirectory Installation' window. The title bar includes the Novell logo and window controls. The main area is titled 'Enter eDirectory information to create a new tree.' It contains two sections: 'eDirectory Information' and 'Administrator Information'. In the first section, 'Tree Name' is 'ELEVEN' and 'New server object context' is 'Server1-2000-NDS.novell.com'. In the second section, 'Admin Name' is 'Admin', 'Admin Context' is 'novell.com', and both 'Password' and 'Retype Password' are masked with asterisks. A large 'N' logo and 'RSA SECURED' badge are on the left. Navigation buttons 'Cancel', 'Help', '< Back', and 'Next >' are at the bottom right.

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\.* in the Username field when logging in to iMonitor (see Figure 5).

Figure 5 iMonitor Login Screen



The screenshot shows the 'Login' screen. It has a title bar with the word 'Login'. Below it are two input fields: 'Username:' with the value 'admin.novell\.' and 'Password:' with masked characters '*****'. A 'Login' button is at the bottom.

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™ 8.8 on a Linux* server:

- ♦ “System Requirements” on page 23
- ♦ “Prerequisites” on page 23
- ♦ “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/lgnls/install/data/front.html>).

System Requirements

- ☐ One of the following:
 - ♦ SUSE® Linux Enterprise Server 9.1 (OES), SUSE Linux Enterprise Server 9, or SUSE® Linux Enterprise Server 8.x
To determine the version of SUSE Linux you are running, see the `/etc/SuSE-release` file.
 - ♦ Red Hat* Advanced Server 3
Ensure that the latest glibc patches are applied from Red Hat Errata (<http://rhn.redhat.com/errata>) on Red Hat systems. The minimum required version of the glibc library is version 2.1.
- ☐ 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

Prerequisites

- ☐ (Conditional) NCI 2.7 and eDirectory 8.8 support key sizes up to 4096 bits. If you want to use a 4 KB key size, every server must be upgraded to eDirectory 8.8. In addition, every workstation using the management utilities, for example, iManager and ConsoleOne, must have NCI 2.7 installed on it.

When you upgrade your Certificate Authority (CA) server to eDirectory 8.8, the key size will not change; it will be 2 KB. The only way to create a 4 KB key size is recreate the CA on an eDirectory 8.8 server. In addition, you would have to change the default from 2 KB to 4 KB for the key size, during the CA creation.

For more information, refer to “Installing NCI” on page 29.

☐ SLP installed and configured

With eDirectory 8.8, SLP does not get installed as part of the eDirectory installation.

Only a root user can install SLP.

For more information on installing SLP, refer to “Using SLP with eDirectory” on page 27.

☐ The NCI Foundation Key (NFK) file

☐ The Linux host enabled 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.

☐ Network server time synchronized

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

☐ compat-libstdc++ RPM

If the compat-libstdc++ RPM is not present on your host machine, install it. This RPM contains libstdc++-libc6.1-1.so.2.

☐ compat

If the compat RPM is not present on your machine, install it. This RPM contains libncurses.so.4.

☐ For YaST based installation:

- ♦ Install the java2 jre package. This contains libjava.so and libjvm.so.

☐ (Conditional) 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.

☐ (Conditional) (to verify) If you are installing a secondary server into an existing tree as a nonadministrator user, ensure that you have the following rights:

- ♦ Supervisor rights to the container the server is being installed into.
- ♦ Supervisor rights to the partition where you want to add the server.

NOTE: This is required for adding the replica when the replica count is less than 3.

- ♦ All Attributes rights: read, compare, and write rights over the W0.KAP.Security object.

- ♦ Entry rights: browse rights over Security container object.
- ♦ All Attributes rights: read and compare rights over Security container object.

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 8.8 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

If you have eDirectory 8.5.x or 8.6.x, you have to first upgrade to eDirectory 8.7x and then upgrade to eDirectory 8.8

To upgrade to eDirectory 8.8 enter the following:

```
./nds-install
```

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

After the upgrade to eDirectory 8.8, the default location of the configuration files, data files, and log files are changed to /etc/opt/novell/eDirectory/conf, /var/opt/novell/eDirectory/data, and /var/opt/novell/eDirectory/log respectively.

The new directory /var/opt/novell/eDirectory/data uses a symbolic link to the /var/nds directory.

The old configuration file /etc/nds.conf is migrated to /etc/opt/novell/eDirectory/conf directory. The old configuration file /etc/nds.conf and the old log files under /var/nds are retained for reference.

Upgrading Through ZENworks Linux Management

eDirectory 8.8 on Linux leverages ZENworks® Linux Management to provide easy upgrade distribution and deployment. For more information on ZENworks Linux Management, refer to ZENworks Linux Management (<http://www.novell.com/products/zenworks/linuxmanagement/index.html>).

To upgrade through ZENworks Linux Management, complete the following steps:

1 Stop the server

2 Upgrade the packages

As the eDirectory 8.8 package names have changed, the package names will not appear in the Updates list. You have to manually select the updated packages from the Available Software list using any of the following methods:

- ♦ The Redcarpet administrator can create a single package set with all eDirectory 8.8 packages and the you can use them to upgrade to eDirectory 8.8.
- ♦ You can individually select the packages and install them.

3 Export the paths

4 Run ndsconfig upgrade

If you want to use ZENworks Linux Management server to upgrade from eDirectory 8.7.3 to eDirectory 8.8 on multiple machines, put Step 1 into a pre-transaction script and Step 3 and Step 4 into a post-transaction script.

NOTE: You can upgrade only from eDirectory 8.7.3 IR5 onwards.

For more information on transactions, refer to the Ximian Desktop Website (<http://www.ximian.com/products/redcarpet>).

You can apply eDirectory patches in the same way as normal upgrade. Follow the above steps. However, all the packages will not be present. Additionally, the specific steps to be followed during applying a patch would be given during the release of a patch.

Installing eDirectory

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

- ♦ “Server Health Checks” on page 27
- ♦ “Using SLP with eDirectory” on page 27
- ♦ “Installing NICT” on page 29

- ♦ “Using the nds-install Utility to Install eDirectory Components” on page 30
- ♦ “Nonroot User Installing eDirectory 8.8” on page 32
- ♦ “Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server” on page 34
- ♦ “Using ndsconfig to Configure Multiple Instances of eDirectory 8.8” on page 37
- ♦ “Using ndsconfig to Install a Linux Server into a Tree with Dotted Name Containers” on page 41
- ♦ “Using YaST to Install and Configure eDirectory 8.8” on page 42
- ♦ “Using the nmasinst Utility to Configure NMA” on page 44

Server Health Checks

With eDirectory 8.8, when you upgrade eDirectory, two server health checks are conducted by default to ensure that the server is safe for the upgrade:

- ♦ “Basic Server Health” on page 110
- ♦ “Partitions and Replica Health” on page 110

Based on the results obtained from the health checks, the upgrade will either continue or exit as follows:

- ♦ If all the health checks are successful, the upgrade will continue.
- ♦ If there are minor errors, the upgrade will prompt you to continue or exit.
- ♦ If there are critical errors, the upgrade will exit.

See Appendix B, “Server Health Checks,” on page 109 for a list of minor and critical error conditions.

Skipping Server Health Checks

To skip server health checks, use `nds-install -j` or `ndsconfig upgrade -j`.

For more information, see Appendix B, “Server Health Checks,” on page 109.

Using SLP with eDirectory

In earlier releases of eDirectory, SLP was installed during the eDirectory install. But with eDirectory 8.8, you need to separately install SLP before proceeding with the eDirectory install.

If you plan to use SLP to resolve tree names, it should have been properly installed and configured and the SLP DAs should be stable.

- 1** Install SLP by entering the following:

```
rpm -ivh SLP_rpm_file_name_with_path
```

The SLP RPM is present in the setup directory in the build. For example, if you have the build in the /home/build directory, enter the following command:

```
rpm -ivh /home/build/Linux/Linux/setup/novell-NDSSlp-8.8-20i386.rpm
```

- 2** Follow the onscreen instructions to complete the SLP installation.
- 3** Start SLP manually as follows:

```
/etc/init.d/slpuasa start
```

Similarly, when you uninstall the SLP package, you need to stop SLP manually, as follows:

```
/etc/init.d/slpuasa stop
```

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 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. In the `hosts.nds` file, for each tree or server, a single line contains the following information:

- ◆ Tree/Server Name: Tree names end with a trailing dot (.).
- ◆ Internet Address: This can be a DNS name or IP address.
- ◆ Server Port: Optional, appended with a colon (:) to the Internet address.

The syntax followed in the `hosts.nds` file is as follows:

```
<[partition name.]tree name>. <host-name/ip-addr>[:<port>]
<server name> <dns-addr/ip-addr>[:<port>]
```

For example:

```
# This is an example of a hosts.nds file:
# Tree name
Internet address
CORPORATE.
myserver.mycompany.com
novell.CORPORATE.
164.99.154.24:524

# Server name
Internet address
CORPSERVER
myserver.mycompany.com
```

See the `hosts.nds` man page for more details.

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 example, to search for the services whose `svcname-ws` attribute match with the value `SAMPLE_TREE`, enter the following command:

```
/usr/bin/slpinfo -s "ndap.novell///(svcname-ws==SAMPLE_TREE)/"
```

If you have a service registered with its `svcname-ws` attribute as `SAMPLE_TREE`, then the output will be similar to the following:

```
service:ndap.novell:///SAMPLE_TREE
```

If you do not have a service registered with its `svcname-ws` attribute as `SAMPLE_TREE`, there will be no output.

For more information, see Appendix C, "Configuring OpenSLP for eDirectory," on page 115.

Installing NICI

NICI should be installed before you proceed with the eDirectory installation. Both root and nonroot users can install NICI.

Root User Installing NICI

To install NICI, complete the following procedure:

- 1 Enter the following command:

```
rpm -ivh nici_rpm_file_name_with_path
```

For example:

```
rpm -ivh nici-2.7.0-5.i386.rpm
```

- 2 Execute the following script:

```
/var/opt/novell/nici/set_server_mode
```

Nonroot User Installing NICI

Nonroot users can make use of the sudo utility to install NICI. Sudo (superuser do) allows a root user to give certain users the ability to run some commands as root. A root user can do this by editing the /etc/sudoers configuration file and adding appropriate entries in it.

For more information, refer to the sudo Website (<http://www.sudo.ws>).

WARNING: sudo enables you to give limited root permissions to nonroot users. Therefore, we strongly recommend you to understand the security implications before proceeding.

A root user needs to complete the following procedure to enable a nonroot user (for example, john) to install NICI:

- 1 Log in as root.
- 2 Edit the /etc/sudoers configuration file using the visudo command.

NOTE: There is no space between vi and sudo in the command.

Make an entry with the following information:

```
Username    hostname=(root) NOPASSWD: /bin/rpm
```

For example, to enable john to run /bin/rpm as root on the hostname lnx-2, type the following:

```
john        lnx-2=(root) NOPASSWD: /bin/rpm
```

A nonroot user (john in the example) needs to do the following to install NICI:

- 1 Log in as john and execute the following command:

```
sudo rpm -ivh nici_rpm_file_name_with_path
```

For example:

```
sudo rpm -ivh /88/Linux/Linux/setup/nici-2.7.0-5.i386.rpm
```

- 2 Execute the following script:

```
sudo /var/opt/novell/nici/set_server_mode
```

NICI gets installed in the server mode.

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 or the downloaded file for the Linux platform. The utility adds the required packages based on what components you choose to install.

IMPORTANT: If the ZENworks Linux Management client is installed and the daemon (rcd) is running, then before running nds-install, stop the daemon using `/etc/init.d/rcd stop`.

- 1 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] [--help] [-i] [-j] [-u]
```

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	<p>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.</p> <p>There are two components you can install: the eDirectory server and the eDirectory administration utilities.</p> <ul style="list-style-type: none"> ♦ To install the server, enter <code>-c server</code>. ♦ To install the administration utilities, enter <code>-c admutils</code>. <p>For example, to install Novell eDirectory Server packages, you would enter the following command:</p> <pre>./nds-install -c server</pre>
-h or --help	Displays help for nds-install.
-i	Prevents the nds-install script from invoking the ndsconfig upgrade if a DIB is detected at the time of the upgrade.
-j	Jumps or overrides the health check option before installing eDirectory. For more information about health checks, refer to Appendix B, "Server Health Checks," on page 109.
-u	<p>Specifies the option to use in an unattended install mode.</p> <p>For unattended install to proceed, you need to enter at least the -c option at the command line, or else the install will abort.</p>

- 2 When prompted, accept the license agreement.

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

- 3 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	novell-NDSbase novell-NDScommon novell-NDSmasv novell-NDSserv novell-NDSimon novell-NDSrepair novell-NDSdextrnt novell-NOVLsubag novell-NOVLsnmp novell-NOVLpkis novell-NOVLpkis novell-NOVLpkia novell-NOVLembox novell-NOVLimgnt novell-NOVLstlog novell-NOVLxis novell-NLDAPsdk novell-NLDAPbase novell-NOVLsas novell-NOVLntls novell-NOVLnmas	The eDirectory replica server is installed on the specified server.
Administration Utilities	novell-NOVLice novell-NDSbase novell-NLDAPbase novell-NLDAPsdk novell-NOVLpkia novell-NOVLxis novell-NOVLimgnt	The Novell Import Conversion Export and LDAP Tools administration utilities are installed on the specified workstation.

4 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, the mounted license diskette, or the current directory).

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

5 After the installation is complete, you need to update the following environment variables and export them. You can either do it manually or use a script.

♦ **Manually export the environment variables**

```
export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/opt/
novell/eDirectory/lib/nds-modules:/opt/novell/
lib:$LD_LIBRARY_PATH

export PATH=/opt/novell/eDirectory/bin:/opt/novell/
eDirectory/sbin:$PATH

export MANPATH=/opt/novell/man:/opt/novell/eDirectory/
man:$MANPATH

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/
locale:$TEXTDOMAINDIR
```

♦ **Use the ndspath script to export the environment variables**

If you do not want to export the paths manually, you can use the `/opt/novell/eDirectory/bin/ndspath` script as follows:

- ♦ Prefix the `ndspath` script to the utility and run the utility you want as follows:

```
/opt/novell/eDirectory/bin/ndspath utility_name_with_parameters
```

- ♦ Export the paths in the current shell as follows:

```
. /opt/novell/eDirectory/bin/ndspath
```

After entering the above command, run the utilities as you would normally do.

- ♦ Call the script in your profile, `bashrc`, or similar scripts. Therefore, whenever you log in or open a new shell, you can start using the utilities directly.

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 93.

For more information on the `nmasinst` utility, see “Using the nmasinst Utility to Configure NMAS” on page 44.

Nonroot User Installing eDirectory 8.8

A nonroot user can install eDirectory 8.8 using the tarball.

Prerequisites

- ☐ Ensure that NCI is installed.

For information on installing NCI, refer to “Installing NCI” on page 29.

- ☐ If you want to use SLP and SNMP, ensure that they are installed by the root user.
- ☐ Write rights to the directory where you want to install eDirectory.

If you are a nonadministrator user, ensure that you have the appropriate rights as mentioned in the “Prerequisites” on page 23 section.

Installing eDirectory

- 1** Go to the directory where you want to install eDirectory.

- 2** Untar the tar file as follows:

```
tar xvf /tar_file_name
```

The `etc`, `opt`, and `var` directories are created.

- 3** Export the paths as follows:

- ♦ **Manually export the environment variables**

```
export LD_LIBRARY_PATH=custom_location/opt/novell/
eDirectory/lib:custom_location/opt/novell/eDirectory/lib/
nds-modules:custom_location/opt/novell/lib:/opt/novell/
lib:/opt/novell/eDirectory/lib:$LD_LIBRARY_PATH
```



```
export PATH=custom_location/opt/novell/eDirectory/
bin:custom_location/opt/novell/eDirectory/sbin:/opt/
novell/eDirectory/bin:$PATH

export MANPATH=custom_location/opt/novell/
man:custom_location/opt/novell/eDirectory/man:$MANPATH

export TEXTDOMAINDIR=custom_location/opt/novell/
eDirectory/share/locale:$TEXTDOMAINDIR
```

- ◆ Use the `ndspath` script to export the environment variables

If you do not want to export the paths manually, you can use the `custom_location/opt/novell/eDirectory/bin/ndspath` script as follows:

- ◆ Prefix the `ndspath` script to the utility and run the utility you want as follows:

```
custom_location/opt/novell/eDirectory/bin/ndspath
utility_name_with_parameters
```

- ◆ Go to the `custom_location/opt/novell/eDirectory/bin/` directory and export the paths in the current shell as follows:

```
. custom_location/opt/novell/eDirectory/bin/ndspath
```

NOTE: Ensure that you enter the above command from the `custom_location/opt` directory.

After entering the above command, run the utilities as you would normally do.

- ◆ Call the script in your profile, `bashrc`, or similar scripts. Therefore, whenever you log in or open a new shell, you can start using the utilities directly.

4 Configure eDirectory in the usual manner.

You can configure eDirectory in any of the following ways:

- ◆ Use the `ndsconfig` utility as follows:

```
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] [-b port_to_bind] [-B
interface1@port1, interface2@port2,...] [-D custom_location] [--
config-file configuration_file]
```

For example:

```
ndsconfig new -t mary-tree -n novell -a admin.novell -S linux1 -d /
home/mary/inst1/data -b 1025 -L 1026 -l 1027 -o 1028 -O 1029 -D /home/
mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

The port numbers you enter need to be in the range 1024 to 65535. Port numbers lesser than 1024 are normally reserved for the super-user and standard applications. Therefore, you cannot assume the default port 524 for any eDirectory applications.

This might cause the following applications to break:

- ◆ The applications that don't have an option to specify the target server port.
- ◆ The older applications that use NCP, and run as root for 524.
- ◆ Use the `ndsmanage` utility to configure a new instance. For more information, refer to the "Creating an Instance through `ndsmanage`" on page 38.

Follow the onscreen instructions to complete the configuration.

For more information, see “Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server” on page 34

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 93.

Prerequisite for Configuring eDirectory in a Specific Locale

If you want to configure eDirectory in a specific locale, you need to export LC_ALL and LANG to that particular locale before eDirectory configuration. For example, to configure eDirectory in the Japanese locale, enter the following:

```
export LC_ALL=ja
export LANG=ja
```

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] [-b port to bind] [-B interface1@port1, interface2@port2,...]
[-D custom_location] [--config-file configuration_file]
```

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
- ♦ *admin FDN*: 64 characters
- ♦ *server context*: 64 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] [-D custom_location] [--config-file configuration_file]
```

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:port] [-m module] [-b port to bind] [-B interface1@port1,
interface2@port2,..] [-D custom_location] [--config-file configuration_file]
[-E]
```

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 -s srv1
```

You can enable encrypted replication in the server you want to add using the -E option. For more information on encrypted replication, refer to *Novell eDirectory 8.8 Administration Guide* (<http://www.novell.com/documentation/edir88/index.html>).

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> .

ndsconfig Parameter	Description
-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/opt/novell/eDirectory/conf/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/opt/novell/eDirectory/conf/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 and port number of a server hosting the tree. If this option is used, SLP is not used for tree lookup. Use the -b <i>port_number</i> option along with -p.
-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, SNMP services, and SecretStore (ss) using the add command. If the module name is not specified, by default, all the modules are installed.
-o	Specifies the HTTP clear port number.
-O	Specifies the HTTP secure port number.
-E	Enables encrypted replication on the server you want to add. For more information on encrypted replication, refer to <i>Novell eDirectory 8.8 Administration Guide</i> (http://www.novell.com/documentation/edir88/index.html).
-j	Jumps or overrides the health check option before installing eDirectory.
-b	Sets the port number that a particular instance should listen on.
-B	Specifies the port number along with the IP address or interface. For example: -B eth0@524 or -B 100.1.1.2@524 NOTE: -b and -B are mutually exclusive.
--config-file	Specifies the absolute path and filename to store the nds.conf configuration file. For example, to store the configuration file in the /etc/opt/novell/eDirectory/ directory, you would specify --config-file /etc/opt/novell/eDirectory/nds.conf.
-D	Creates the data, dib, and log directories in the path mentioned.
set	Sets the value for the specified eDirectory configurable parameters. If the parameter list is not specified, ndsconfig lists all the eDirectory configurable parameters.

ndsconfig Parameter	Description
get	Displays the current value of the eDirectory configurable parameters.
get help	Displays the help strings for the eDirectory configurable parameters.

Using ndsconfig to Configure Multiple Instances of eDirectory 8.8

You can configure multiple instances of eDirectory 8.8 on a single host. For conceptual information on multiple instances, see *Multiple Instance Support in the Novell eDirectory 8.8 What's New Guide* (<http://www.novell.com/documentation/edir88/edir88new/data/bqebx8t.html>).

The method to configure multiple instance is similar to configuring a single instance multiple times. Each instance should have unique instance identifiers, such as the following:

- ◆ Different data and log file location
You can use the ndsconfig --config-file, -d, and -D options to do this.
- ◆ Unique portnumber for the instance to listen to
You can use the ndsconfig -b and -B options to do this.

NOTE: All the instances share the same server key (NICI).

You can also create a new instance using the ndsmanage utility. For more information, see “Creating an Instance through ndsmanage” on page 38.

To list all the instances on a specific host and do other operations on them, you can use the ndsmanage utility.

This sections explains the following:

- ◆ “The ndsmanage Utility” on page 37
- ◆ “Listing the Instances” on page 38
- ◆ “Creating an Instance through ndsmanage” on page 38
- ◆ “Performing Operations for a Specific Instance” on page 38

The ndsmanage Utility

The ndsmanage utility enables you to do the following:

- ◆ List the instances configured
- ◆ Create a new instance
- ◆ Do the following for a selected instance:
 - ◆ List the replicas on the server
 - ◆ Start the instance
 - ◆ Stop the instance
 - ◆ Run ndstrace for the instance
 - ◆ Deconfigure the instance
- ◆ Start and Stop all instances

Listing the Instances

The following table describes how to list the eDirectory instances.

Table 1 ndsmanage Usage for Listing the Instances

Syntax	Description
ndsmanage	Lists all the instances configured by you.
ndsmanage -a --all	List instances of all the users who are using a particular installation of eDirectory.
ndsmanage <i>username</i>	List the instances configured by a specific user

The following fields are displayed for every instance:

- ♦ Configuration file path
- ♦ Server FDN and port
- ♦ Status (whether the instance is active or inactive)

NOTE: This utility lists all the instances configured for a single binary.

Refer to Figure 6, “ndsmanage Utility Output Screen,” on page 38 for more information.

Creating an Instance through ndsmanage

To create a new instance through ndsmanage:

- 1** Enter the following command:

```
ndsmanage
```

If you have two instances configured, the following screen is displayed:

Figure 6 ndsmanage Utility Output Screen

```

root@MYSOL-8 / $ ndsmanage

The following are the instances configured by root

[1] /etc/opt/novell/eDirectory/conf/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@524 : ACTIVE

[2] /builds/server2/eDirectory/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@1525 : ACTIVE

Enter [1 - 2] for more options, [c] for creating a new instance or [q] to quit:

```

- 2** Enter c to create a new instance.

You can either create a new tree or add a server to an existing tree. Follow the instructions on the screen to create a new instance.

Performing Operations for a Specific Instance

You can perform the following operations for every instance:

- ♦ “Starting a Specific Instance” on page 39
- ♦ “Stopping a Specific Instance” on page 39
- ♦ “Deconfiguring an Instance” on page 40

Other than the ones listed above, you can also run `ndstrace` for a selected instance.

Starting a Specific Instance

To start an instance configured by you, do the following:

- 1 Enter the following:

```
ndsmanage
```

- 2 Select the instance you want to start.

The menu expands to include the options you can perform on a specific instance.

Figure 7 ndsmanage Utility Output Screen with Instance Options

```
root@mysol-8 / $ ndsmanage root

The following are the instances configured by root

[1] /etc/opt/novell/eDirectory/conf/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@524 : ACTIVE

[2] /builds/server2/eDirectory/nds.conf : .MYSOL-8.NOVELL.88SOL. : 164.99.148.175
@1525 : ACTIVE

Enter [1 - 2] for more options, [c] for creating a new instance or [q] to quit: 1
[1] List the replicas on the server
[s] Start the instance
[k] Stop the instance
[t] Run ndstrace
[d] Deconfigure
[q] Quit
What do you want to do with this instance? [ Choose from above]:
```

- 3 Enter **s** to start the instance.

Alternatively, you can also enter the following at the command prompt:

```
ndsmanage start --config-file  
configuration_file_of_the_instance_configured_by_you
```

Stopping a Specific Instance

To stop an instance configured by you, do the following:

- 1 Enter the following:

```
ndsmanage
```

- 2 Select the instance you want to stop.

The menu expands to include the options you can perform on a specific instance. For more information, refer to *ndsmanage Utility Output Screen with Instance Options* (page 39).

- 3 Enter **k** to stop the instance.

Alternatively, you can also enter the following at the command prompt:

```
ndsmanage stop --config-file
configuration_file_of_the_instance_configured_by_you
```

Deconfiguring an Instance

To deconfigure an instance, do the following:

- 1 Enter the following:

```
ndsmanage
```

- 2 Select the instance you want to deconfigure.

The menu expands to include the options you can perform on a specific instance. For more information, refer to *ndsmanage Utility Output Screen with Instance Options* (page 39).

- 3 Enter **d** to deconfigure the instance.

Starting and Stopping All Instances

You can start and stop all the instances configured by you.

Starting all the Instances

To start all the instances configured by you, enter the following at the command prompt:

```
ndsmanage startall
```

To start a specific instance, refer to “Starting a Specific Instance” on page 39.

Stopping All Instances

To stop all the instances configured by you, enter the following at the command prompt:

```
ndsmanage stopall
```

To stop a specific instance, refer to “Stopping a Specific Instance” on page 39.

Example

Mary wants to configure 2 trees on a single host machine.

Planning the Setup

Mary specifies the following instance identifiers.

♦ Instance 1:

Port number the instance should listen on	1524
Configuration file path	/home/maryinst1/nds.conf
DIB directory	/home/mary/inst1/var

♦ Instance 2:

Port number the instance should listen on	2524
Configuration file path	/home/mary/inst2/nds.conf

DIB directory

/home/mary/inst2/var

Configuring the Instances

To configure the instances based on the above mentioned instance identifiers, Mary must enter the following commands.

♦ Instance 1:

```
ndsconfig new -t mytree -n o=novell -a cn=admin.o=company -b 1524 -D
/home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

♦ Instance 2:

```
ndsconfig new -t corptree -n o=novell -a cn=admin.o=company -b 2524 -D
/home/mary/inst2/var --config-file /home/mary/inst2/nds.conf
```

Invoking a Utility for an Instance

If Mary wants to run the `ndstrace` utility for instance 1 that is listening on port 1524, with its configuration file in `/home/mary/inst1/nds.conf` location and its DIB file located in `/home/mary/inst1/var`, then she can run the utility as follows:

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

or

```
ndstrace -h 164.99.146.109:1524
```

If Mary does not specify the instance identifiers, the utility displays all the instances owned by Mary and prompts her to select an instance.

Listing the Instances

If Mary wants to know details about the instances in the host, she can run the `ndsmanage` utility.

♦ To display all instances owned by Mary:

```
ndsmanage
```

♦ To display all instances owned by John (username is john):

```
ndsmanage john
```

♦ To display all instances of all users that are using a particular installation of eDirectory:

```
ndsmanage -a
```

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, ndsmmerge, ndslogin, and ldapconfig.

Using YaST to Install and Configure eDirectory 8.8

YaST is the management foundation of SUSE LINUX. It makes installing on SUSE Linux easy. You can use YaST to upgrade, install, and configure eDirectory 8.8.

- ♦ “Upgrading to eDirectory 8.8” on page 42
- ♦ “Installing eDirectory 8.8” on page 43
- ♦ “Configuring eDirectory 8.8” on page 43

Upgrading to eDirectory 8.8

You can upgrade eDirectory 8.7.3 to eDirectory 8.8 from Open Enterprise Server (OES) only.

NOTE: You can upgrade only from eDirectory 8.7.3 IR5 onwards.

To upgrade to eDirectory 8.8, complete the following steps:

- 1** Stop the eDirectory 8.7.3 server as follows:

```
/etc/init.d/ndsctl stop
```

- 2** Download and untar the YaST build. (download from where?)
- 3** Start the YaST Control Center from the SUSE menu (SystemYaST).
The YaST Control Center screen is displayed.

- 4** Click on the Software option present in the left pane.
The options are displayed in the right pane.

- 5** Select Change Source of Installation.
The Software Source Media screen is displayed.

- 6** Select the location where the eDirectory installation files are present.

- 7** Click on Finish to return to the YaST Control Center screen.

- 8** Click the Install and Remove Software option on the right pane of the YaST Control Center screen.

- 9** Change the Filters to Selections in the Filters pane, located on the left.

The Selection list in the Filters pane gets populated with the available program packages. The packages already installed on the system are preselected.

- 10** Select Novell eDirectory and click on Accept.

The packages get installed in the default location.

During the upgrade, you might get the following warning for dependency conflict:

```
NOVLpkia 2.7.6-2 Conflict
NOVLpkis 2.7.6-2 Conflict
NOVLpkit 2.7.6-2 Conflict
```

To resolve this error, select Do not set NOVLpkia to protected and click Ok, try again. Similarly, do it for NOVLpkis and NOVLpkit.

Installing eDirectory 8.8

You can install eDirectory 8.8 on SLES 9 and above.

Before proceeding with the installation, ensure that OpenSLP is present on your system. Complete the following procedure to install eDirectory 8.8:

1 Download and untar the YaST build. (download from where?)

2 Start the YaST Control Center from the SUSE menu (SystemYaST).

The YaST Control Center screen is displayed.

3 Click on the Software option present in the left pane.

The options are displayed in the right pane.

4 Select Change Source of Installation.

The Software Source Media screen is displayed.

5 Select the location where the eDirectory installation files are present.

6 Click on Finish to return to the YaST Control Center screen.

7 Click the Install and Remove Software option on the right pane of the YaST Control Center screen.

8 Change the Filters to Selections in the Filters pane, located on the left.

The Selection list in the Filters pane gets populated with the available program packages. The packages already installed on the system are preselected.

9 Select Novell eDirectory and click on Accept.

The packages get installed in the default location.

You can refer to the online help for more information.

Configuring eDirectory 8.8

After installing eDirectory 8.8, to configure the eDirectory 8.8 server, complete the following procedure:

1 Click on Network Services in the YaST Control Center screen.

2 Select Novell eDirectory.

This invokes the eDirectory configuration.

3 Select Create Instance.

4 Create the new instance in a new or existing tree.

To create the instance for a new tree do the following:

4a Select New Tree

4b Enter the name of the tree

4c Click Next

The eDirectory Configuration - New Tree Information screen is displayed.

4d Enter the admin name with context.

For example, cn=admin.o=novell

4e Enter the password and confirm it.

4f Click Next

The eDirectory Configuration - Instance Information screen is displayed.

To add the instance to an existing tree, do the following:

4g Select Existing Tree.

4h Enter the name of the existing tree.

4i Click Next.

The eDirectory Configuration - Existing Tree Information screen is displayed.

4j Enter the hostname along with the NCP and secure LDAP port numbers.

4k Enter the admin FDN.

For example, cn=admin.o=novell

4l Enter the password.

4m Click Next

The eDirectory Configuration - Instance Information screen is displayed.

5 Enter the instance details, such as, server context, server name, instance, dib, and configuration locations.

6 Specify the NTP and SLP settings.

Using the nmasinst Utility to Configure NMAS

From eDirectory 8.7.3 onwards, by default, ndsconfig configures NMAS. You can also use nmasinst on Linux, Solaris, AIX, and HP-UX 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 44
- ♦ “Installing Login Methods” on page 45

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/beta/nmas30/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™ 8.8 on a Solaris* server:

- ♦ “System Requirements” on page 47
- ♦ “Prerequisites” on page 47
- ♦ “Hardware Requirements” on page 48
- ♦ “Forcing the Backlink Process to Run” on page 49
- ♦ “Upgrading eDirectory” on page 49
- ♦ “Installing eDirectory” on page 50

System Requirements

- ☐ One of the following:
 - ♦ Solaris 10 on Sun SPARC
 - ♦ Solaris 9 on Sun SPARC (with patch 108827-20 or later)
- ☐ All latest recommended set of patches available on the SunSolve* Web page (<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

- ☐ (Conditional) NCI 2.7 and eDirectory 8.8 support key sizes up to 4096 bits. If you want to use a 4 KB key size, every server must be upgraded to eDirectory 8.8. In addition, every workstation using the management utilities, for example, iManager and ConsoleOne, must have NCI 2.7 installed on it.

When you upgrade your Certificate Authority (CA) server to eDirectory 8.8, the key size will not change; it will be 2 KB. The only way to create a 4 KB key size is recreate the CA on an eDirectory 8.8 server. In addition, you would have to change the default from 2 KB to 4 KB for the key size, during the CA creation.

The package containing NCI 2.7 is named NOVLniu0-2.7 on Solaris.

For more information, refer to “Installing NCI” on page 51.

- ❑ SLP should be installed and configured.

With eDirectory 8.8, SLP does not get installed as part of the eDirectory installation.

If you are a root user, you need to install and configure SLP before proceeding with the eDirectory installation.

If you are a nonroot user, SLP should be installed and configured before you proceed with the eDirectory installation. A nonroot user cannot install SLP.

For more information on installing SLP, refer to “Using SLP with eDirectory” on page 50.

- ❑ The NCI Foundation Key (NFK) file
- ❑ Enable the Solaris 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 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
```

- ❑ 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, AIX, or HP-UX systems with NetWare® servers, use timesync.nlm 5.09 or later.

- ❑ (Conditional) 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.
- ❑ (Conditional) (to verify) If you are installing a secondary server into an existing tree as a nonadministrator user, ensure that you have the following rights:
 - ♦ Supervisor rights to the container the server is being installed into.
 - ♦ Supervisor rights to the partition where you want to add the server.

NOTE: This is required for adding the replica when the replica count is less than 3.
 - ♦ All Attributes rights: read, compare, and write rights over the W0.KAP.Security object.
 - ♦ Entry rights: browse rights over Security container object.
 - ♦ All Attributes rights: read and compare rights over Security container object.

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 8.8 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

If you have eDirectory 8.5.x or 8.6.x, you have to first upgrade to eDirectory 8.7x and then upgrade to eDirectory 8.8

./nds-install

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

After the upgrade to eDirectory 8.8, the default location of the configuration files, data files, and log files are changed to `/etc/opt/novell/eDirectory/conf`, `/var/opt/novell/eDirectory/data`, and `/var/opt/novell/eDirectory/log` respectively.

The new directory `/var/opt/novell/eDirectory/data` uses a symbolic link to the `/var/nds` directory.

The old configuration file `/etc/nds.conf` is migrated to `/etc/opt/novell/eDirectory/conf` directory. The old configuration file `/etc/nds.conf` and the old log files under `/var/nds` are retained for reference.

Installing eDirectory

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

- ♦ “Server Health Checks” on page 50
- ♦ “Using SLP with eDirectory” on page 50
- ♦ “Installing NICT” on page 51
- ♦ “Using the Nds-install Utility to Install eDirectory Components” on page 52
- ♦ “Nonroot User Installing eDirectory 8.8” on page 55
- ♦ “Using the Ndsconfig Utility to Add or Remove the eDirectory Replica Server” on page 57
- ♦ “Using ndsconfig to Configure Multiple Instances of eDirectory 8.8” on page 60
- ♦ “Using Ndsconfig to Install a Solaris Server into a Tree with Dotted Name Containers” on page 60
- ♦ “Using the Nmasinst Utility to Configure NMAS” on page 60

Server Health Checks

With eDirectory 8.8, when you upgrade or install eDirectory, two server health checks are conducted by default to ensure that the server is safe for the upgrade.

- ♦ “Basic Server Health” on page 110
- ♦ “Partitions and Replica Health” on page 110

Based on the results obtained from the health checks, the upgrade will either continue or exit as follows:

- ♦ If all the health checks are successful, the upgrade will continue.
- ♦ If there are minor errors, the upgrade will prompt you to continue or exit.
- ♦ If there are critical errors, the upgrade will exit.

See Appendix B, “Server Health Checks,” on page 109 for a list of minor and critical error conditions.

Skipping Server Health Checks

To skip server health checks, use `nds-install -j` or `ndsconfig upgrade -j`.

For more information, see Appendix B, “Server Health Checks,” on page 109.

Using SLP with eDirectory

In earlier releases of eDirectory, SLP was installed during the eDirectory install. But with eDirectory 8.8, you need to separately install SLP before proceeding with the eDirectory install.

If you plan to use SLP to resolve tree names, it should have been properly configured and SLP DAs should be stable.

- 1 To install SLP, enter the following:

```
pkgadd -d filename_and_absolute_path_of_NDSslp.pkg
```

The SLP package is present in the setup directory in the build. For example, if you have the build in the /home/build directory, enter the following command:

```
pkgadd -d /home/build/Solaris/Solaris/setup/NDSSslp.pkg
```

2 Follow the onscreen instructions to complete SLP installation.

3 Start SLP.

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. For more information on hosts.nds, refer to "Using SLP with eDirectory" on page 27 and the hosts.nds manpage.

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 example, to search for the services whose svcname-ws attribute match with the value SAMPLE_TREE, enter the following command:

```
/usr/bin/slpinfo -s "ndap.novell///(svcname-ws==SAMPLE_TREE)/"
```

If you have a service registered with its svcname-ws attribute as SAMPLE_TREE, then the output will be similar to the following:

```
service:ndap.novell:///SAMPLE_TREE
```

If you do not have a service registered with its svcname-ws attribute as SAMPLE_TREE, there will be no output.

For more information, see Appendix C, "Configuring OpenSLP for eDirectory," on page 115.

Installing NCI

NCI should be installed before you proceed with the eDirectory installation. Both root and nonroot users can install NCI, though the procedure to do so is different.

Root User Installing NCI

To install NCI, complete the following procedure:

1 Enter the following command:

```
pkgadd -d NCI_package_absolute_path_and_filename NOVLniu0
```

For example:

```
pkgadd -d /home/build/Solaris/Solaris/setup/NOVLniu0.pkg  
NOVLniu0
```

2 Execute the following script:

```
/var/opt/novell/nci/set_server_mode
```

Nonroot User Installing NCI

Nonroot users can make use of the sudo utility to install NCI. Sudo (superuser do) allows a root user to give certain users the ability to run some commands as root. A root user can do this by editing the /etc/sudoers configuration file and adding appropriate entries in it.

For more information, refer to the sudo Website (<http://www.sudo.ws>).

WARNING: sudo enables you to give limited root permissions to nonroot users. Therefore, we strongly recommend you to understand the security implications before proceeding.

A root user needs to complete the following procedure to enable a nonroot user (for example, john) to install NCI:

- 1 Log in as root.
- 2 Edit the /etc/sudoers configuration file using the visudo command.

NOTE: There is no space between vi and sudo in the command.

Make an entry with the following information:

```
Username    hostname=(root) NOPASSWD: /usr/sbin/pkgadd
```

For example, to enable john to run /usr/sbin/pkgadd as root on the hostname sol-2, type the following:

```
john       sol-2=(root) NOPASSWD: /usr/sbin/pkgadd
```

A nonroot user (john in the example) needs to do the following to install NCI:

- 1 Log in as john and execute the following command:

```
sudo pkgadd -d absolute_path_of_the_NCI_package NOVLniu0
```

For example:

```
sudo pkgadd -d /home/build/Solaris/Solaris/setup/NOVLniu0.pkg  
NOVLniu0
```

- 2 Execute the following script:

```
sudo /var/opt/novell/nici/set_server_mode
```

NCI gets installed in the server mode.

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.

A nonroot user can install using only tarballs. For more information, refer to “Nonroot User Installing eDirectory 8.8” on page 55.

- 1 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] [-i] [-j] [-u]
```

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	<p>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.</p> <p>There are two components you can install, the eDirectory server and the eDirectory administration utilities. To install the server, enter -c nds. To install the administration utilities, enter -c adminutils.</p> <p>For example, to install Novell eDirectory Server packages, you would enter the following command:</p> <pre>./nds-install -c server -n /var</pre>
-h	Displays help for nds-install.
-i	Prevents the nds-install script from invoking ndsconfig upgrade if a DIB is detected at the time of the upgrade.
-j	Jumps or overrides the health check option before installing eDirectory. For more information about health checks, refer to Appendix B, "Server Health Checks," on page 109.
-u	Specifies the option to use an unattended install mode.

2 When prompted, accept the license agreement.

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

3 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 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.

4 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, the 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. 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 93.

For more information on the nmasinst utility, see “Using the Nmasinst Utility to Configure NMASTM” on page 60.

5 After the installation is complete, you need to update the following environment variables and export them as follows:

- ♦ **Manually export the environment variables**

```
export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/opt/
novell/eDirectory/lib/nds-modules:/opt/novell/
lib:$LD_LIBRARY_PATH

export PATH=/opt/novell/eDirectory/bin:/opt/novell/
eDirectory/sbin:$PATH

export MANPATH=/opt/novell/man:/opt/novell/eDirectory/
man:$MANPATH

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/
locale:$TEXTDOMAINDIR
```

- ♦ **Use the ndspath script to export the environment variables**

If you do not want to export the paths manually, you can use the /opt/novell/eDirectory/bin/ndspath script as follows:

- ♦ Prefix the ndspath script to the utility and run the utility you want as follows:

```
/opt/novell/eDirectory/bin/ndspath utility_name_with_parameters
```

- ♦ Export the paths in the current shell as follows:

```
. /opt/novell/eDirectory/bin/ndspath
```

After entering the above command, run the utilities as you would normally do.

- ♦ Call the script in your profile, bashrc, or similar scripts. Therefore, whenever you log in or open a new shell, you can start using the utilities directly.

Nonroot User Installing eDirectory 8.8

A nonroot user can install eDirectory 8.8 using the tarball.

Prerequisites

- ☐ Ensure that NCI is installed.

For information on installing NCI, refer to “Installing NCI” on page 51.

- ☐ If you want to use SLP and SNMP, ensure that they are installed by the root user.
- ☐ Write rights to the directory where you want to install eDirectory.

If you are a nonadministrator user, ensure that you have the appropriate rights as mentioned in the “Prerequisites” on page 47 section.

Installing eDirectory

- 1** Go to the directory where you want to install eDirectory .
- 2** Untar the tar file as follows:

```
tar xvf /tar_file_name
```

- 3** Export the paths as follows:

- ♦ **Manually export the environment variables**

```
export LD_LIBRARY_PATH=custom_location/opt/novell/
eDirectory/lib:custom_location/opt/novell/eDirectory/lib/
nds-modules:custom_location/opt/novell/lib:/opt/novell/
lib:/opt/novell/eDirectory/lib:$LD_LIBRARY_PATH
```

```
export PATH=custom_location/opt/novell/eDirectory/
bin:custom_location/opt/novell/eDirectory/sbin:/opt/
novell/eDirectory/bin:$PATH

export MANPATH=custom_location/opt/novell/
man:custom_location/opt/novell/eDirectory/man:$MANPATH

export TEXTDOMAINDIR=custom_location/opt/novell/
eDirectory/share/locale:$TEXTDOMAINDIR
```

- ♦ Use the `ndspath` script to export the environment variables

If you do not want to export the paths manually, you can use the *custom_location*/opt/novell/eDirectory/bin/`ndspath` script as follows:

- ♦ Prefix the `ndspath` script to the utility and run the utility you want as follows:

```
custom_location/opt/novell/eDirectory/bin/ndspath
utility_name_with_parameters
```

- ♦ Go to the *custom_location*/opt/novell/eDirectory/bin/ directory and export the paths in the current shell as follows:

```
. custom_location/opt/novell/eDirectory/bin/ndspath
```

NOTE: Ensure that you enter the above command from the *custom_location*/opt directory.

After entering the above command, run the utilities as you would normally do.

- ♦ Call the script in your profile, `bashrc`, or similar scripts. Therefore, whenever you log in or open a new shell, you can start using the utilities directly.

4 Configure eDirectory in the usual manner.

You can configure eDirectory in any of the following ways:

- ♦ Use the `ndsconfig` utility as follows:

```
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] [-b port_to_bind] [-B
interface1@port1, interface2@port2,..] [-D custom_location] [--
config-file configuration_file]
```

For example:

```
ndsconfig new -t mary-tree -n novell -a admin.novell -S linux1 -d /
home/mary/inst1/data -b 1025 -L 1026 -l 1027 -o 1028 -O 1029 -D /home/
mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

The port numbers you enter need to be in the range 1024 to 65535. Port numbers lesser than 1024 are normally reserved for the super-user and standard applications. Therefore, you cannot assume the default port 524 for any eDirectory applications.

This might cause the following applications to break:

- ♦ The applications that don't have an option to specify the target server port.
- ♦ The older applications that use NCP, and are run as root for 524.
- ♦ Use the `ndsmanage` utility to configure a new instance. For more information, refer to the "Creating an Instance through `ndsmanage`" on page 38.

Follow the onscreen instructions to complete the configuration.

For more information, see “Using the Ndsconfig Utility to Add or Remove the eDirectory Replica Server” on page 57.

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 93.

Prerequisite for Configuring eDirectory in a Specific Locale

If you want to configure eDirectory in a specific locale, you need to export LC_ALL and LANG to that particular locale before eDirectory configuration. For example, to configure eDirectory in the Japanese locale, enter the following:

```
export LC_ALL=ja
export LANG=ja
```

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] [-b port to bind] [-B interface1@port1, interface2@port2,..]
[-D custom_location] [--config-file configuration_file]
```

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
- ♦ *admin FDN*: 64 characters
- ♦ *server context*: 64 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] [-D custom_location] [--config-file configuration_file]
```

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:port] [-m module] [-b port to bind] [-B interface1@port1,
interface2@port2,..] [-D custom_location] [--config-file configuration_file]
[-E]
```

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 -s srv1
```

You can enable encrypted replication in the server you want to add using the -E option. For more information on encrypted replication, refer to *Novell eDirectory 8.8 Administration Guide* (<http://www.novell.com/documentation/edir88/index.html>).

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> .

ndsconfig Parameter	Description
-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/opt/novell/eDirectory/conf/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/opt/novell/eDirectory/conf/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 and port number of a server hosting the tree. If this option is used, SLP is not used for tree lookup. Use the -b <i>port_number</i> option along with -p.
-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, SNMP services, and SecretStore (ss) using the add command. If the module name is not specified, by default, all the modules are installed.
-o	Specifies the HTTP clear port number.
-O	Specifies the HTTP secure port number.
-E	Enables encrypted replication on the server you want to add. For more information on encrypted replication, refer to <i>Novell eDirectory 8.8 Administration Guide</i> (http://www.novell.com/documentation/edir88/index.html).
-j	Jumps or overrides the health check option before installing eDirectory.
-b	Sets the port number on which a particular instance should listen on.
-B	Specify the port number along with the IP address or interface. For example, -B eth0@524 or -B 100.1.1.2@524 NOTE: -b and -B are mutually exclusive.

ndsconfig Parameter	Description
--config-file	Saves the nds.conf configuration file in the path mentioned.
-D	Creates the data, dib and log directories in the path mentioned.
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 Configure Multiple Instances of eDirectory 8.8

You can configure multiple instances of eDirectory 8.8 on a single host. For information on multiple instances, refer to “Using ndsconfig to Configure Multiple Instances of eDirectory 8.8” on page 37 in the Linux chapter.

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 8.8, by default, ndsconfig configures NMAS. You can also use nmasinst on Linux, Solaris, AIX, and HP-UX 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 61
- ◆ “Installing Login Methods” on page 61

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/beta/nmas30/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™ 8.8 on an AIX* server:

- ♦ “System Requirements” on page 63
- ♦ “Prerequisites” on page 63
- ♦ “Hardware Requirements” on page 64
- ♦ “Forcing the Backlink Process to Run” on page 65
- ♦ “Upgrading eDirectory” on page 65
- ♦ “Installing eDirectory” on page 65

System Requirements

- ☐ AIX 5L Version 5.2
- ☐ All recommended AIX OS patches, available at the IBM* Tech Support (<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 `mROUTED` is running.
If it is not running, configure and start the multicast daemon `mROUTED`.
See the “`mROUTED.conf` File” section in the *Files Reference* book in AIX Documentation (http://www16.boulder.ibm.com/pseries/en_US/infocenter/base/aix.htm) for an example configuration file.
- ☐ (Conditional) NCI 2.7 and eDirectory 8.8 support key sizes up to 4096 bits. If you want to use a 4 KB key size, every server must be upgraded to eDirectory 8.8. In addition, every workstation using the management utilities, for example, iManager and ConsoleOne, must have NCI 2.7 installed on it.

When you upgrade your Certificate Authority (CA) server to eDirectory 8.8, the key size will not change; it will be 2 KB. The only way to create a 4 KB key size is recreate the CA on an eDirectory 8.8 server. In addition, you would have to change the default from 2 KB to 4 KB for the key size, during the CA creation.

The package containing NCI 2.7 is named NOVLniu0-2.7 on AIX. For more information, refer to “Installing NCI” on page 67.

- ☐ The NCI Foundation Key (NFK) file
- ☐ 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, AIX, or HP-UX systems with NetWare® servers, use timesync.nlm 5.09 or later.

- ☐ (Conditional) 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.
- ☐ (Conditional) (to verify) If you are installing a secondary server into an existing tree as a nonadministrator user, ensure that you have the following rights:
 - ♦ Supervisor rights to the container the server is being installed into.
 - ♦ Supervisor rights to the partition where you want to add the server.
 - NOTE:** This is required for adding the replica when the replica count is less than 3.
 - ♦ All Attributes rights: read, compare, and write rights over the W0.KAP.Security object.
 - ♦ Entry rights: browse rights over Security container object.
 - ♦ All Attributes rights: read and compare rights over Security container object.

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 8.8 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 8.8 from eDirectory 8.7, 8.7.1, or 8.7.3 enter the following:

```
./nds-install
```

After the upgrade to eDirectory 8.8, the default location of the configuration files, data files, and log files are changed to `/etc/opt/novell/eDirectory/conf`, `/var/opt/novell/eDirectory/data`, and `/var/opt/novell/eDirectory/log` respectively.

The new directory `/var/opt/novell/eDirectory/data` uses a symbolic link to the `/var/nds` directory.

The old configuration file `/etc/nds.conf` is migrated to `/etc/opt/novell/eDirectory/conf` directory. The old configuration file `/etc/nds.conf` and the old log files under `/var/nds` are retained for reference.

Installing eDirectory

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

- ♦ “Server Health Checks” on page 66
- ♦ “Using SLP with eDirectory” on page 66
- ♦ “Installing NCI” on page 67
- ♦ “Using the Nds-install Utility to Install eDirectory Components” on page 68
- ♦ “Nonroot User Installing eDirectory 8.8” on page 70
- ♦ “Using the Ndsconfig Utility to Add or Remove the eDirectory Replica Server” on page 72
- ♦ “Using ndsconfig to Configure Multiple Instances of eDirectory 8.8” on page 75
- ♦ “Using Ndsconfig to Install an AIX Server into a Tree with Dotted Name Containers” on page 75

- ♦ “Using the Nmasinst Utility to Configure NMA” on page 75

Server Health Checks

With eDirectory 8.8, when you upgrade or install eDirectory, two server health checks are conducted by default to ensure that the server is safe for the upgrade.

- ♦ “Basic Server Health” on page 110
- ♦ “Partitions and Replica Health” on page 110

Based on the results obtained from the health checks, the upgrade will either continue or exit as follows:

- ♦ If all the health checks are successful, the upgrade will continue.
- ♦ If there are minor errors, the upgrade will prompt you to continue or exit.
- ♦ If there are critical errors, the upgrade will exit.

See Appendix B, “Server Health Checks,” on page 109 for a list of minor and critical error conditions.

Skiping Server Health Checks

To skip server health checks, use `nds-install -j` or `ndsconfig upgrade -j`.

For more information, see Appendix B, “Server Health Checks,” on page 109.

Using SLP with eDirectory

In earlier releases of eDirectory, SLP was installed during the eDirectory install. But with eDirectory 8.8, you need to separately install SLP before proceeding with the eDirectory install.

If you plan to use SLP to resolve tree names, it should have been properly configured and SLP DAs should be stable.

- 1 Install SLP using the following command:

```
installp -acgXd absolute_path_of_NDSslp_fileset NDS.NDSslp
```

The SLP fileset is present in the setup directory in the build. For example, if you have the build in the /home/build directory, enter the following command:

```
installp -acgXd /home/build/Aix/Aix/setup/NDS.NDSslp
```

- 2 Follow the onscreen instructions to complete the SLP installation.
- 3 Start SLP.

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. For more information on `hosts.nds`, refer to “Using SLP with eDirectory” on page 27 and the `hosts.nds` manpage.

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 example, to search for the services whose svcname-ws attribute match with the value SAMPLE_TREE, enter the following command:

```
/usr/bin/slpinfo -s "ndap.novell:/// (svcname-ws==SAMPLE_TREE) /"
```

If you have a service registered with its svcname-ws attribute as SAMPLE_TREE, then the output will be similar to the following:

```
service:ndap.novell:///SAMPLE_TREE
```

If you do not have a service registered with its svcname-ws attribute as SAMPLE_TREE, there will be no output.

For more information, see Appendix C, “Configuring OpenSLP for eDirectory,” on page 115.

Installing NICI

NICI should be installed before you proceed with the eDirectory installation. Both root and nonroot users can install NICI, though the procedure to do so is different.

Root User Installing NICI

To install NICI, complete the following procedure:

- 1 Enter the following command:

```
installp -acgXd absolute_path_of_the_NICI_fileset NOVLniu0
```

For example:

```
installp -acgXd /home/build/AIX/AIX/setup/NOVLniu0.2.7.0.0  
NOVLniu0
```

- 2 Execute the following script:

```
/var/opt/novell/nici/set_server_mode
```

Nonroot User Installing NICI

Nonroot users can make use of the sudo utility to install NICI. Sudo (superuser do) allows a root user to give certain users the ability to run some commands as root. A root user can do this by editing the /etc/sudoers configuration file and adding appropriate entries in it.

For more information, refer to the sudo Website (<http://www.sudo.ws>).

WARNING: sudo enables you to give limited root permissions to nonroot users. Therefore, we strongly recommend you to understand the security implications before proceeding.

A root user needs to complete the following procedure to enable a nonroot user (for example, john) to install NICI:

- 1 Log in as root.
- 2 Edit the /etc/sudoers configuration file using the visudo command.

NOTE: There is no space between vi and sudo in the command.

Make an entry with the following information:

```
Username    hostname=(root) NOPASSWD: /usr/sbin/installp
```

For example, to enable john to run /bin/rpm as root on the hostname aix-2, type the following:

```
john      aix-2=(root) NOPASSWD: /usr/sbin/installp
```

A nonroot user (john in the example) needs to do the following to install NICI:

- 1 Log in as john and execute the following command:

```
sudo installp -acgXd absolute_path_of_the_NICI_fileset
NOVLniu0
```

For example:

```
sudo installp -acgXd /home/build/AIX/AIX/setup/
NOVLniu0.2.7.0.0 NOVLniu0
```

- 2 Execute the following script:

```
sudo /var/opt/novell/nici/set_server_mode
```

NICI gets installed in the server mode.

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 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] [-i] [-j] [-u]
```

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	<p>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.</p> <p>There are two components you can install, the eDirectory server and the eDirectory administration utilities. To install the server, enter -c nds. To install the administration utilities, enter -c adminutils.</p> <p>For example, to install Novell eDirectory Server packages, you would enter the following command:</p> <pre>./nds-install -c server -n /var</pre>
-h	Displays help for nds-install.
-i	Prevents the nds-install script from invoking ndsconfig upgrade if a DIB is detected at the time of the upgrade.
-j	Jumps or overrides the health check option before installing eDirectory. For more information about health checks, refer to Appendix B, "Server Health Checks," on page 109.

nds-install Parameter	Description
-u	Specifies the option to use an unattended install mode.

2 When prompted, accept the license agreement.

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

3 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 NDSdexvnt NOVLsubag NOVLsnmp NOVLpkit NOVLpkis NOVLpkia NOVLebox 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.

4 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, the 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 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 93.

For more information on the nmasinst utility, see “Using the Nmasinst Utility to Configure NMAS” on page 75.

- 5 After the installation is complete, you need to update the following environment variables and export them as follows:

- ♦ **Manually export the environment variables**

```
export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/opt/
novell/eDirectory/lib/nds-modules:/opt/novell/lib:/opt/
novell/lib:/opt/novell/eDirectory/lib:$LD_LIBRARY_PATH

export LIBPATH=/opt/novell/eDirectory/lib:/opt/novell/
eDirectory/lib/nds-modules:/opt/novell/lib:/opt/novell/
lib:/opt/novell/eDirectory/lib:$LIBPATH

export PATH=/opt/novell/eDirectory/bin:/opt/novell/
eDirectory/sbin:$PATH

export MANPATH=/opt/novell/man:/opt/novell/eDirectory/
man:$MANPATH

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/
locale:$TEXTDOMAINDIR
```

- ♦ **Use the ndspath script to export the environment variables**

If you do not want to export the paths manually, you can use the /opt/novell/eDirectory/bin/ndspath script as follows:

- ♦ Prefix the ndspath script to the utility and run the utility you want as follows:

```
/opt/novell/eDirectory/bin/ndspath utility_name_with_parameters
```

- ♦ Export the paths in the current shell as follows:

```
. /opt/novell/eDirectory/bin/ndspath
```

After entering the above command, run the utilities as you would normally do.

- ♦ Call the script in your profile, bashrc, or similar scripts. Therefore, whenever you log in or open a new shell, you can start using the utilities directly.

Nonroot User Installing eDirectory 8.8

A nonroot user can install eDirectory 8.8 using the tarball.

Prerequisites

- ☐ Ensure that NCI is installed.

For information on installing NCI, refer to “Installing NCI” on page 67.

- ☐ If you want to use SLP and SNMP, ensure that they are installed by the root user.
- ☐ Write rights to the directory where you want to install eDirectory.

If you are a nonadministrator user, ensure that you have the appropriate rights as mentioned in the “Prerequisites” on page 63 section.

Installing eDirectory

- 1 Go to the directory where you want to install eDirectory.

- 2 Untar the tar file as follows:

```
tar xvpf /tar_file_name
```

- 3 Export the paths as follows:

- ♦ **Manually export the environment variables**

```
export LD_LIBRARY_PATH=custom_location/opt/novell/
eDirectory/lib:custom_location/opt/novell/eDirectory/lib/
nds-modules:custom_location/opt/novell/lib:/opt/novell/
lib:/opt/novell/eDirectory/lib:$LD_LIBRARY_PATH
```

```
export LIBPATH=custom_location/opt/novell/eDirectory/
lib:custom_location/opt/novell/eDirectory/lib/nds-
modules:custom_location/opt/novell/lib:/opt/novell/lib:/
opt/novell/eDirectory/lib:$LIBPATH
```

```
export PATH=custom_location/opt/novell/eDirectory/
bin:custom_location/opt/novell/eDirectory/sbin:/opt/
novell/eDirectory/bin:$PATH
```

```
export MANPATH=custom_location/opt/novell/
man:custom_location/opt/novell/eDirectory/man:$MANPATH
```

```
export TEXTDOMAINDIR=custom_location/opt/novell/
eDirectory/share/locale:$TEXTDOMAINDIR
```

- ♦ **Use the ndspath script to export the environment variables**

If you do not want to export the paths manually, you can use the *custom_location/opt/novell/eDirectory/bin/ndspath* script as follows:

- ♦ Prefix the ndspath script to the utility and run the utility you want as follows:

```
custom_location/opt/novell/eDirectory/bin/ndspath
utility_name_with_parameters
```

- ♦ Go to the *custom_location/opt/novell/eDirectory/bin/* directory and export the paths in the current shell as follows:

```
. custom_location/opt/novell/eDirectory/bin/ndspath
```

NOTE: Ensure that you enter the above command from the *custom_location/opt* directory.

After entering the above command, run the utilities as you would normally do.

- ♦ Call the script in your profile, bashrc, or similar scripts. Therefore, whenever you log in or open a new shell, you can start using the utilities directly.

- 4 Configure eDirectory in the usual manner.

You can configure eDirectory in any of the following ways:

- ♦ Use the ndsconfig utility as follows:

```
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 [-b port_to_bind] [-B
interface1@port1, interface2@port2,...] [-D custom_location] [--
config-file configuration_file]
```

For example:

```
ndsconfig new -t mary-tree -n novell -a admin.novell -S linux1 -d /
home/mary/inst1/data -b 1025 -L 1026 -l 1027 -o 1028 -O 1029 -D /home/
mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

The port numbers you enter need to be in the range 1024 to 65535. Port numbers lesser than 1024 are normally reserved for the super-user and standard applications. Therefore, you cannot assume the default port 524 for any eDirectory applications.

This might cause the following applications to break:

- ♦ The applications that don't have an option to specify the target server port.
- ♦ The older applications that use NCP, and are run as root for 524.
- ♦ Use the ndsmanage utility to configure a new instance. For more information, refer to the "Creating an Instance through ndsmanage" on page 38.

Follow the onscreen instructions to complete the configuration.

For more information, see "Using the Ndsconfig Utility to Add or Remove the eDirectory Replica Server" on page 72.

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 93.

Prerequisite for Configuring eDirectory in a Specific Locale

If you want to configure eDirectory in a specific locale, you need to export LC_ALL and LANG to that particular locale before eDirectory configuration. For example, to configure eDirectory in the Japanese locale, enter the following:

```
export LC_ALL=ja
export LANG=ja
```

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
- ♦ *admin FDN*: 64 characters
- ♦ *server context*: 64 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:port] [-m module] [-E]
```

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 -s srv1
```

You can enable encrypted replication in the server you want to add using the `-E` option. For more information on encrypted replication, refer to *Novell eDirectory 8.8 Administration Guide* (<http://www.novell.com/documentation/edir88/index.html>).

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/opt/novell/eDirectory/conf/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/opt/novell/eDirectory/conf/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 and port number of a server hosting the tree. If this option is used, SLP is not used for tree lookup. Use the <code>-b port_number</code> option along with <code>-p</code> .
-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, SNMP services, and SecretStore (ss) using the add command. If the module name is not specified, by default, all the modules are installed.
-o	Specifies the HTTP clear port number.
-O	Specifies the HTTP secure port number.
-E	Enables encrypted replication on the server you want to add. For more information on encrypted replication, refer to <i>Novell eDirectory 8.8 Administration Guide</i> (http://www.novell.com/documentation/edir88/index.html).

ndsconfig Parameter	Description
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 Configure Multiple Instances of eDirectory 8.8

You can configure multiple instances of eDirectory 8.8 on a single host. For information on multiple instances, refer to “Using ndsconfig to Configure Multiple Instances of eDirectory 8.8” on page 37 in the Linux chapter.

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 8.8, by default, ndsconfig configures NMAS. You can also use nmasinst on Linux, Solaris, AIX, and HP-UX 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 75
- ♦ “Installing Login Methods” on page 76

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/beta/nmas30/admin/data/a53vj9a.html>) in the *Novell Modular Authentication Service Administration Guide*.

6

Installing or Upgrading Novell eDirectory on HP-UX

Use the following information to install or upgrade Novell® eDirectory™ 8.8 on an HP-UX* server:

- ♦ “System Requirements” on page 77
- ♦ “Prerequisites” on page 77
- ♦ “Hardware Requirements” on page 78
- ♦ “Forcing the Backlink Process to Run” on page 79
- ♦ “Upgrading eDirectory” on page 79
- ♦ “Installing eDirectory” on page 80

System Requirements

☐ HP-UX 11i Operating System

Ensure that the OS is updated with the patch PHSS_26560. You can download this patch from the HP IT Resource Center (<http://www.itrc.hp.com>) > maintenance and support for HP products.

NOTE: If you have installed the patch PHSS_28436, we recommend that you uninstall it and install patch PHSS_26560.

- ☐ Ensure that the HP-UX 11i Quality Pack (GOLDQPK11i) is installed. Download and install it from HP Support Plus Quality Pack Bundles (http://www.software.hp.com/SUPPORT_PLUS/qpk.html#N0.110).
- ☐ PA-RISC 2.0 Processor
- ☐ 256 MB RAM minimum
- ☐ 300 MB of hard disk space
- ☐ Ensure that gettext is installed. You can download it from The HP-UX Porting and Archive Center (<http://hpux.connect.org.uk/hppd/hpux/Gnu>).
- ☐ Ensure that libiconv is installed. You can download it from The HP-UX Porting and Archive Center (<http://hpux.connect.org.uk/hppd/hpux/Development/Libraries>).

Prerequisites

- ☐ (Conditional) NCI 2.7 and eDirectory 8.8 support key sizes up to 4096 bits. If you want to use a 4 KB key size, every server must be upgraded to eDirectory 8.8. In addition, every workstation using the management utilities, for example, iManager and ConsoleOne, must have NCI 2.7 installed on it.

When you upgrade your Certificate Authority (CA) server to eDirectory 8.8, the key size will not change; it will be 2 KB. The only way to create a 4 KB key size is recreate the CA on an eDirectory 8.8 server. In addition, you would have to change the default from 2 KB to 4 KB for the key size, during the CA creation.

For more information, refer to “Installing NICT” on page 81.

- ☐ Enable the Linux host for multicast routing.

On HP-UX systems, enter the following command:

```
/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 224.0.0.0 host_IP_address or gateway
```

- ☐ 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, AIX, or HP-UX systems with NetWare® servers, use timesync.nlm 5.09 or later.

- ☐ (Conditional) 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.
- ☐ (Conditional) (to verify) If you are installing a secondary server into an existing tree as a nonadministrator user, ensure that you have the following rights:
 - ♦ Supervisor rights to the container the server is being installed into.
 - ♦ Supervisor rights to the partition where you want to add the server.
 - NOTE:** This is required for adding the replica when the replica count is less than 3.
 - ♦ All Attributes rights: read, compare, and write rights over the W0.KAP.Security object.
 - ♦ Entry rights: browse rights over Security container object.
 - ♦ All Attributes rights: read and compare rights over Security container object.

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 8.8 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 HP-UX.

Objects	Processor	Memory	Hard Disk
100,000	PA-RISC 2.0	384 MB	144 MB

Objects	Processor	Memory	Hard Disk
1 million	PA-RISC 2.0	2 GB	1.5 GB
10 million	PA-RISC 2.0	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 DSTRACE=*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 8.8 from eDirectory 8.7.1, or 8.7.3 complete the following steps:

- 1 Enter the following to stop the eDirectory server:

```
/sbin/init.d/ndsd stop
```

- 2 Backup the `/etc/nds.conf` file.
- 3 Remove the eDirectory 8.7.x packages using `swremove`. For more information about the package names, refer to “Package Name Specifications for HP-UX” on page 107.
- 4 Install the eDirectory 8.8 packages using `swinstall` and export the paths. For more information, see “Installing eDirectory Components” on page 82.
- 5 Restore the `nds.conf` file you had backed up in the `/etc` directory.
- 6 Configure eDirectory as follows:

```
ndsconfig upgrade --config-file configuration_file_path
```

After the upgrade to eDirectory 8.8, the default location of the configuration files, data files, and log files are changed to `/etc/opt/novell/eDirectory/conf`, `/var/opt/novell/eDirectory/data`, and `/var/opt/novell/eDirectory/log` respectively.

The new directory `/var/opt/novell/eDirectory/data` uses a symbolic link to the `/var/nds` directory.

The old configuration file `/etc/nds.conf` is migrated to `/etc/opt/novell/eDirectory/conf` directory. The old configuration file `/etc/nds.conf` and the old log files under `/var/nds` are retained for reference.

Installing eDirectory

The following sections provide information about installing Novell eDirectory on HP-UX:

- ♦ “Server Health Checks” on page 80
- ♦ “Using OpenSLP for HP-UX” on page 80
- ♦ “Installing NICT” on page 81
- ♦ “Installing eDirectory Components” on page 82
- ♦ “Nonroot User Installing eDirectory 8.8” on page 84
- ♦ “Using the Ndsconfig Utility to Add or Remove the eDirectory Replica Server” on page 86
- ♦ “Using ndsconfig to Configure Multiple Instances of eDirectory 8.8” on page 89
- ♦ “Using Ndsconfig to Install an HP-UX Server into a Tree with Dotted Name Containers” on page 89
- ♦ “Using the Nmasinst Utility to Configure NMAS” on page 89

Server Health Checks

With eDirectory 8.8, when you upgrade or install eDirectory, two server health checks are conducted by default to ensure that the server is safe for the upgrade.

- ♦ “Basic Server Health” on page 110
- ♦ “Partitions and Replica Health” on page 110

Based on the results obtained from the health checks, the upgrade will either continue or exit as follows:

- ♦ If all the health checks are successful, the upgrade will continue.
- ♦ If there are minor errors, the upgrade will prompt you to continue or exit.
- ♦ If there are critical errors, the upgrade will exit.

See Appendix B, “Server Health Checks,” on page 109 for a list of minor and critical error conditions.

Skiping Server Health Checks

To skip server health checks, use `ndsconfig upgrade -j`.

For more information, see Appendix B, “Server Health Checks,” on page 109.

Using OpenSLP for HP-UX

You can use OpenSLP for dynamic tree lookup.

If OpenSLP is not installed on your machine, you can use the static file `/etc/hosts.nds` to locate a tree across the network.

Entries in `/etc/hosts.nds` are of the following format:

`.TREE_NAME. <IP address of the server hosting the tree>`

For more information, refer to the `hosts.nds` man page.

Installing and Configuring OpenSLP

- 1** Download and install OpenSLP for HP-UX from the HP SLP-Service Location Protocol (http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXSLP) Web site.
- 2** The SLP daemon can be configured to function either as a Directory Agent or as a Service Agent. In either case, the following changes need to be done before starting the SLP daemon.
 - ♦ Uncomment the following lines in the SLP configuration file, `/etc/slp.conf`, when configuring the SLP daemon as a Directory Agent (DA):


```
net.slp.DAAddresses = <IP address of the machine>
net.slp.isDA = true
```
 - ♦ Uncomment the following line in the SLP configuration file, `/etc/slp.conf`, when configuring the SLP daemon as a Service Agent:


```
net.slp.isDA = false
```
 - ♦ Uncomment the following line in the SLP configuration file, `/etc/slp.conf`, when configuring the SLP daemon if DA is configured in the network:


```
net.slp.DAAddresses = <IP address of the Directory Agent in the network>
```
- 3** If the DA is not configured, ensure that the system is configured 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 <host_IP_address/gateway>
```

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


```
route add 224.0.0.0 host_IP_address/gateway
```
- 4** In case of other eDirectory replication on Solaris, Linux, AIX, and HP-UX, if Native SLP is also installed, ensure that you are using Open SLP by exporting `NDS_SLP_VERSION` to 2, using the following command:


```
export NDS_SLP_VERSION=2
```
- 5** Stop the `NDS_SLP` daemon.
- 6** Enter the following command to start the SLP daemon:


```
/usr/bin/slpdc start
```

Installing NICI

NICI should be installed before you proceed with the eDirectory installation. Both root and nonroot users can install NICI, though the procedure to do so is different.

Root User Installing NCI

To install NCI, complete the following procedure:

- 1 Enter the following command:

```
swinstall -s absolute_path_of_depot NOVLniu0
```

For example:

```
swinstall -s /home/build/HPUX/HPUX/setup/eDirectory.depot  
NOVLniu0
```

- 2 Execute the following script:

```
/var/opt/novell/nici/set_server_mode
```

Nonroot User Installing NCI

Nonroot users can make use of the sudo utility to install NCI. Sudo (superuser do) allows a root user to give certain users the ability to run some commands as root. For more information, refer to the sudo Website (<http://www.sudo.ws>).

WARNING: sudo enables you to give limited root permissions to nonroot users. Therefore, we strongly recommend you to understand the security implications before proceeding.

A root user needs to complete the following procedure to enable a nonroot user (for example, john) to install NCI:

- 1 Log in as root.
- 2 Edit the /etc/sudoers file using the visudo command.

NOTE: There is no space between vi and sudo in the command.

Make an entry with the following information:

```
Username    hostname=(root) NOPASSWD: /bin/rpm
```

For example, to enable john to run /bin/rpm as root on the hostname hpux-2, type the following:

```
john        hpux-2=(root) NOPASSWD: /bin/rpm
```

A nonroot user (john in the example) needs to do the following to install NCI:

- 1 Log in as john and execute the following command:

```
sudo swinstall -s absolute_path_of_depot NOVLniu0
```

For example:

```
sudo swinstall -s /home/build/HPUX/HPUX/setup/eDirectory.depot  
NOVLniu0
```

- 2 Execute the following script:

```
sudo /var/opt/novell/nici/set_server_mode
```

NCI gets installed in the server mode.

Installing eDirectory Components

Use the swinstall utility to install eDirectory components on HP-UX systems. The utility adds the required packages based on what components you choose to install.

The eDirectory packages are contained in eDirectory.depot and the administration utilities are contained in eDirectory-admutils.depot.

To install eDirectory, enter the following:

```
swinstall -s 'pwd'/eDirectory.depot/*
```

To install only the eDirectory administration utilities, enter the following:

```
swinstall -s 'pwd'/eDirectory-admutils.depot/*
```

For more information, refer to the swinstall man page.

Based on the component you choose to install, the installation program proceeds to add the appropriate depots. The following table lists the depots installed for each eDirectory component.

eDirectory Component	Packages Installed	Description
eDirectory Server	eDirectory.DirectoryUserAgent eDirectory.NDScommon eDirectory.NDSmasv eDirectory.NDSServ eDirectory.NDSmonitor eDirectory.DSRepair eDirectory.NOVLsubag eDirectory.NOVLsnmp novell-npki.npkit novell-pkiserver.pkiserver novell-npkiapi.npkiapi eDirectory.NOVLembox eDirectory.NOVLmgnt eDirectory.NOVLstlog eDirectory.NOVLxis eDirectory.NLDAPsdk eDirectory.NLDAPbase novell-ntls.NTLS novell-nmas.novell-nmas eDirectory.ICE	The eDirectory replica server is installed on the specified server.
Administration Utilities	eDirectory.DirectoryUserAgent eDirectory.NLDAPbase eDirectory.NLDAPsdk novell-npkiapi.npkiapi eDirectory.NOVLxis eDirectory.NOVLmgnt NOVLniu0.NICI	The LDAP Tools administration utilities are installed on the specified workstation.

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 93.

For more information on the nmasinst utility, see “Using the Nmasinst Utility to Configure NMAS” on page 89.

After the installation is complete, you need to update the following environment variables and export them as follows:

- ♦ **Manually export the environment variables**

```
export SHLIB_PATH=/opt/novell/eDirectory/lib:/opt/novell/
eDirectory/lib/nds-modules:/opt/novell/lib:$SHLIB_PATH

export PATH=/opt/novell/eDirectory/bin:/opt/novell/eDirectory/
sbin:$PATH

export MANPATH=/opt/novell/man:/opt/novell/eDirectory/
man:$MANPATH

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/
locale:$TEXTDOMAINDIR
```

- ♦ **Use the ndspath script to export the environment variables**

If you do not want to export the paths manually, you can use the /opt/novell/eDirectory/bin/ndspath script as follows:

- ♦ Prefix the ndspath script to the utility and run the utility you want as follows:

```
/opt/novell/eDirectory/bin/ndspath utility_name_with_parameters
```

- ♦ Export the paths in the current shell as follows:

```
. /opt/novell/eDirectory/bin/ndspath
```

After entering the above command, run the utilities as you would normally do.

- ♦ Call the script in your profile, bashrc, or similar scripts. Therefore, whenever you log in or open a new shell, you can start using the utilities directly.

Nonroot User Installing eDirectory 8.8

A nonroot user can install eDirectory 8.8 using the tarballs as follows:

Prerequisites

- ☐ Ensure that NCI is installed.

For information on installing NCI, refer to “Installing NCI” on page 81.

- ☐ If you want to use SLP and SNMP, ensure that they are installed by the root user.

- ☐ Write rights to the directory where you want to install eDirectory.

If you are a nonadministrator user, ensure that you have the appropriate rights as mentioned in the “Prerequisites” on page 77 section.

Installing eDirectory

- 1** Go to the directory where you want to install eDirectory.

- 2** Untar the tar file in your home directory as follows:

```
tar xvf /tar_file_name
```

The etc, opt, and var directories are created.

- 3** Export the paths as follows:

- ♦ **Manually export the environment variables**

```
export SHLIB_PATH=custom_location/opt/novell/eDirectory/
lib:custom_location/opt/novell/eDirectory/lib/nds-
modules:custom_location/opt/novell/lib:/opt/novell/lib:/
opt/novell/eDirectory/lib:$SHLIB_PATH

export PATH=custom_location/opt/novell/eDirectory/
bin:custom_location/opt/novell/eDirectory/sbin:/opt/
novell/eDirectory/bin:$PATH

export MANPATH=custom_location/opt/novell/
man:custom_location/opt/novell/eDirectory/man:$MANPATH

export TEXTDOMAINDIR=custom_location/opt/novell/
eDirectory/share/locale:$TEXTDOMAINDIR
```

- ♦ **Use the ndspath script to export the environment variables**

If you do not want to export the paths manually, you can use the *custom_location/opt/novell/eDirectory/bin/ndspath* script as follows:

- ♦ Prefix the ndspath script to the utility and run the utility you want as follows:

```
custom_location/opt/novell/eDirectory/bin/ndspath
utility_name_with_parameters
```

- ♦ Go to the *custom_location/opt/novell/eDirectory/bin/* directory and export the paths in the current shell as follows:

```
. custom_location/opt/novell/eDirectory/bin/ndspath
```

NOTE: Ensure that you enter the above command from the *custom_location/opt* directory.

After entering the above command, run the utilities as you would normally do.

- ♦ Call the script in your profile, bashrc, or similar scripts. Therefore, whenever you log in or open a new shell, you can start using the utilities directly.

4 Configure eDirectory in the usual manner.

You can configure eDirectory in any of the following ways:

- ♦ Use the ndsconfig utility as follows:

```
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 [-b port_to_bind] [-B
interface1@port1, interface2@port2,...] [-D custom_location] [--
config-file configuration_file]
```

For example:

```
ndsconfig new -t mary-tree -n novell -a admin.novell -S linux1 -d /
home/mary/inst1/data -b 1025 -L 1026 -l 1027 -o 1028 -O 1029 -D /home/
mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

The port numbers you enter need to be in the range 1024 to 65535. Port numbers lesser than 1024 are normally reserved for the super-user and standard applications. Therefore, you cannot assume the default port 524 for any eDirectory applications.

This might cause the following applications to break:

- ♦ The applications that don't have an option to specify the target server port.
- ♦ The older applications that use NCP, and are run as root for 524.

- ♦ Use the `ndsmanage` utility to configure a new instance. For more information, refer to the “Creating an Instance through `ndsmanage`” on page 38.

Follow the onscreen instructions to complete the configuration.

For more information, see “Using the `Ndsconfig` Utility to Add or Remove the eDirectory Replica Server” on page 86

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 93.

Prerequisite for Configuring eDirectory in a Specific Locale

If you want to configure eDirectory in a specific locale, you need to export `LC_ALL` and `LANG` to that particular locale before eDirectory configuration. For example, to configure eDirectory in the Japanese locale, enter the following:

```
export LC_ALL=ja
export LANG=ja
```

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
- ♦ *admin FDN*: 64 characters
- ♦ *server context*: 64 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:port] [-m module] [-E]
```

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 -s srv1
```

Using the -E option you can enable encrypted replication for the server you want to add. For more information, refer to *Novell eDirectory 8.8 Administration Guide* (<http://www.novell.com/documentation/edir88/index.html>)

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> .

ndsconfig Parameter	Description
-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/opt/novell/eDirectory/conf/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/opt/novell/eDirectory/conf/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 and port number of a server hosting the tree. If this option is used, SLP is not used for tree lookup. Use the -b <i>port_number</i> option along with -p.
-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, SNMP services, and SecretStore (ss) using the add command. If the module name is not specified, by default, all the modules are installed.
-o	Specifies the HTTP clear port number.
-O	Specifies the HTTP secure port number.
-E	Enables encrypted replication for the server you want to add. For more information on encrypted replication, refer to <i>Novell eDirectory 8.8 Administration Guide</i> (http://www.novell.com/documentation/edir88/index.html)
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 Configure Multiple Instances of eDirectory 8.8

You can configure multiple instances of eDirectory 8.8 on a single host. For information on multiple instances, refer to “Using ndsconfig to Configure Multiple Instances of eDirectory 8.8” on page 37 in the Linux chapter.

Using Ndsconfig to Install an HP-UX Server into a Tree with Dotted Name Containers

You can use ndsconfig to install an HP-UX 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 HP-UX 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 8.8, by default, ndsconfig configures NMAS. You can also use nmasinst on Linux, Solaris, AIX, and HP-UX 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 61
- ♦ “Installing Login Methods” on page 61

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/beta/nmas30/admin/data/a53vj9a.html>) in the *Novell Modular Authentication Service Administration Guide*.

7

Relocating the DIB

After installing and configuring Novell® eDirectory™, if there is a need to relocate the DIB, you can do it. You might want to relocate your DIB for multiple reasons, such as, if the number of objects in the tree is expected to grow but the current file system where the DIB exists does not have sufficient space.

Linux and UNIX

Complete the following procedure to relocate your DIB:

- 1** Check the server status as follows:

```
ndscheck
```

- 2** Stop the eDirectory service using ndsmanage as follows:

- 2a** Enter ndsmanage at the command prompt.

- 2b** Select the instance you want to stop.

The menu expands to include the options you can perform on a specific instance.

- 2c** Enter k to stop the instance.

- 3** Get the current DIB location using the following command:

```
ndsconfig get n4u.nds.dibdir
```

NOTE: In eDirectory 8.8, by default the DIB is located at /var/opt/novell/eDirectory/data/dib and on pre-eDirectory 8.8 servers, it is located at /var/nds/dib.

- 4** Copy the DIB to the new location as follows:

```
cp -rp current_DIB_location new_DIB_location
```

For example: To copy the DIB to /home/nds/dib, enter the following:

```
cp -rp /var/opt/novell/eDirectory/data/dib/* /home/nds/dib/
```

- 5** Edit the instance-specific nds.conf configuration file and change the parameter value of n4u.nds.dibdir as follows:

```
n4u.nds.dibdir=new_DIB_location
```

For example, if you are changing the DIB from /var/nds/dib to /home/nds/dib, type the following:

```
n4u.nds.dibdir=/home/nds/dib
```

- 6** Start the eDirectory service as follows

- 6a** Enter ndsmanage at the command prompt.

- 6b** Select the instance you want to start.

The menu expands to include the options you can perform on a specific instance.

6c Enter `s` to start the instance.

7 Check the server status as follows:

`ndscheck`

NetWare and Windows

DIB relocation is currently not supported. However, on Windows you can locate the DIB in a custom location during the eDirectory installation.

8

Configuring Novell eDirectory on Linux, Solaris, AIX, or HP-UX Systems

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

- ♦ “Configuration Utilities” on page 93
- ♦ “Configuration Parameters” on page 94

Configuration Utilities

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

- ♦ “The Ndsconfig Utility” on page 93
- ♦ “Using the Ldapconfig Utility to Configure the LDAP Server and LDAP Group Objects” on page 93
- ♦ “Using the Nmasinst Utility to Configure Novell Modular Authentication Service” on page 94

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 34.

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 35 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, AIX, and HP-UX systems to modify, view, and refresh the attributes of LDAP Server and Group objects.

For more information, see “Using the `ldapconfig` Utility on Linux and UNIX” in the *Novell eDirectory 8.8 Administration Guide*.

Using the Nmasinst Utility to Configure Novell Modular Authentication Service

For eDirectory 8.8, by default, ndsconfig configures NMAS. You can also use nmasinst on Linux, Solaris, AIX, and HP-UX 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 44.

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. We recommend you to use ndsmanage to restart ndsd.

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-thresholdn4u.nds.heartbeat-scheman4u.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/opt/novell/eDirectory/data 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	<p>The interval (in minutes) after which eDirectory backlink consistency is checked.</p> <p>Default=780 Range=2 to 10080</p>
n4u.nds.flatcleaning-interval	<p>The interval (in minutes) after which the flatcleaner process automatically begins purging and deleting entries from the database.</p> <p>Default=720 Range=1 to 720</p>
n4u.nds.server-state-up-threshold	<p>The server state up threshold, in minutes. This is the time after which eDirectory checks the server state before returning -625 errors.</p> <p>Default=30 Range=1 to 720</p>
n4u.nds.heartbeat-schema	<p>The heartbeat base schema synchronization interval in minutes.</p> <p>Default=240 Range=2 to 1440</p>
n4u.nds.heartbeat-data	<p>The heartbeat synchronization interval in minutes.</p> <p>Default=60 Range=2 to 1440</p>
n4u.nds.drl-interval	<p>The interval (in minutes) after which eDirectory distributed reference link consistency is checked.</p> <p>Default=780 Range=2 to 10080</p>
n4u.server.tcp-port	<p>The default port used if the port number is not specified in the n4u.server.interfaces parameter.</p>
n4u.server.max-interfaces	<p>This parameter specifies maximum number of interfaces that eDirectory will use. This value can range from 1 to 2048. Default value is 128.</p>
n4u.server.max-openfiles	<p>This parameter specifies the maximum number of file descriptors that eDirectory can use.</p> <p>Default=maximum allowed by the administrator</p>
n4u.ldap.lburp.transize	<p>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.</p> <p>Default=25 Range=1 to 250</p>
n4u.server.sid-caching	<p>Enables SSL session ID caching. Refer to the SSL v3.0 RFC for more details about session ID caching in SSL.</p>

Parameter	Description
n4u.server.max-threads	<p>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.</p> <p>Default=64 Range=32 to 512</p>
n4u.server.idle-threads	<p>The maximum number of idle threads that are allowed in the eDirectory server.</p> <p>Default=8 Range=1 to 128</p>
n4u.nds.dofsync	<p>Setting this parameter to 0 increases update performance significantly for large databases, but there is a risk of database corruption if the system crashes.</p>
n4u.server.configdir	<p>The eDirectory configuration files are placed here.</p> <p>Default=/etc/opt/novell/eDirectory/conf</p>
n4u.server.vardir	<p>The eDirectory and utilities log files are placed here.</p> <p>Default=/var/opt/novell/</p>
n4u.server.libdir	<p>The eDirectory specific libraries are placed here in the nds-modules directory.</p> <p>Default=/opt/novell/eDirectory/lib</p>
n4u.server.start-threads	<p>Initial number of threads to be started up.</p> <p>Default=8</p>
n4u.server.log-levels	<p>This parameter helps to configure the error logging settings for the server-side messages. It sets the message log level to LogFatal, LogWarn, LogErr, LogInfo, or LogDbg.</p>
n4u.server.log-file	<p>This parameter specifies the log file location where the messages would be logged. By default, the messages are logged into the ndsd.log file.</p>
http.server.interfaces	<p>Comma-separated list of interfaces that HTTP server should use.</p>
https.server.interfaces	<p>Comma-separated list of interfaces that HTTPS should use.</p>
http.server.request-io-buffer-size	<p>Default IO buffer size.</p>
http.server.request_timeout-seconds	<p>Server request timeout.</p>
http.server.keep-timeout-seconds	<p>Number of seconds to wait for the next request from the same client on the same connection.</p>
http.server.threads-per-processor	<p>HTTP thread pool size per processor.</p>
http.server.session-exp-seconds	<p>Session expiration time in seconds.</p>

Parameter	Description
http.server.sadmin-passwd	Session administrator password.
http.server.module-base	HTTP server webroot.
https.server.cached-cert-dn	HTTPS server cached certificate DN.
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.

9

Installing iManager Plug-ins

Novell® iManager™ is a browser-based tool used for administering, managing, and configuring eDirectory™ objects. Novell iManager gives you the ability to assign specific tasks or responsibilities to users and to present the user with only the tools (with the accompanying rights) necessary to perform those sets of tasks.

For more information on installing iManager, refer to the *iManager 2.5 Installation Guide* (<http://www.novell.com/documentation/imanager25/index.html>).

You can use iManager to perform management functions based on plug-ins that have been loaded into iManager.

The following eDirectory plug-ins are available with iManager 2.5:

- ♦ eDirectory Backup and Restore
- ♦ eDirectory Merge
- ♦ eDirectory Repair
- ♦ Import Convert Export Wizard
- ♦ Index Management
- ♦ LDAP
- ♦ Universal Password
- ♦ Filtered Replica Configuration Wizard
- ♦ SNMP

You need to upgrade the existing plug-ins (mentioned above) and install the following new ones:

- ♦ Priority Sync
- ♦ Encrypted Attributes
- ♦ Encrypted Replication

To install the iManager plug-ins, complete the following procedure:

- 1** Go to the *eDirectory_untarred_path/iManager_Plugins/* directory.

This directory contains the eDir_88_Plugins.npm file. This NPM file contains all the eDirectory iManager plug-ins listed above.

- 2** Install the NPM as mentioned in the *iManager 2.5 Installation Guide* (http://www.novell.com/documentation/imanager25/imanager_install_25/data/bnpta1r.html).

10 Uninstalling Novell eDirectory

This chapter contains the following information:

- ♦ “Uninstalling eDirectory on NetWare” on page 101
- ♦ “Uninstalling eDirectory on Windows” on page 101
- ♦ “Uninstalling eDirectory on Linux, Solaris, or AIX” on page 102

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 8.8 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 8.8 installation package.
See “Installing or Upgrading Novell eDirectory 8.8 on NetWare” on page 10 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 8.8 Administration Guide*.

- ♦ “Uninstalling eDirectory, ConsoleOne, and SLP DA” on page 102
- ♦ “Uninstalling NICI” on page 102

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 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 8.8 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-install 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 -c 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
```

`nds-uninstall` does not uninstall the following packages:

Package	Reasons for Not Removing
NICI package	NICI could be used by any of the following: <ul style="list-style-type: none">♦ Any other product♦ eDirectory installed in a custom location♦ eDirectory installed by a nonroot user
NOVLsubag	NOVLsubag could be used by any of the following: <ul style="list-style-type: none">♦ eDirectory installed in a custom location♦ eDirectory installed by a nonroot user

Uninstalling eDirectory on HP-UX

Use the `swremove` utility to uninstall eDirectory components from your HP-UX systems.

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 8.8 Administration Guide*.

For more information, refer to the `swremove` man page.

A

Linux, Solaris, AIX, and HP-UX Packages for Novell eDirectory

Novell® eDirectory™ includes a Linux, Solaris, AIX, and HP-UX 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, AIX, or HP-UX tools installed with the OS.

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

NOTE: On Linux, all the packages are prefixed with *novell-*. For example, NDSserv is novell-NDSserv.

Package	Description
NOVLice	Contains the Novell Import Convert Export utility and is dependent on the NOVImgmt, 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>
NLDAPbase	<p>Contains LDAP libraries, extensions to LDAP libraries, and the following LDAP tools:</p> <ul style="list-style-type: none"> ♦ ldapdelete ♦ ldapmodify ♦ ldapmodrdn ♦ ldapsearch <p>This package is dependent on the NLDAPsdk package.</p>
NOVLnmas	<p>Contains all the NMAAS libraries and the nmasinst binaries needed for NMAAS server. This package is dependent on the NCI and NDSmasv packages.</p>
NLDAPsdk	<p>Contains Novell extensions to LDAP runtime and Security libraries (Client NCI).</p>
NOVLsubag	<p>Contains the runtime libraries and utilities for the eDirectory SNMP subagent. This package is dependent on the NCI, NDSbase, and NLDAPbase packages.</p>
NOVLpkit	<p>Provides PKI Services which do not require eDirectory. This package is dependent on the NCI and NLDAPsdk packages.</p>
NOVLpkis	<p>Provides PKI Server Service. This package is dependent on the NCI, NDSbase, and NLDAPsdk packages.</p>

Package	Description
NOVLSnmp	The runtime libraries and utilities for SNMP. This package is dependent on the NICI package.
NDSdextvnt	Contains the library that manages events generated in Novell eDirectory to other databases. NOTE: This package is not available on HP-UX
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. NOTE: This package is not available on HP-UX
NOVLntls	Contains Novell TLS library. This package is identified as: <ul style="list-style-type: none"> NOVLntls on Solaris, AIX, and HP-UX ntls on Linux

Package Name Specifications for HP-UX

With eDirectory 8.8, the package names are in the *product_name.fileset* format.

Package Names on other UNIX Platforms	Package Names in eDirectory 8.7.1 and 8.7.3	Package Names in eDirectory 8.8
NOVLice	NOVLice.ICE	eDirectory.ICE
NDSbase	NDSbase.DirectoryUserAgent	eDirectory.DirectoryUserAgent
NDScommon	NDScommon.NDScommon	eDirectory.NDScommon
NDSmasv	NDSmasv.NDSmasv	eDirectory.NDSmasv
NDSserv	NDSserv.DirectoryUserAgent	eDirectory.NDSserv
NDSimon	NDSimon.NDSimonitor	eDirectory.NDSimonitor
NDSrepair	NDSrepair.DSrepair	eDirectory.DSRepair
NLDAPbase	NLDAPbase.NLDAPbase	eDirectory.NLDAPbase
NOVLnmas	NOVLnmas.NOVLnmas	novell-nmas.novell-nmas
NLDAPsdk	NLDAPsdk.NLDAPsdk	eDirectory.NLDAPsdk
NOVLsubag	NOVLsubag.NOVLsubag	eDirectory.NOVLsubag

Package Names on other UNIX Platforms	Package Names in eDirectory 8.7.1 and 8.7.3	Package Names in eDirectory 8.8
NOVLpkkit	NOVLpkis.NPKIT	novell-npki.npkit
NOVLpkis	NOVLpkis.PKIS	novell-pkiserver.pkiserver
NOVLsnmp	NOVLsnmp.NOVLsnmp	eDirectory.NOVLsnmp
NOVLpkia	NOVLpkia.NPKIAPI	novell-npkiapi.npkiapi
NOVLembox	NOVLembox.NOVLembox	eDirectory.NOVLembox
NOVLimgnt	NOVLimgnt.NOVLimgnt	eDirectory.NOVLimgnt
NOVLstlog	NOVLstlog.NOVLstlog	eDirectory.NOVLstlog
NOVLxis	NOVLxis.NOVLxis	eDirectory.NOVLxis
NOVLntls	NOVLntls.NTLS	novell-ntls.NTLS

B

Server Health Checks

Novell® eDirectory™ 8.8 provides a diagnostic tool to help you determine whether your server health is safe. The primary use of this tool is to check if the health of the server is safe before upgrading.

The health checks run by default with every upgrade and they occur before the actual package upgrade. However, you can run the diagnostic tool, `ndscheck` (or `dscheck` on NetWare), to do the health checks at anytime.

Need for Health Checks

In earlier releases of eDirectory, the upgrade did not check the health of the server before proceeding with the upgrade. If the health was unstable, the upgrade operation would fail and eDirectory would be in an inconsistent state. In some cases, you probably could not roll back to the pre-upgrade settings.

This new health check tool resolves this, letting you to ensure that your server is ready to upgrade.

Performing Health Checks

You can perform server health checks in two ways:

NOTE: You need administrative rights to run the health check utility.

- ♦ “With the Upgrade” on page 109
- ♦ “As a Standalone Utility” on page 110

With the Upgrade

The health checks are run by default every time you upgrade eDirectory.

Linux and UNIX

Every time you upgrade, the health checks are run by default before the actual upgrade operation starts.

To skip the default health checks, you can use the `-j` option with `nds-install`.

NetWare and Windows

The server health checks happen as part of the installation wizard. You can enable or disable the health checks when prompted to do so.

As a Standalone Utility

You can run the server health checks as a standalone utility anytime you want. The following table lists the health check utility names for each platform.

Table 2 Health Check Utilities

Platform	Utility Name
Linux and UNIX	ndsccheck
	Syntax: <code>ndsccheck -h hostname:port -a admin_FDN -w password -F logfile_path --config-file configuration_file_name_and_path --version</code>
NetWare®	dscheck
Windows	ndsccheck

Types of Health Checks

When you run the ndsccheck utility or upgrade, the following types of health checks are done:

- ♦ Basic Server Health
- ♦ Partitions and Replica Health

When you run the ndsccheck utility, the results are displayed on the screen and logged in ndsccheck.log. For more information on log files, refer to “Log Files” on page 113.

If the health checks are done as part of the upgrade, you are either prompted to continue the upgrade process or the process is aborted, depending on the types of errors found (if any). The types of the errors are described in “Categorization of Health” on page 111.

Basic Server Health

This is the first stage of the health check, where the health check utility checks for the following:

1. The eDirectory service is up. The DIB is open and able to read some basic tree information such as tree name.
2. The server is listening on the respective port numbers.

For LDAP, it gets the TCP and the SSL port numbers and checks if the server is listening on these ports.

Similarly, it gets the HTTP and HTTP secure port numbers and checks if the server is listening on these ports.

Partitions and Replica Health

After checking the basic server health, it then checks the partitions and replica health as follows:

1. Checks the health of the replicas of the locally held partitions.
2. Reads the replica ring of every partition held by the server and checks whether all servers in the replica ring are up and all the replicas are in the ON state.

3. Checks the time synchronization of all the servers in the replica ring, showing any time difference between the servers.

Categorization of Health

There are three possible categories of health, based on the errors found while checking the health of a server:

- ♦ Normal (page 111)
- ♦ Warning (page 111)
- ♦ Critical (page 112)

The status of the health checks is logged into a logfile. For more information, refer to “Log Files” on page 113.

Normal

All the health checks were successful and the server health is normal.

The upgrade proceeds without an interruption.

Warning

Minor errors were found while checking the server health.

If the health check is run as part of the upgrade, you are prompted to either abort or continue. For more information, see Figure 8 on page 112.

Warnings normally occur in the following scenarios:

- ♦ Server not listening on LDAP and HTTP ports (normal, secure, or both).
- ♦ Unable to contact any of the nonmaster servers in the replica ring.
- ♦ Servers in the replica ring are not in sync.

Figure 8 Health Check with a Warning

```

osg-dt-srv27(>)ndsconfig upgrade -a admin.org
[1] Instance at /etc/opt/novell/eDirectory/conf/nds.conf: osg-dt-srv27.org.S0
0615
Enter the password for admin.org:

Starting health check...
Mon Jun 21 08:20:48 2004
Performing health check on the eDirectory server ".CN=osg-dt-srv27.0=org.T=SOL
615." ...

-----
Checking the LDAP and HTTP configuration...
WARNING: eDirectory server is not listening on the LDAP port 389
WARNING: eDirectory server is not listening on the LDAP port 636
Checking health of partitions ...

Status of partition ".T=SOLIT0615." ... [OK]
Checking the status of the replica ring...
Number of replicas = 2
+-----+-----+-----+-----+-----+
+-----+
Server Name                               Status   Time Sync   Time Delta   Replica
state
+-----+-----+-----+-----+-----+
.CN=osg-dt-srv27.0=org.T=SOLIT0615.      UP       YES         0 m:0 s      ON
.CN=osg-dt-srv9.0=org.T=SOLIT0615.       UP       YES         0 m:23 s     ON
+-----+-----+-----+-----+-----+
+-----+

Checking replication delta on the partition...
Maximum replica ring delta "0:3:35 <hh:mm:ss>"
Perishable delta on this server: "0:3:35 <hh:mm:ss>"

eDirectory health check completed.

Errors were detected during the server health check. Refer log file "/var/opt/
novell/eDirectory/data/./log/ndscheck.log" for more details.

For a possible solution refer the following locations -
1. Cool solutions: http://www.novell.com/cool solutions/nds/
2. Support forums: http://support.novell.com/forums/2ed.html
3. Documentation (trouble shooting section): http://www.novell.com/documenta
on/edirectory.html
4. Error codes: http://www.novell.com/documentation/lg/nwec/index.html
5. Patches: http://support.novell.com/filefinder/5069/index.html

WARNING: Errors were detected during the server health check.
Continue (y/n)? _

```

Critical

Critical errors were found while checking the server health.

If the health check is run as part of the upgrade, the upgrade operation is aborted. For more information, see Figure 9 on page 113.

The critical state normally occurs in the following scenarios:

- ♦ Unable to read or open the DIB (might be locked or corrupt).
- ♦ Unable to contact all the servers in the replica ring.
- ♦ Locally held partitions are busy.
- ♦ Replica is not in the ON state.

Figure 9 Health Check with a Critical Error

```

osg-dt-srv27(>)ndsconfig upgrade -a admin.org
[1] Instance at /etc/opt/novell/eDirectory/conf/nds.conf: osg-dt-srv27.org.S0
0615
Enter the password for admin.org:

Starting health check...
Mon Jun 21 08:14:46 2004
Performing health check on the eDirectory server ".CN=osg-dt-srv27.0=org.I=SOL
615." ...

-----
Checking the LDAP and HTTP configuration... [OK]
Checking health of partitions ...

Status of partition ".I=$OLT0615." ... [OK]
Checking the status of the replica ring...
Number of replicas = 2
+-----+-----+-----+-----+-----+
+-----+
Server Name                Status   Time Sync   Time Delta   Replica
state
+-----+-----+-----+-----+-----+
+-----+
.CN=osg-dt-srv27.0=org.I=$OLT0615.    UP      YES        0 m:0 s      ON
.CN=osg-dt-srv9.0=org.I=$OLT0615.     DOWN    -          -            ON
+-----+-----+-----+-----+-----+
+-----+

Checking replication delta on the partition...
Maximum replica ring delta "0:0:23 (hh:mm:ss)"
Perishable delta on this server: "0:0:0 (hh:mm:ss)"

eDirectory health check completed.

Errors were detected during the server health check. Refer log file "/var/opt/
novell/eDirectory/data/./log/ndscheck.log" for more details.

For a possible solution refer the following locations -
1. Cool solutions: http://www.novell.com/cool solutions/nds/
2. Support forums: http://support.novell.com/forums/2ed.html
3. Documentation (trouble shooting section): http://www.novell.com/documenta
on/edirectory.html
4. Error codes: http://www.novell.com/documentation/lg/nwec/index.html
5. Patches: http://support.novell.com/filefinder/5069/index.html

ERROR 2: Check the errors before continuing with the eDirectory upgrade.
osg-dt-srv27(>)_

```

Log Files

Every server health check operation, whether it is run with the upgrade or as a standalone utility, maintains the status of the health in a log file.

The content of the log file is similar to the messages displayed on the screen when the checks are happening. For example, see Figure 8 on page 112 and Figure 9 on page 113.

The health check log file contains the following:

- ♦ Status of the health checks (normal, warning, or critical).
- ♦ URLs where possible solutions can be found.

The following table gives you the locations for the log file on the various platforms:

Table 3 Health Check Log File Location

Platform	Log Filename	Location
Linux and UNIX	ndscheck.log	<p>Depends on the location you have given with the ndscheck -F utility.</p> <p>If you have not used the -F option, the location of the ndscheck.log file is determined by the other options you mention at the ndscheck command line, as follows:</p> <ol style="list-style-type: none">1. If you use the -h option, the ndscheck.log file is saved in the user's home directory.2. If you use the --config-file option, the ndscheck.log file is saved in the server instance's log directory. You can also select an instance from the multiple instances list.
NetWare	dscheck.log	sys:\system
Windows	nsdcheck.log	<i>install_directory</i> \novell nds

C

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 115
- ♦ “SLP Fundamentals” on page 115
- ♦ “Configuration Parameters” on page 117

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>).

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>).

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>) Web site and the SourceForge (<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 116.).

Configuration Parameters

Certain configuration parameters in the %systemroot%/slp.conf file control DA discovery as well:

```
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.DAAActiveDiscoveryInterval = <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.