Installation Guide

Novell®
eDirectory™

8.8 SP4

BETA August, 2008

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 registerd 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).

Contents

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:

Audience

The guide is intended for network administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

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.

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 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.

Installing or Upgrading Novell eDirectory on NetWare

<div align="right">1</div>

Use the following information to install or upgrade Novell® eDirectory™ 8.8 on a NetWare® server:

1.1 System Requirements

System requirements vary depending on the version to which eDirectory is upgraded. The following sections contain the system requirements for upgrading to eDirectory 8.8 and eDirectory 8.8 SP4.

1.1.1 Upgrade to eDirectory 8.8

❑ You can upgrade to eDirectory 8.8 on the following version of NetWare:

- NetWare 6.5 SP7

❑ Administrative rights to the eDirectory tree so you can modify the schema.

1.1.2 Upgrade to eDirectory 8.8 SP4

❑ You can upgrade to eDirectory 8.8 SP4 on the following version of NetWare:

- NetWare 6.5 with Support Pack 4 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 Section 1.3, "Hardware Requirements," on page 13.

1.2 Prerequisites

IMPORTANT: Check the currently installed Novell and Third Party applications to determine if eDirectory 8.8 is supported before upgrading your existing eDirectory environment. You can find out the current status for Novell products in the TID - What Novell products are supported with Novell eDirectory 8.8? (http://support.novell.com/cgi-bin/search/searchtid.cgi?10099872.htm) It is also highly recommended to backup eDirectory prior to any upgrades.

❑ 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) NICI 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 NICI 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) 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.

❑ (Conditional) If you are installing a secondary server into an existing tree as a nonadministrator user, ensure that at least one of the servers in the tree has the same or higher eDirectory version as that of the secondary being added as container admin. In case the secondary being added is of later version, then the schema needs to be extended by the admin of the tree before adding the secondary using container admin.

Configuring Static IP Address

Static IP address must be configured on the server for the eDirectory to perform efficiently. Configuring eDirectory on the servers with DHCP address can lead to unpredictable results.

1.3 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.

1.4 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`.

1.5 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 Section 2.5, "Updating the eDirectory Schema for Windows," on page 26.

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 `dsrepair.nlm` and select *Rebuild Operational Schema*, schema enhancements made by the Post NetWare 5 Schema Update will be lost. To resolve lost schema enhancements, run `dsrepair.nlm` according to the following table.

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

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

7 Close `dsrepair.nlm` before installing eDirectory on the server.

If `dsrepair.nlm` is loaded, the server might not restart.

1.6 Disk Space Check on Upgrading to eDirectory SP4 or later

When eDirectory server is upgraded from previous versions to eDirectory 8.8 SP4 or later, the disk space check for the DIB upgrade would be performed. The free disk space necessary in the file system, where the DIB resides would be equal to that of the DIB size. The messages of the disk space check would be updated in the `sys:\system\dscheck.log`.

NOTE: The disk space check is required only during the DIB upgrade process. For more information, refer to Chapter 7, "Upgrade Requirements of eDirectory 8.8," on page 117.

1.7 Installing or Upgrading Novell eDirectory on NetWare

This section contains the following information:

- "Installing or Upgrading Novell eDirectory 8.8 on NetWare" on page 15
- "Server Health Checks" on page 16
- "Installing NMAS Server Software" on page 16
- "Installing NMAS Client Software" on page 17
- "Installing into a Tree with Dotted Name Containers" on page 17
- "Unattended Upgrade to eDirectory 8.8 SP4 on Netware" on page 18
- "Remote Installation or Upgrade" on page 22

NOTE: Unattended Upgrade feature is supported only for SP3 and later releases.

1.7.1 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 29.

7 Select the NMAS™ login method you want to install, then click *Next*.

See "Installing NMAS Server Software" on page 16 and "Installing NMAS Client Software" on page 17 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.

1.7.2 Server Health Checks

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

 - Section B.3.2, "Partitions and Replica Health," on page 151

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, "eDirectory Health Checks," on page 149 for a list of minor and critical error conditions.

Skipping Server Health Checks

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

For more information, see Appendix B, "eDirectory Health Checks," on page 149.

1.7.3 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.

1.7.4 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.

1.7.5 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 1-1).
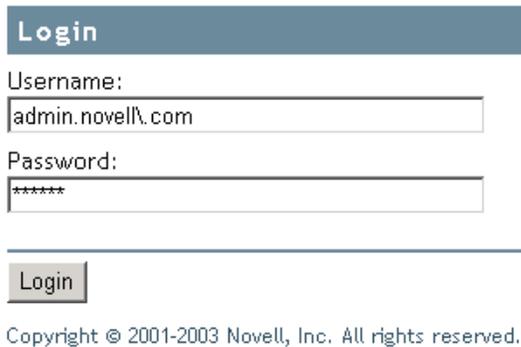
1.7.6 Unattended Upgrade to eDirectory 8.8 SP4 on Netware

The SPK for eDirectory 8.8 upgrade is provided with the Netware installation package. SPK has to be inserted into the ConsoleOne "Server Software Packages" snap-in for customizing into local environments. Once the Server Software Package ConsoleOne snap-in is installed, you can insert this SPK in the ConsoleOne.

NOTE: Pre upgrade health check is not run during unattended upgrade, ensure you run dscheck.nlm manually before starting the upgrade.

To perform this,

1 Import the applicable SPK into ConsoleOne.

2 To do this, right click on the Server Software Packages name space and select *Insert New Package* (see Figure 1-2).

Figure 1-2   *Adding the package into ConsoleOne*
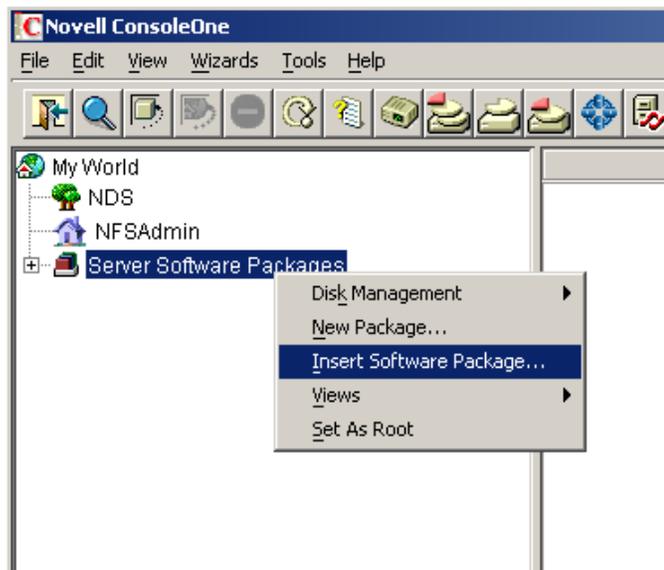
An SPK has components and properties. To see the components, click on the SPK's expand box. The properties include a description, requirements, and variables. The Support Pack SPKs use variables, which is the only place where each site will need to make specific modifications. All of the SPK's components may use the SPK's variables. To see the variables, right click on the *SPK* and select *Properties* (see Figure 1-3).

Figure 1-3 *Editing the package properties*
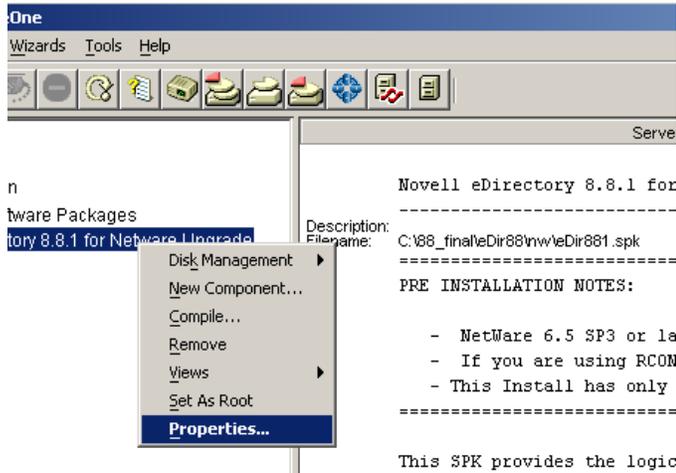
3 Click on the *Variables* tab to make the site-specific changes needed by the installation process (see Figure 1-4).

Figure 1-4 *Modifying the package variables*
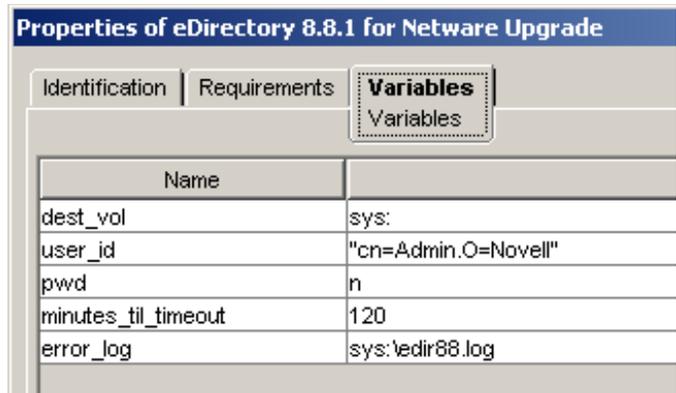
Edit and change the values of the two variables "user_id" and "pwd".

- ◆ user_id

  administrator name that the install program will use to extend the tree.

- ◆ pwd

  password for the above username

These are the only two fields that need to be edited. Leave the values of rest of the variables as defined.

WARNING: The installation source folders will be partially removed for security reasons. You need to copy the installation source again in case you restart the installation on failures, e.g, Disk Space unavailability errors.

Adding Upgrade Source to the SPK

The automated upgrade for eDirectory on Netware for ZFS environment is delivered as SPK along with the source. The compiled CPK is not provided since the user is expected to provide values for the variables containing administrator credentials. This SPK needs to be compiled to a CPK in the customer site after providing values to these variables.

As mentioned earlier, the source is delivered along with the SPK and the source has to be attached to the SPK before compiling the CPK. Steps for attaching the source to the SPK is given below:

1 Copy the source to the local machine and name the folder as "eDir88". There are references to this folder name inside the SPK and hence please use this suggested name.

2 Right click on the "Copying files" component and select *Properties* and browse to the *Copy File* Tab.

3 Remove the file set (if given as a sample) by right clicking on the file group and choosing *Remove*. Choose "Add File" by right clicking on the *File Group* as given below:

Figure 1-5   *Adding the source to the SPK*
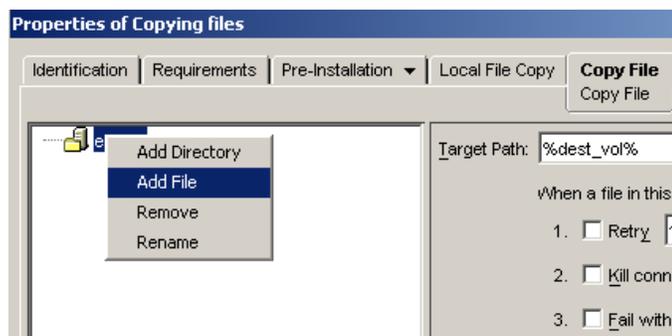
4 Then select the "eDir88" folder that contains the source files that are delivered along with the SPK as given below:

Figure 1-6   *Selecting the upgrade source*
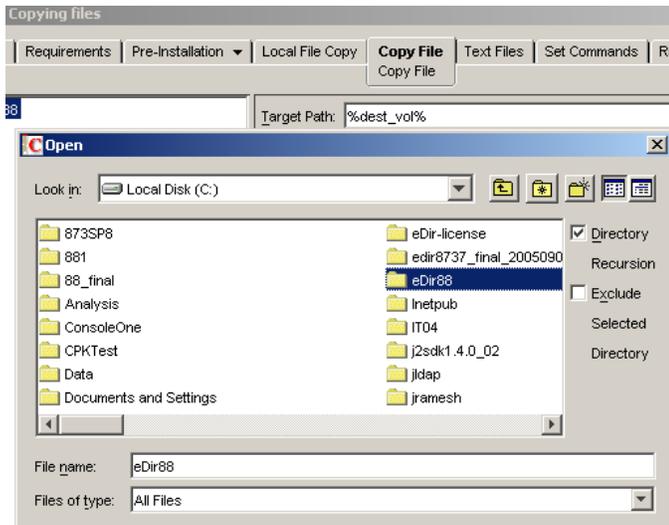
Fully Automated Standalone Upgrade

Once the above changes are performed, compile the SPK to make a CPK using the right-click menu option in the main component to compile (see Figure 1-7).

Figure 1-7   *Compiling the SPK*
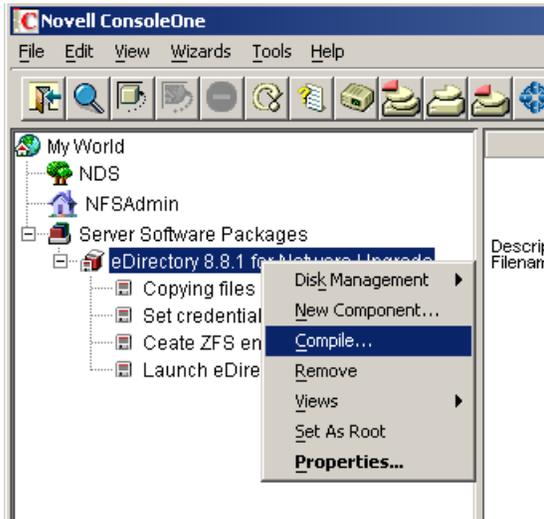
This CPK is ready to be imported into the Policy distributor to be used in the upgrade at all customer sites. For more information on CPKs, refer to the Compiling Software Packages (http://www.novell.com/documentation/zenworks7/sm7admin/index.html?page=/documentation/zenworks7/sm7admin/data/a32jldl.html).

IMPORTANT: This script contains the admin username and password in clear text in a temporary file until the server is automatically restarted and used to start nwconfig again. Soon after the script is called, this temporary file <NDS8.NCF> and the script files are deleted permanently from the system.

1.7.7 Remote Installation or Upgrade

During Install or Upgrade, the Installer provides the following message and prompts for user input:

"Are you installing remotely through rconsole?"

  "No-Local"

  "Yes-Remote"

After prompting this message, the Installation typically continues in the XServer Console displaying options to choose the NMAS methods to be installed, followed by configuration progress.

If you are performing the installation or upgrade from a remote terminal, you will not be able to access the XServer Console to choose the NMAS methods to be installed. In this case, you could choose "Yes-Remote", which by default installs all NMAS methods without any further indications in the System Console.

NOTE: The Installer will restart the server once the installation is complete.

Installing or Upgrading Novell eDirectory on Windows

2

Use the following information to install or upgrade Novell® eDirectory™ 8.8 on a Windows* 2000 or Windows Server 2003:

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 27.

2.1 System Requirements

❑ One of the following:

- Windows* 2003 Server SP2
- Windows* 2008 Server 32 and 64-bit

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.

2.2 Prerequisites

IMPORTANT: Check the currently installed Novell and Third Party applications to determine if eDirectory 8.8 is supported before upgrading your existing eDirectory environment. You can find out the current status for Novell products in the TID - What Novell products are supported with Novell eDirectory 8.8? (http://support.novell.com/cgi-bin/search/searchtid.cgi?10099872.htm) It is also highly recommended to backup eDirectory prior to any upgrades.

❑ 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) NICI 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 NICI 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.

 NOTE: The Windows Silent Installer requires that NICI is already installed.

❑ 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) 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.

❑ (Conditional) If you are installing a secondary server into an existing tree as a nonadministrator user, ensure that at least one of the servers in the tree has the same or higher eDirectory version as that of the secondary being added as container admin. In case the secondary being added is of later version, then the schema needs to be extended by the admin of the tree before adding the secondary using container admin.

Configuring Static IP Address

Refer to "Configuring Static IP Address" on page 12 for more information on configuring static IP addresses.

2.3 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.

2.4 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).

2.5 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 Section 1.5, "Updating the eDirectory Schema for NetWare," on page 14.

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.

2.6 Disk Space Check on Upgrading to eDirectory SP4 or later

When eDirectory server is upgraded from previous versions to eDirectory 8.8 SP4 or later, the disk space check for the DIB upgrade would be performed. The free disk space necessary in the file system, where the DIB resides would be equal to that of the DIB size. The messages of the disk space check would be updated in the `ni.log` and `<Install Path>/novell/nds/ndscheck.log`.

NOTE: The disk space check is required only during the DIB upgrade process. For more information, refer to Chapter 7, "Upgrade Requirements of eDirectory 8.8," on page 117.

2.7 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 27
- "Server Health Checks" on page 29
- "Communicating with eDirectory through LDAP" on page 29
- "Installing NMAS Server Software" on page 32
- "Installing NMAS Client Software" on page 32
- "Installing into a Tree with Dotted Name Containers" on page 32
- "Unattended Install and Upgrade to eDirectory 8.8 SP4 on Windows" on page 34

2.7.1 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 155
- 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* SP4 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.

- NICI 2.7

For more information on the Novell International Cryptographic Infrastructure (NICI), see the *NICI 2.7 Administration Guide* (http://www.novell.com/documentation/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.

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 32.

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 2.6 Administration Guide* (http://www.novell.com/documentation/imanager26/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 29.

12 Select the NMAS™ login methods you want to install, then click *Next*.

See and for more information.

13 Click *Finish* to complete the eDirectory installation.

2.7.2 Server Health Checks

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

-

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 for a list of minor and critical error conditions.

Skipping Server Health Checks

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

For more information, see .

2.7.3 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 2-1   *Defaults for the LDAP Configuration Screen*
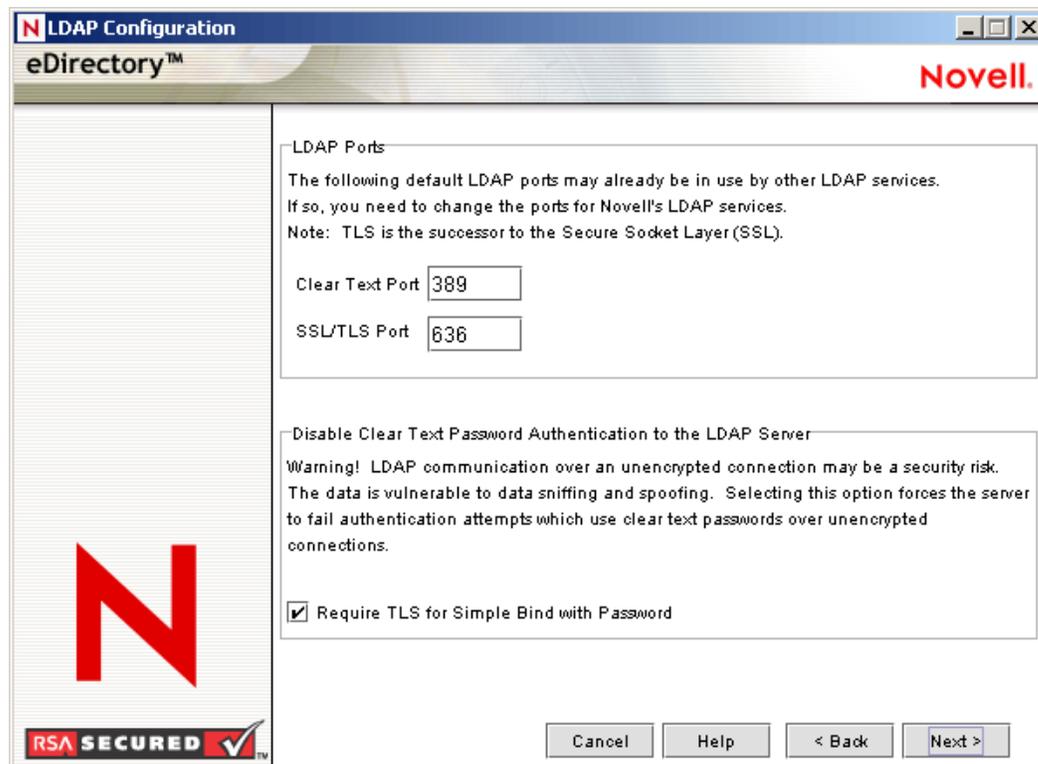
Scenario: Require TLS for Simple Bind with Password Is Enabled: Olga is using a client that asks for a password. After Olga enters a password, the client connects to the server. However, the LDAP server does not allow the connection to bind to the server over the clear-text port. Everyone is able to view Olga's password, but Olga is unable to get a bound connection.

The *Require TLS for Simple Bind with Password* 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 2-2 *LDAP Server Connections Page in iManager*

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 (http://www.novell.com/documentation/edir88/edir88/data/ai8wt35.html) 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 (http://www.novell.com/documentation/edir88/edir88/data/ai8wt35.html) in the *Novell eDirectory 8.8 Administration Guide* for more information.

2.7.4 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.

2.7.5 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.

2.7.6 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 2-3 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 2-3   *eDirectory Installation Information Screen*

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 2-4).

Figure 2-4   *iMonitor Login Screen*

2.7.7 Unattended Install and Upgrade to eDirectory 8.8 SP4 on Windows

Prerequisites

- Ensure Microsoft Visual C++ 2005 Runtime Libraries are installed. Install them manually from vcredist_x86.exe, located at `eDirectory\nt\i386\redist_pkg`.

eDirectory 8.8 SP4 automates the eDirectory installation and upgrade so that eDirectory is installed or upgraded silently on Windows servers without human intervention.

On Windows, the unattended installation of eDirectory uses predefined text files that facilitate the unattended installation.The following sections discuss various features that can be used to configure the unattended installation, including the install location, no display of splash screens, port configurations, additional NMAS methods, stopping and starting SNMP services, etc.

- "Response Files" on page 34
- "Adding Features to the Automated Installation" on page 35
- "Controlling Automated Installation" on page 40
- "Unattended Installation of eDirectory using Response File" on page 43

Response Files

Installing or upgrading to eDirectory 8.8 SP4 on Windows operating system can be made silent and more flexible by using a response file for the following:

- Complete unattended installation with all required user inputs
- Default configuration of components
- Bypassing all prompts during the installation

A response file is a text file containing sections and keys, similar to a `Windows.ini` file. You can create and edit a response file using any ASCII text editor. The eDirectory upgrade reads the installation parameters directly from the response file and replaces the default installation values with response file values. The installation program accepts the values from the response file and continues to install without prompts.

Response.ni File Sections and Keys

The eDirectory 8.8 SP4 installation requires changes to the sections in the response file to add information about the eDirectory instance to be installed, including the tree name, administrator context, administrator credentials (including user name and passwords), installation locations, etc. A full list of the keys and their default values is available in the sample `response.ni` file that is delivered with the eDirectory installation.

NOTE: You should use the provided `response.ni` file available at `eDirectory\nt\i386\NDSonNT\response.ni` in the eDirectory installation.There are essential parameters and set by default in this file. When editing the `response.ni` file, ensure there are no blank spaces between the key and the values along with the equals sign ("=") in each key-value pair.

Installation Syntax

You can also use a response file for two scenarios in an upgrade:

- To provide the values of the tree parameters and to configure an unattended installation
- To input values during an upgrade

IMPORTANT: You provide the administrator user credentials in the `response.ni` file for an unattended installation. Therefore, you should permanently delete the file after the installation to prevent the administrator credentials from being compromised.

Adding Features to the Automated Installation

Most details for configuring the eDirectory Installer have default setting for the manual installation. However, during unattended installation, each configuration parameter must be explicitly configured. This section discusses the basic settings to be configured, irrespective of any sequence of installation or additional features.

eDirectory Server Details

Regardless of whether it is an upgrade or a primary/secondary server installation, the details of the server being installed or upgraded must be provided to the Installer. Most of this information is configured in two tags, `[NWI:NDS]` and `[Initialization]`.

`[NWI:NDS]`

- **Upgrade Mode:** This key applies only to a server upgrade. Though not essential, set this parameter to False for fresh installations. For an upgrade, you can either set it to True or to Copy.
- **Server Context:** This is the complete DN of the server object (server name), along with the container object. For example, if the server being installed is 'EDIR-TEST-SERVER', the value for this parameter will be "EDIR-TEST-SERVER.Novell" if the Server container is 'Novell'.
- **Tree Name:** For a primary server installation, this is the name of the tree that needs to installed; for a secondary server installation, this is the tree to which this server must be added.
- **Server Name:** The name of the server that is being installed.
- **Server Container:** Any server added to a tree has a server object containing all the configuration details specific to the server. This parameter is the container object in the tree to which the server object will be added. For primary server installations, this container will be created with the server object.
- **Admin Login Name:** The name (RDN) of the Administrator object in the tree that has full rights, at least to the context to which this server is added. All operations in the tree will be performed as this user.
- **Admin Context:** Any user added to a tree has a user object that contains all the user-specific details. This parameter is the container object in the tree to which the Administrator object will be added. For primary server installations, this container will be created with the server object.
- **Admin password:** The password for the Administrator object created in the previous parameters. This password will be configured to the Administrator object during primary server installations. For secondary server installations, this needs to be the password of the Administrator object in the primary server that has rights to the context to which the new server is added.

- **NDS Location:** The eDirectory install location in the local system where the libraries and binaries are copied. By default, eDirectory is installed into `C:\Novell\NDS` unless it is changed in the response file.

- **DataDir:** Until eDirectory version 8.8, the DIB was installed inside the NDS location as a subfolder. Later, administrators were given the option to provide a different DIB location, because there might be too much data stored in the DIB to fit into the NDS location. Currently, by default the DIB is installed in the `DIBFiles` subfolder inside the NDS location, but administrators can change this parameter and provide a different location.

The following is a sample of text in the response file for all the basic parameters described above:

```
[NWI:NDS]

Upgrade Mode=copy

Tree Name=SLP-TEST

Server Name=NDS-LDAP-P2-NDS

Server Container=Novell

Server Context=NDS-LDAP-P2-NDS.Novell

Admin Context=Novell

Admin Login Name=Admin

Admin Password=novell

NDS Location=E:\Novell\NDS

DataDir=E:\Novell\NDS\DIBFiles
```

You can also configure two additional parameters:

- **Installation Location:** This is the same as the NDS Location configured in the previous section. This location is used by the Installer while copying files to the install location, and the other location is used by the components to refer to the base eDirectory installation while they are configured. The default value is `C:\Novell\NDS`, if not specified in the response file.

  For example:

  ```
  [Novell:DST:1.0.0_Location]

  Path=file:/C:\Novell\NDS
  ```

- **System Location:** The eDirectory Installer requires access to the system folder to copy `DLLs` and to access system-specific files during installation. This parameter must be configured with the path to the system folder of the machine where the server is installed.

  For example:

  ```
  [Novell:SYS32_DST:1.0.0_Location]

  Path=file:/C:\WINNT\system32
  ```

The following screen appears when the server collects the above parameters from the response file.

Figure 2-5   *Installing eDirectory*

Adding NMAS Methods

eDirectory supports installation of multiple NMAS methods, both during install and upgrade. During manual installations, you can select the NMAS methods to install and configure. This can also be achieved in automated installations.

The NMAS-related configuration settings are provided inside the [NWI:NMAS] tag. The tag has two keys to be configured, and both are mandatory:

 ◆ **Choices:** This key informs the eDirectory installation component on the number of NMAS methods that need to be installed.

 ◆ **Methods:** This key lists the NMAS method options that need to be installed. Currently, there are 12 supported NMAS methods. The method names and their types are as follows:

Table 2-1   *NMAS Methods*

Method Name	Method Type
X509 Advanced Certificate	NMAS Advanced X.509 authentication method
CertMutual	Certificate mutual login method
Challenge Response	The Novell challenge response NMAS method
DIGEST-MD5	Digest MD5 login method
EnhancedPassword	Enhanced password login NMAS method
Entrust	Entrust certificate login method
GSSAPI	SASL GSSAPI mechanism for eDirectory. Authentication to eDirectory through LDAP using a Kerberos ticker
NDS	NDS login method (default)
Change Password	NDS change password post-login method
Simple Password	Simple password NMAS login method
Universal Smart Card	NMAS universal smart card X.509 authentication method
X509 Certificate	The Novell X.509 certificate server certificate

NOTE: The method names should exactly match those listed in the above table, as options to the Methods key. The Installer matches the exact string (with case) for choosing the NMAS methods to install.

The NDS NMAS method is mandatory and will be installed automatically if no NMAS methods list is provided. However, if you are creating an explicit list, do not remove this method from the list.

If the NMAS methods are configured using this methodology in the response file, eDirectory shows the following status while installing, without prompting for user input.

Figure 2-6   *NMAS Login Method Creation*
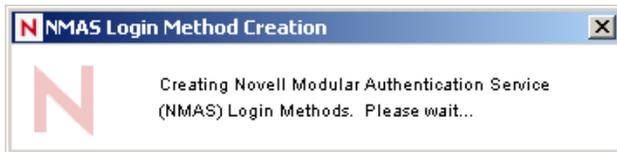
The following is sample text in the response file for choosing the NMAS methods:

```
[NWI:NMAS]

Choices=12
Methods=X509 Advanced Certificate,CertMutual,Challenge Response,DIGEST-
MD5,Enhanced Password,Entrust,GSSAPI,NDS,NDS Change Password,Simple
Password,Universal Smart Card,X509 Certificate
```

HTTP Ports

eDirectory listens on preconfigured HTTP ports for access through the Web. For example, iMonitor accesses eDirectory through Web interfaces. They need to specify certain in order to access the appropriate applications. There are two keys that can be set prior to installation to configure eDirectory on specific ports:

- **Clear Text HTTP Port:** The port number for the HTTP operations in clear text.
- **SSL HTTP Port:** HTTP port number for operations on the secure socket layer.

The following is sample text in the response file for configuring HTTP port numbers:

```
[eDir:HTTP]

Clear Text HTTP Port=8028

SSL HTTP Port=8030
```

LDAP Configuration

eDirectory supports LDAP operations. It listens for LDAP requests in clear text and SSL, on two different ports. These ports can be configured in the response file prior to installation so that when eDirectory is started, it listens on these configured ports.

There are three keys in the `[NWI:NDS]` tag that configure the LDAP ports:

- **LDAP TLS Port:** The port on which eDirectory should listen for LDAP requests in clear text.
- **LDAP SSL Port:** The port on which eDirectory should listen for LDAP requests in SSL. You can also use a key to configure whether eDirectory should mandate secure connections when bind requests send the password in clear text.
- **Require TLS:** Whether eDirectory should mandate TLS when receiving LDAP requests in clear text.

Figure 2-7 *LDAP Configuration*

The following is sample text in the response file for LDAP configuration:

```
[NWI:NDS]

Require TLS=No

LDAP TLS Port=389

LDAP SSL Port=636
```

Language Settings

The eDirectory Installer language settings configure the locale and set the display language.

There are currently three locale options that can be set during installation: English, French and Japanese. Each has a specific key in the `[Novell:Languages:1.0.0]` tag that can be set to True/False prior to the start of installation.

- **LangID4:** English. Setting this to True configures the English locale during installation.
- **LangID6:** French. Setting this to True configures the French locale during installation.
- **LangID9:** Japanese. Setting this to True configures the Japanese locale during installation.

These options are mutually exclusive, which is easily enforced in manual installation via radio buttons. In unattended installations, you need to ensure only one of them is set to True.

The following is sample text in the response file for configuring an English locale:

```
[Novell:Languages:1.0.0]

LangID4=true

LangID6=false

LangID9=false
```

Status messages about the configuration of each component are displayed in message boxes throughout the installation. By default, these messages are in English. You can also change the display language during installation by using the DisplayLangauge key in the `[Initialization]` tag.

- ◆ **DisplayLanguage:** This key is in the `[Initialization]` section. Its parameters configure languages.

  The following is sample text in the response file for configuring English as the display language:

  `[Initialization]`

  `DisplayLanguage=en_US`

Controlling Automated Installation

The response file can also be edited to control the flow of automated installation.

Stopping SNMP services

This feature is specific to an eDirectory installation on Windows. Most Windows servers have SNMP configured and running. When eDirectory installs, the SNMP services need to be brought down and restarted after the installation. With manual installations, the Installer prompts the user on-screen to stop the SNMP services before continuing the installation. This prompt can be avoided during automation by setting the key in the `[NWI:SNMP]` tag:

- ◆ **Stop service:** Set the value to Yes to stop the SNMP services without prompting. The status of is displayed on-screen as shown below:

Figure 2-8 SNMP Service Shutdown

The following is sample text in the response file for stopping SNMP services:

`[NWI:SNMP]`

`Stop service=yes`

SLP Services

eDirectory uses SLP services to identify other servers or trees in the subnet during installation or upgrade. If SLP services are already installed on your server, and you want to replace them with the version that ships with the current version of the eDirectory (or use your own SLP services), you can set appropriate keys in the `[NWI:SLP]` tag to uninstall and remove the existing SLP services.

The following is sample text in the response file for uninstalling and removing SLP services:

`[EDIR:SLP]`

`Need to uninstall service=true`

```
Need to remove files=true
```

Primary/Secondary Server Installation

eDirectory Installer provides options for the unattended install of a primary or a secondary server, into a network. There are three keys that help the Installer decide whether it is a primary or a secondary server installation.

- **New Tree:** Use this key in the `[NWI:NDS]` tag and and set it to Yes for a new tree installation, or No for a secondary server installation.
- **ExistingTreeYes:** This key is in the `[Novell:ExistingTree:1.0.0]` tag. Set it to True/false. Set this to False for a new tree or primary server installation and set it to True for a secondary server in an existing tree.
- **ExistingTreeNo:** This key also is in the `[Novell:ExistingTree:1.0.0]` tag. Although it seems to be redundant to the previous key, the Installer refers to both keys, so both of them must be configured properly. Set this one to True for a new tree or primary server installation and set it to False for adding a secondary server in an existing tree.

For example, the keys for installing a primary server in a new tree would be as follows:

```
[NWI:NDS]

New Tree=Yes



[Novell:ExistingTree:1.0.0]

ExistingTreeYes=false

ExistingTreeNo=true
```

and for a secondary server installation into an existing tree:

```
[NWI:NDS]

New Tree=No

[Novell:ExistingTree:1.0.0] ExistingTreeYes=true ExistingTreeNo=false
```

Preconfigured Unattended Installation

All user-specific configuration details can be edited in the response file. However, there are certain parameters that should not be changed. These are for file copy and component information specific to the eDirectory components to be installed. Make sure these parameters in the response file are not modified. Do not change them from the values in the eDirectory release.

Install as Service Tag: eDirectory runs as a service in Windows. It is mandatory that this parameter is always set to Yes to make sure that eDirectory is installed as a service.

```
[NWI:NDS]

Install as Service=Yes
```

Selected Nodes Tag: This tag lists the components that are installed in eDirectory, along with information in the profile database that contains more information about the component, including source location, destination copy location, and component version. These details in the profile database are compiled into a `.db` file that is delivered in the eDirectory release.

```
[Novell:NOVELL_ROOT:1.0.0]
```

File Copy Tag: This tag contains keys for display settings that are handled in the next section, including the file copy profile information:

```
overWriteNewerFile=false
```

```
overWriteNewerFilePrompt=true
```

```
copyToRemoteDestination=true
```

These options specify the response from the eDirectory Installer in scenarios such as file write conflicts, file copying decisions, etc.

Silent Installation Parameters

This section describes parameters that need to be set for the Installer to run unattended.

```
[NWI:NDS]
```

```
Prompt=false
```

The `[NWI:NDS]` section describes eDirectory configuration details such as tree name and server name. If you don't want the Installer to prompt for values for these parameters, set this parameter to False.

```
[Selected Nodes]
```

```
Prompt=false
```

If you don't want the Installer to prompt for the destination copy location, version details, etc. for all components configured with the eDirectory, set this parameter to False in the `[Selected Nodes]` tag.

```
[Novell:NOVELL_ROOT:1.0.0]
```

```
Prompt=false
```

If you don't want the Installer to prompt for yes/no questions, or for other decisions with parameters in this section, set this parameter to False in the `[Selected Nodes]` tag.

```
[Novell:ExistingTree:1.0.0]
```

```
Prompt=false
```

If you don't want the Installer to prompt for deciding whether is it a new tree installation, or for adding a secondary server to an existing tree, set this parameter False in the `[Selected Nodes]` tag.

```
[Initialization]
```

```
InstallationMode=silent
```

```
SummaryPrompt=false
```

```
prompt=false
```

The `InstallationMode` key must always be explicitly set to Silent for unattended installations.

Status and Image Displays

During installation, there are various images and status information displayed. Most images contain information on what version of eDirectory is installed, what components are installed, a welcome screen, license files, customization options, a status message indicating the component currently being installed, percentage complete, etc. Some applications that intend to embed eDirectory might not want eDirectory displaying these images.

All image and status display details are configured in the `[Novell:NOVELL_ROOT:1.0.0]` tag, including configuration information for the welcome page, close page, summary page, license agreement page, language page, custom choices page, wizard page, welcome page. There are corresponding on/off parameters for each of these configurations.

For example:

- The welcomeScreen parameter is controlled by `showWelcomeScreen=true/false`
- The summaryScreen parameter is controlled by `allowSummary=true/false`
- The licenseAgreementScreen parameter is controlled by `allowLicenseAgreement=true`
- If the progress bar shouldn't be displayed, use `allowStatusBar=false`
- If the final page that reports successful installation is not required, set `[eDirCloseScreen]Silent=true`

Most of the details are preconfigured in the response file that ships with eDirectory. If you need modifications, change the parameters in this tag.

Unattended Installation of eDirectory using Response File

Launching the eDirectory Installer on Windows is easy. The `install.exe` delivered in the eDirectory release is invoked in the command line with a few additional parameters. Assuming that the `response.ni` file is available in `C:\`, the command is:

```
C:\eDirectory\nt\I386\NDSonNT\install.exe /silent /template=C:\response.ni
```

This performs an unattended installation of eDirectory on the Windows server.

Installing or Upgrading Novell eDirectory on Linux

3

Use the following information to install or upgrade Novell® eDirectory™ 8.8 on a Linux* server:

3.1 System Requirements

❑ One of the following:

- 32-bit
    - SUSE Linux Enterprise Server 9 SP4
    - SUSE Linux Enterprise Server 10 SP1
    - SUSE Linux Enterprise Server (SLES) 10 SP1 XEN
    - Red Hat Advanced Server 4
    - Red Hat 5.0
    - Red Hat 5.0 AP
    - Red Hat 5.0 AP Virtualization
- 64-bit
    - SUSE Linux Enterprise Server (SLES) 9 SP4
    - SUSE Linux Enterprise Server (SLES) 10 SP1
    - SUSE Linux Enterprise Server (SLES) 10 SP1 XEN

NOTE: eDirectory 8.8 SP4 is supported on SLES 10 XEN virtualization service that runs the SLES 10 guest OS. The following updates are available at https://update.novell.com (https://update.novell.com).

- SUSE-Linux-Enterprise-Server-X86_64-10-0-20061011-020434
- SLES10-Updates

For registering and updating SUSE Linux Enterprise 10, refer to Registering SUSE Linux Enterprise 10 with the Novell Customer Center (http://support.novell.com/techcenter/articles/RegandUpdate_SLE10.html). After installating the latest update, ensure that the minimum patch level of the installed update is 3.0.2_09763-0.8.

To determine the version of SUSE Linux you are running, see the /etc/SuSE-release file.

- ◆ Red Hat Advanced Server 4
- ◆ Red Hat 5.0
- ◆ Red Hat 5.0 AP
- ◆ Red Hat 5.0 AP Virtualization

  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.

- ◆ 64-bit eDirectory Supported Platform
  - ◆ SLES 10 SP1
- ❑ 256 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

> **NOTE:** By default, gettext is not installed on the base install of SLES9, but is included in the SLES9 install CD's. Ensure you install it before you run nds-install, or you will get messages about it missing.

- ❑ Ensure that net-snmp-32-bit RPM is installed on 64-bit SLES or OES Linux
- ❑ If you use ZLM for patch management, apply the hotpatch ZLM6.6.2 HP4 before upgrading to eDirectory 8.8 SP4. On servers such as Vanilla SLES10 or SLES10 SP1, libredcarpet should be upgraded to the latest patch level using Yast online update.

3.2 Prerequisites

> **IMPORTANT:** Check the currently installed Novell and Third Party applications to determine if eDirectory 8.8 is supported before upgrading your existing eDirectory environment. You can find out the current status for Novell products in the TID - What Novell products are supported with Novell eDirectory 8.8? (http://support.novell.com/cgi-bin/search/searchtid.cgi?10099872.htm). We also highly recommend you to back up eDirectory before any upgrades.

- ❑ (Conditional) NICI 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 NICI 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 Section 3.6.2, "Installing NICI," on page 59.

- ❑ 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

❑ 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, or AIX 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`.

❑ (Conditional) `compat-libstdc++-33-3.2.3-61.i386.rpm`

If you are installing eDirectory on RHEL5.0, install `compat-libstdc++-33-3.2.3-61.i386.rpm`.

❑ 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 `java 1_4_2 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) If you are installing a secondary server into an existing tree as a nonadministrator user, create a container and then partition it. Ensure that you have the following rights:

 ◆ Supervisor rights to this partition.

 ◆ 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.

❑ (Conditional) If you are installing a secondary server into an existing tree as a nonadministrator user, ensure that at least one of the servers in the tree has the same or higher eDirectory version as that of the secondary being added as container admin. In case the secondary being added is of later version, then the schema needs to be extended by the admin of the tree before adding the secondary using container admin.

Configuring Static IP Address

Refer to for more information on configuring static IP addresses.

3.3 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 also improves performance. 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.

3.4 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.

3.5 Upgrading eDirectory

3.5.1 Server Health Checks

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

◆ Section B.3.2, "Partitions and Replica Health," on page 151

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, "eDirectory Health Checks," on page 149 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, "eDirectory Health Checks," on page 149.

3.5.2 Upgrading on Linux Servers Other Than OES

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

To upgrade to eDirectory 8.8, use nds-install utility. this utility is located in the Setup directory of the downloaded file for Linux platform. Enter the following command from Setup directory:

```
./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.

NOTE: "ndsconfig upgrade" has to be run after nds-install, if upgrade of the DIB fails and nds-install asks to do so.

3.5.3 Upgrading Through ZENworks Linux Management on OES Linux SP4

eDirectory 8.8 on OES Linux SP4 leverages ZENworks® Linux Management to provide easy upgrade distribution and deployment using the oes-edir88 channel.

For more information on ZENworks Linux Management, refer to ZENworks Linux Management (http://www.novell.com/products/zenworks/linuxmanagement/index.html).

For more information on registering and updating Novell Linux products, refer to Linux Registration and Updates (http://support.novell.com/linux/registration/).

You can upgrade to eDirectory 8.8 on OES Linux SP4 using either of the following methods:

- Through the Command Line Interface
- Through the GUI

Through the Command Line Interface

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

1 Stop the eDirectory server as follows:

```
rcndsd stop or /etc/init.d/ndsd stop
```

2 Upgrade the packages.

    2a Check if the Novell_Update_Server service exists as follows:

```
rug sl
```

    2b (Conditional) If the service is not present, add it as follows:

```
rug sa URL_for_the_service
```

    For example: `rug sa https://update.novell.com/data`

    2c (Conditional) If the service is not activated, activate it as follows:

```
rug act -s service activation_code e-mail_address
```

    For example: `rug act -s 1 oes user@acme.com`

    NOTE: Use the same activation code that you use to get the OES updates.

    2d Subscribe to the oes-edir88 channel.

```
rug sub oes-edir88
```

    NOTE: Ensure that oes-edir88 channel is the only active channel; if not, this can affect the subsequent command by getting more updates than intended. You can verify active channels with the `rug ch` command.

    2e To upgrade to eDirectory 8.8 rpms, enter the following:

```
rug in --entire-channel oes-edir88
```

This command updates all the eDirectory 8.8 packages including `nici`, `yast2-edirectory`, and `novell-edirectory-install`.

2f Unsubscribe from the oes-edir88 channel.

```
rug unsub oes-edir88
```

2g Subscribe to the oes channel.

```
rug sub oes
```

2h Download the 11148 patch.

```
rug pin patch-11148
```

This command installs the updated `yast2-novell-common` file that detects eDirectory 8.7.3 and eDirectory 8.8 versions appropriately. If you install any other eDirectory dependent services from YaST, it demotes to lower eDirectory versions.

3 Export the paths.

You can export the paths either manually or using the ndspath script.

IMPORTANT: `ndspath` works only in `sh` and `bash` shells. In other shells, you need to set the path manually or in your profile scripts.

For example, to export the paths using the ndspath script, enter the following from a command line:

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

NOTE: There is a space between the period and the path. To preserve the path settings permanantly, you can create a `/etc/bash.bashrc.local` file and append the path `. /opt/novell/eDirectory/bin/ndspath` to this file.

---

4 Run `chkconfig -a ndsd`.

5 To initialize NICI, enter the following:

```
ln -sf /var/opt/novell/nici /var/novell/nici
```

To ensure that NICI is set to server mode, enter the following:

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

6 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 to Step 6 into a post-transaction script.

For more information on transactions, refer to the ZENworks Linux Management (http://www.novell.com/documentation/zlm/index.html).

Through the GUI

1 Stop the server as follows:

```
rcndsd stop or /etc/init.d/ndsd stop
```

2 Upgrade the packages.

    2a Invoke ZENworks Linux Management (or Red Carpet)

        1. Go to *System > Configuration > Red Carpet*

        The Red Carpet screen is displayed.

    2b Add a service

        1. Select *Edit > Service*.

        2. (Conditional) In the dialog box that appears, if the Novell_Update_Server service is not present, add it. Click *Add Service* and enter the service URL, for example, https://update.novell.com/data.

    2c (Conditional) If the service is not activated, activate it as follows:

        1. Select *File > Activate*

        2. Select the service name you had added.

        3. Type the e-mail ID.

        4. Type the activation code. For example, oes.

> **NOTE:** Use the same activation code that you use to get the OES updates.

        5. Click on the *Activate* button.

    2d Subscribe to the channel.

        1. Select *Edit > Channel Subscription*.

        2. In the dialog box that appears, select *oes-edir88*.

        3. Click *Close*.

    2e Apply the packages.

        1. Click on the *Available Software* tab and select the oes-edir88 channel.

        All the eDirectory packages are displayed.

        2. Select all the packages.

        3. Click on *Mark for Installation*.

        4. Click on the *Updates* tab and select the `nici, yast2-edirectory,` and `novell-edirectory-install` packages.

        5. Click on *Mark for Installation*.

        6. Click *Run Now*.

        7. Click *Continue* to apply the packages.

    2f Subscribe to the channel.

        1. Select *Edit > Channel Subscription*.

        2. In the dialog box that appears, select *oes*.

        3. Click *Close*.

    2g Apply the patch.

        1. Click on the *Patches* tab.

        2. Scroll down to *patch-11148*.

        3. Click on *Mark for Installation*.

4. Click *Run Now*.

5. Click *Continue* to apply the patch. This updates the `yast2-novell-common` file.

    This command installs the updated `yast2-novell-common` file that detects eDirectory 8.7.3 and eDirectory 8.8 versions appropriately. If you install any other eDirectory dependent services from YaST, it demotes to lower eDirectory versions.

3 Export the paths.

You can export the paths either manually or using the ndspath script.

For example, to export the paths using the ndspath script, enter the following from a command line:

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

NOTE: There is a space between the period and the path. To preserve the path settings permanantly, you can create a `/etc/bash.bashrc.local` file and append the path `. /opt/novell/eDirectory/bin/ndspath` to this file.

---

4 Run `chkconfig -a ndsd`.

5 To initialize NICI, enter the following:

`ln -sf /var/opt/novell/nici /var/novell/nici`

To ensure that NICI is set to server mode, enter the following:

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

6 Run `ndsconfig upgrade`.

NOTE: It is recommended upgrade eDirectory 8.8.*x* to eDirectory 8.8.2 on OES linux 1.0 through the CLI. See "Through the Command Line Interface" on page 64 for more information.

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 to Step 6 into a post-transaction script.

For more information on transactions, refer to the ZENworks Linux Management (http://www.novell.com/documentation/zlm/index.html).

Configuring eDirectory 8.8 Multiple Instances Through YaST After Upgrade

After upgrading 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 *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.

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

5a Select *Existing Tree*.

5b Enter the name of the existing tree.

5c Click *Next*.

The eDirectory Configuration - Existing Tree Information screen is displayed.

5d Enter the hostname along with the NCP and secure LDAP port numbers.

5e Enter the admin FDN.

For example, `cn=admin.o=novell`

5f Enter the password.

5g Click *Next*.

The eDirectory Configuration - Instance Information screen is displayed.

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

7 Specify the NTP and SLP settings.

3.5.4 Upgrading eDirectory During OES 1.0 to OES 2.0 Upgrade

eDirectory should be upgraded when OES upgrades from OES 1.0 to OES 2.0. For more information on OES upgrade, refer to OES Linux Installation Guide (http://www.novell.com/documentation/oes/install_linux/data/bujr8yu.html).

Perform the following checks before upgrading the OES or eDirectory server:

◆ eDirectory Health Check

Ensure that eDirectory health status is normal using the procedures specified in Appendix B, "eDirectory Health Checks," on page 149. You can use the applicable tools for verification:

- ◆ Use iMonitor for eDirectory version prior to 8.8, see Using Novell iMonitor 2.4 (http://www.novell.com/documentation/edir88/edir88/data/acavuil.html#a6l60fc) from *Novell eDirectory 8.8 Administration Guide*.

- ◆ Use ndscheck utility for eDirectory version 8.8 or later, see General Utilities (http://www.novell.com/documentation/edir88/edir88/data/ai33u7x.html) from *Novell eDirectory 8.8 Administration Guide*.

◆ Disk Space Check

For eDirectory version prior to 8.8 SP1, ensure disk space available on the file system that holds the DIB atleast equals the DIB size. For e.g, if the DIB size is 100 MB, the available disk space should not be less than 100 MB.

If the eDirectory health status is not normal or an error is detected, refer to the Section B.5, "Log Files," on page 153.

3.5.5 Upgrading the Tarball Deployment of eDirectory 8.8

If you want to upgrade the Tarball deployment from eDirectory 8.8 to eDirectory 8.8 SP4, perform the following steps:

1 Download the tarball build.

2 Take backup of the following configuration files:
- $NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ndsimon.conf
- $NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ice.conf
- $NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ndsimonhealth.conf
- $NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ndssnmp/ndssnmp.cfg
- $NDSHOME is the location where eDirectory is installed.

3 For upgrade of eDirectory versions lower than 8.8 SP1, do the following:
- Perform disk space check using `ndscheck -D --config-file conf_file_path`
- Create an empty file `upgradeDIB` under the DIB location of each server instance.

  The list of instances can be obtained using the `ndsmanage` utility.

4 Run pre upgrade health check for the all instances using `ndscheck` and check the ndscheck.log file for any errors before proceeding with the upgrade.

5 Stop all instances using `ndmanage`.

6 Untar the tarball in the same location ($NDSHOME) where eDirectory is installed. By untaring the tarball in the same location, we are overwriting the binaries and libraries.

7 Upgrade the following packages if necessary.

Platform	Command	Packages
Linux	• rpm -Uvh <rpm name>	• novell-NOVLsubag-8.8.1-2.i386.rpm
		• nici-2.7.0-0.01.i386.rpm
		NOTE: For more information on installing 32 and 64-bit NICI, refer to the Section 3.6.2, "Installing NICI," on page 59.
		• novell-NDSslp-8.8-1.i386.rpm
Solaris	• Remove the older version using "pkgrm <pkg name>	• NOVLsubag.pkg
	• Install new version using "pkgadd -d <pkg name>"	• NOVLniu0.pkg
		• NDSslp.pkg
AIX	• installp -acgXd <pkg name with full path> <pkg name> all	• NDS.NOVLsubag.8.8.1.0
		• NOVLniu0.2.7.0.0
		• NDS.NDSslp.8.8.1.0

8 Restore the configuration files.

9 Run the `$NDSHOME/eDirectory/opt/novell/eDirectory/bin/ndspath` for setting all environment variables.

10 Run `ndsconfig upgrade -j` for all instances. While running `ndsconfig upgrade` follow the order in which the master replica is the first and followed by R/W and others.

3.5.6 Upgrading Multiple Instances

This section contains the following information:

- "Root User has Multiple Instances" on page 56
- "Non Root User's Instances" on page 56
- "Order of Upgrade" on page 56

Root User has Multiple Instances

If you run nds-install after doing the package upgrade, it will prompt you asking "The DIB of all the Novell eDirectory Server instances need to be upgraded. This may take long time to complete. If you wish to perform the DIB upgrade parallely, you could do it manually (Refer the readme). Do you wish to continue with the DIB upgrade for all the active instances one by one?"

If you select this, it will run "ndsconfig upgrade" for all the instances one by one. In case of larger DIBs, you can select "no" here and run "ndsconfig upgrade" parallely in separate shells. It would help reducing the time of each instances.

Non Root User's Instances

If you have non root user's instances which are using root user's binaries, then before doing the package upgrade you need to run "ndscheck" for all those instances and make sure that their health is proper by referring ndscheck.log. If you run nds-install, it will stop all the instances including non root user's instances. After doing the package upgrade, nds-install won't call "ndsconfig upgrade" for non root user's instances. We need to run "ndsconfig upgrade" for all non root user's instances manually. This will start those instances.

Order of Upgrade

While running "ndsconfig upgrade", we need to follow the order in which master replica comes first and then R/W or other replicas. Otherwise upgrade fails.

3.5.7 Disk Space Check on Upgrading to eDirectory SP4 or later

When eDirectory server is upgraded from previous versions to eDirectory 8.8 SP4 or later, the disk space check for the DIB upgrade would be performed. The free disk space necessary in the file system, where the DIB resides would be equal to that of the DIB size. The messages of the disk space check would be updated in the `ndscheck.log` located in the instance's specific log directory. For default instance, `/var/opt/novell/eDirectory/log/ndscheck.log`.

NOTE: The disk space check is required only during the DIB upgrade process. For more information, refer to Chapter 7, "Upgrade Requirements of eDirectory 8.8," on page 117.

3.6 Installing eDirectory

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

3.6.1 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.
1.2.3.4:524

# 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 155.

3.6.2 Installing NICI

NICI should be installed before you proceed with the eDirectory installation. Both root and nonroot users can install NICI. With eDirectory 8.8.3 version, 32 and 64-bit applications can coexist in a single system. This requires installing both 32 and 64-bit NICI. Use the `--force` option while installing the NICI packages. The command looks like as follows:

```
rpm -ivh --force nici_rpm_file_name_with_path
```

For 32-bit: The command is

```
rpm -ivh --force nici64-2.7.4-0.01.x86.rpm
```

For 64-bit: The command is

```
rpm -ivh --force nici-2.7.4-0.01.i386_64.rpm
```

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 To initialize NICI, enter the following:

```
ln -sf /var/opt/novell/nici /var/novell/nici
```

To ensure that NICI is set to server mode, enter the following:

```
/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 To initialize NICI, enter the following:

```
ln -sf /var/opt/novell/nici /var/novell/nici
```

To ensure that NICI is set to server mode, enter the following:

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

NICI gets installed in the server mode.

3.6.3 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 of 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	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.
	There are two components you can install: the eDirectory server and the eDirectory administration utilities.
	◆ To install the server, enter `-c server`.
	◆ To install the administration utilities, enter `-c admutils`.
	For example, to install Novell eDirectory Server packages, you would enter the following command:
	`./nds-install -c server`
-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, "eDirectory Health Checks," on page 149.
-u	Specifies the option to use in an unattended install mode.
	For unattended install to proceed, you need to enter at least the -c option at the command line, or else the install will abort.

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

2 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-NDSdexvnt novell-NOVLsubag novell-NOVLsnmp novell-NOVLpkit novell-NOVLpkis novell-NOVLpkia novell-NOVLembox novell-NOVLlmgnt novell-NOVLxis novell-NLDAPsdk novell-NLDAPbase novell-NOVLsas novell-NOVLntls novell-NOVLnmas novell-NOVLldif2dib novell-NOVLncp	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-NOVLlmgnt	The Novell Import Conversion Export and LDAP Tools administration utilities are installed on the specified workstation.

3 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.

4 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**

❖ For 32-bit

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

❖ For 64-bit

```
export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib64:/opt/novell/
eDirectory/lib64/nds-modules:/opt/novell/lib64:$LD_LIBRARY_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.

◆ The path exporting instructions should be placed at the end of `/etc/profile` or `~/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.

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 123.

For more information on the nmasinst utility, see "Using the nmasinst Utility to Configure NMAS" on page 80.

3.6.4 Installing Through ZENworks Linux Management on OES Linux SP4

eDirectory 8.8 on OES Linux SP4 leverages ZENworks® Linux Management to provide easy install distribution and deployment using the oes-edir88 channel.

For more information on ZENworks Linux Management, refer to ZENworks Linux Management (http://www.novell.com/products/zenworks/linuxmanagement/index.html).

For more information on registering and updating Novell Linux products, refer to Linux Registration and Updates (http://support.novell.com/linux/registration/).

You can install to eDirectory 8.8 on OES Linux SP4 using either of the following methods:

◆ Through the Command Line Interface
◆ Through the GUI

Through the Command Line Interface

To install through ZENworks Linux Management through your terminal, complete the following steps:

1 Install the packages.

    1a Check if the Novell_Update_Server service exists as follows:

```
rug sl
```

    1b (Conditional) If the service is not present, add it as follows:

```
rug sa URL_for_the_service
```

    For example: `rug sa https://update.novell.com/data`

    1c (Conditional) If the service is not activated, activate it as follows:

```
rug act -s service activation_code e-mail_address
```

    For example: `rug act -s 1 oes user@acme.com`

    NOTE: Use the same activation code that you use to get the OES updates.

    1d Subscribe to the oes-edir88 channel.

```
rug sub oes-edir88
```

    1e To install the eDirectory 8.8 rpms, enter the following:

```
rug in --entire-channel oes-edir88
```

    This command installs all the eDirectory 8.8 packages including `nici`, `yast2-edirectory`, and `novell-edirectory-install`.

    1f Subscribe to the oes channel.

```
rug sub oes
```

    1g Install the 11148 patch.

```
rug pin patch-11148
```

    This command installs the updated `yast2-novell-common` file that detects eDirectory 8.7.3 and eDirectory 8.8 versions appropriately. If you install any other eDirectory dependent services from YaST, it demotes to lower eDirectory versions.

2 Export the paths.

You can export the paths either manually or using the ndspath script.

For example, to export the paths using the ndspath script, enter the following from a command line:

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

NOTE: There is a space between the period and the path. To preserve the path settings permanantly, you can create a `/etc/bash.bashrc.local` file and append the path `. /opt/novell/eDirectory/bin/ndspath` to this file.

3 Run `chkconfig -a ndsd`

4 To initialize NICI, enter the following:

```
ln -sf /var/opt/novell/nici /var/novell/nici
```

To ensure that NICI is set to server mode, enter the following:

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

5 Run `ndsconfig add`.

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

For more information on transactions, refer to the ZENworks Linux Management (http://www.novell.com/documentation/zlm/index.html).

Through the GUI

1 Install the packages.

    1a Invoke ZENworks Linux Management (or Red Carpet)

        1. Go to *System > Configuration > Red Carpet*

        The Red Carpet screen is displayed.

    1b Add a service

        1. Select *Edit > Service*.

        2. (Conditional) In the dialog box that appears, if the Novell_Update_Server service is not present, add it. Click *Add Service* and enter the service URL, for example, https://update.novell.com/data.

    1c (Conditional) If the service is not activated, activate it as follows:

        1. Select *File > Activate*

        2. Select the service name you had added.

        3. Type the e-mail ID.

        4. Type the activation code. For example, oes.

> **NOTE:** Use the same activation code that you use to get the OES updates.

        5. Click on the *Activate* button.

    1d Subscribe to the channel.

        1. Select *Edit > Channel Subscription*.

        2. In the dialog box that appears, select *oes-edir88*.

        3. Click *Close*.

    1e Apply the packages.

        1. Click on the *Available Software* tab and select the oes-edir88 channel.

        All the eDirectory packages are displayed.

        2. Select all the packages.

        3. Click on *Mark for Installation*.

        4. Click on the *Updates* tab and select the `nici, yast2-edirectory`, and `novell-edirectory-install` packages.

        5. Click on *Mark for Installation*.

6. Click *Run Now*.

7. Click *Continue* to apply the packages.

1f Subscribe to the channel.

1. Select *Edit > Channel Subscription*.

2. In the dialog box that appears, select *oes*.

3. Click *Close*.

1g Apply the patch.

1. Click on the *Patches* tab.

2. Scroll down to *patch-11148*.

3. Click on *Mark for Installation*.

4. Click *Run Now*.

5. Click *Continue* to apply the patch. This updates the yast2-novell-common file.

   This command installs the updated `yast2-novell-common` file that detects eDirectory 8.7.3 and eDirectory 8.8 versions appropriately. If you install any other eDirectory dependent services from YaST, it demotes to lower eDirectory versions.

2 Export the paths.

You can export the paths either manually or using the ndspath script.

For example, to export the paths using the ndspath script, enter the following from a command line:

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

NOTE: There is a space between the period and the path. To preserve the path settings permanantly, you can create a `/etc/bash.bashrc.local` file and append the path `. /opt/novell/eDirectory/bin/ndspath` to this file.

---

3 Run `chkconfig -a ndsd`.

4 To initialize NICI, enter the following:

```
ln -sf /var/opt/novell/nici /var/novell/nici
```

To ensure that NICI is set to server mode, enter the following:

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

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

For more information on transactions, refer to the ZENworks Linux Management (http://www.novell.com/documentation/zlm/index.html).

Configuring eDirectory 8.8 Through YaST After Upgrade

After installing the packages, configure eDirectory 8.8 as follows:

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

2 Select *eDirectory*.

This invokes the eDirectory configuration.

Configuring eDirectory 8.8 Multiple Instances Through YaST After Upgrade

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 *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.

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

5a Select *Existing Tree*.

5b Enter the name of the existing tree.

5c Click *Next*.

The eDirectory Configuration - Existing Tree Information screen is displayed.

5d Enter the hostname along with the NCP and secure LDAP port numbers.

5e Enter the admin FDN.

For example, `cn=admin.o=novell`

5f Enter the password.

5g Click *Next*.

The eDirectory Configuration - Instance Information screen is displayed.

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

7 Specify the NTP and SLP settings.

3.6.5 Nonroot User Installing eDirectory 8.8

A nonroot user can install eDirectory 8.8 using the tarball.

Prerequisites

❑ Ensure that NICI is installed.

For information on installing NICI, refer to Section 3.6.2, "Installing NICI," on page 59.

❑ Ensure that SNMP subagent is installed using the command "rpm --nodeps <path of snmp subagent rpm>".

❑ 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 Section 3.2, "Prerequisites," on page 46 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**

◆ For 32-bit

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

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

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

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

◆ For 64-bit

```
export LD_LIBRARY_PATH=custom_location/eDirectory/opt/novell/
eDirectory/lib64:custom_location/eDirectory/opt/novell/eDirectory/
lib64/nds-modules:custom_location/eDirectory/opt/novell/
lib64:$LD_LIBRARY_PATH
```

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

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


export TEXTDOMAINDIR=custom_location/eDirectory/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, prefix the ndspath script to the utility.

    - Run the utility you want as follows:

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

    - Export the paths in the current shell as follows :

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

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

    After entering the above commands, 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>] [-w
<admin password>] [-i] [-S <server_name>] [-d <path_for_dib>] [-m
<module>] [e] [-L <ldap_port>] [-l <SSL_port>] [-o <http_port>] -O
<https_port>] [-p <IP address:[port]>] [-c] [-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 76.

Follow the onscreen instructions to complete the configuration.

For more information, see Section 3.6.6, "Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 70.

IMPORTANT: Security Services cannot be updated separately with the tarball installation of eDirectory unlike the package installs. For tarball installation, the security updates can be obtained only through eDirectory support packs.

3.6.6 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 123.

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>] [-p <IP address:[port]>] [-R] [-c] [-w
<admin password>] [-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>] [-w <admin
password>] [-c] [-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>] [-w <admin
password>] [-e] [-P <LDAP URL(s)>][-L <ldap port>] [-l <SSL port>] [-o <http port>]
[-O <https port>] [-S <server name>] [-d <path for dib>] [-m <module>] [-p <IP
address:[port]>] [-R] [-c] [-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>] [-w <admin password>] [-p <IP address:[port]>] [-c]
```

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 from `/var/opt/novell/eDirectory/data/dsreports` 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. Also adds LDAP and SAS services, after eDirectory has been configured in the existing tree.
rm	Removes the Server object and directory services from a tree.
upgrade	Upgrades eDirectory to a later version.
-i	While configuring a new tree, ignores checking whether a tree of the same name exists. Multiple trees of the same name can exist.
-S server name	Specifies the server name. The server name can also contain dots (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 UNIX server using "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 '.' 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 cannot start a name with a dot. For example, you cannot install a server that has the name ".novell", because it starts with a dot ('.').
-t treename	The tree name to which the server has to be added. It can have a maximum of 32 characters. If not specified, ndsconfig takes the tree name from the n4u.nds.tree-name parameter that is specified in the /etc/opt/novell/eDirectory/conf/nds.conf file. The default treename is $LOGNAME-$HOSTNAME-NDStree.
-n server context	Specifies the context of the server in which the server object is added. It can have a maximum of 64 characters. If the context is not specified, ndsconfig takes the context from the configuration parameter n4u.nds.server-context specified in the /etc/opt/novell/eDirectory/conf/nds.conf file. The server context should be specified in the typed form. The default context is org.
-d path for dib	The directory path where the database files will be stored.
-L ldap_port	Specifies the TCP port number on the LDAP server. If the default port 389 is already in use, it prompts for a new port.
-l ssl_port	Specifies the SSL port number on the LDAP server. If the default port 636 is already in use, it prompts for a new port.

ndsconfig Parameter	Description
-a admin FDN	Specifies the fully distinguished name of the User object with Supervisor rights to the context in which the server object and Directory services are to be created. The admin name should be specified in the typed form. It can have a maximum of 64 characters. The default admin name is admin.org.
-e	Enables clear text passwords for LDAP objects.
-m modulename	Specifies the module name to configure. While configuring a new tree, you can configure only the ds module. After configuring the ds module, you can add the NMAS, LDAP, SAS, SNMP, HTTP services, and Novell SecretStore (ss) using the add command. If the module name is not specified, all the modules are installed.
-o	Specifies the HTTP clear port number.
-O	Specifies the HTTP secure port number.
-p <IP address:[port]>	This option is used for secondary server addition ('add' command) to a tree. It specifies the IP address of the remote host that holds a replica of the partition to which this server is being added. The default port number is 524. This helps in faster lookup of the tree since it avoids SLP lookup.
-R	By default a replica of the partition to which the server is added would be replicated to the local server. This option disallows adding replicas to the local server.
-c	This option avoids prompts during ndsconfig operation, such as yes/no to continue the operation, or prompt to re-enter port numbers when there is a conflict, etc. The user receives prompts only for entering mandatory parameters if they are not passed on command line.
-w <admin password>	This option allows passing the admin user password in clear text. **NOTE:** Since password is passed in clear text, this is not recomended as a safe option owing to password insecurity.
-E	Enables encrypted replication for the server you are trying to add.
-j	Jumps or overrides the health check option before installing eDirectory.
-b port to bind	Sets the default port number on which a particular instance should listen on. This sets the default port number on n4u.server.tcp-port and n4u.server.udp-port. If an NCP port is passed using the -b option, then it is assumed to be the default port and the TCP and UDP params are updated accordingly. **NOTE:** -b and -B are exclusively used.
-B interface1@port1, interface2@port2,...	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.

ndsconfig Parameter	Description
--config-file configuration file	Specify the absolute path and file name to store the nds.conf configuration file. For example, to store the configuration file in the `/etc/opt/novell/eDirectory/ directory`, enter `--config-file /etc/opt/novell/eDirectory/ nds.conf`.
-P <LDAP URL(s)>	Allows the LDAP URLs to configure the LDAP interface on the LDAP Server object. For example: -P ldap://1.2.3.4:1389,ldaps://1.2.3.4:1636
-D path_for_dat a	Creates the `data`, `dib`, and `log` directories in the path mentioned.
set valuelist	Sets the value for the specified eDirectory configurable parameters. It is used to set the bootstrapping parameters before configuring a tree. When configuration parameters are changed, ndsd needs to be restarted for the new value to take effect. However, for some configuration paramters, ndsd need not be restarted. These paramters are listed below: • n4u.nds.inactivity-synchronization-interval • n4u.nds.synchronization-restrictions • n4u.nds.janitor-interval • n4u.nds.backlink-interval • n4u.nds.drl-interval • n4u.nds.flatcleaning-interval • n4u.nds.server-state-up-threshold • n4u.nds.heartbeat-schema • n4u.nds.heartbeat-data
get help paramlist	Use to view the help strings for the specified eDirectory configurable parameters. If the parameter list is not specified, ndsconfig lists the help strings for all the eDirectory configurable parameters.
set valuelist	Sets the value for the specified eDirectory configurable parameters. It is used to set the bootstrapping parameters before configuring a tree. When configuration parameters are changed, ndsd needs to be restarted for the new value to take effect.
get paramlist	Use to view the current value of the specified eDirectory configurable parameters. If the parameter list is not specified, ndsconfig lists all the eDirectory configurable parameters.

3.6.7 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.

- Unique server name for the instance

  You can use the ndsconfig -S server name option to do this.

IMPORTANT: During eDirectory configuration, the default NCP server name is set as the host server name. When configuring multiple instances, you must change NCP server name. Use the `ndsconfig` command line option, `-S <server_name>` to specify a different server name.

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 76.

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

IMPORTANT: The *install_location*/etc/opt/novell/eDirectory/conf directory contains some of the critical configuration information used for tracking and managing the eDirectory instances running on your server. Do not remove any contents from this directory.

This sections explains the following:

- "The ndsmanage Utility" on page 75
- "Listing the Instances" on page 76
- "Creating an Instance through ndsmanage" on page 76
- "Performing Operations for a Specific Instance" on page 77

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 3-1   *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 *username*	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 3-1 on page 76 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 3-1   *ndsmanage Utility Output Screen*


```
osg-dt-srv27(/space/kprajesh)>
osg-dt-srv27(/space/kprajesh)>ndsmanage
Server instances management utility for Novell eDirectory 8.8 SP 2 v20215.27

The following are the instances configured by root

[1] /etc/opt/novell/eDirectory/conf/nds.conf : .OSG-DT-SRV27.NOVELL.SOLAIX_SNMP_BUG. : 100.1.2.6@524 : ACTIVE

[2] /space/kprajesh/1srv/etc/nds.conf : .OSG-DT-SRV27.NOVELL.KPR-SOL2. : eri0@1524 : ACTIVE

Enter [r] to refresh list, [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:

-
-
-

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 3-2 *ndsmanage Utility Output Screen with Instance Options*

```
osg-dt-srv27(/space/kprajesh)>ndsmanage root
Server instances management utility for Novell eDirectory 8.8 SP 2 v20215.27

The following are the instances configured by root

[1] /etc/opt/novell/eDirectory/conf/nds.conf : .OSG-DT-SRV27.NOVELL.SOLAIX_SNMP_BUG. : 100.1.2.6@524 : ACTIVE

[2] /space/kprajesh/1srv/etc/nds.conf : .OSG-DT-SRV27.NOVELL.KPR-SOL2. : eri0@1524 : ACTIVE

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

SELECTED INSTANCE:
[1] /etc/opt/novell/eDirectory/conf/nds.conf : .OSG-DT-SRV27.NOVELL.SOLAIX_SNMP_BUG. : 100.1.2.6@524 : ACTIVE

[l] List the replicas on the server
[s] Start the instance
[k] Stop the instance
[t] Run ndstrace
[d] Deconfigure
[b] Back to previous menu
[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 77).

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 77).

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 77.

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 77.

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
```

NOTE: On UNIX/Linux, OS restricts sockets creation on the mounted file system. The same restriction is applicable to NSS volumes. With eDirectory, its always recommended to have the var directory on the local file system (-D option with ndsconfig) and DIB directory can be of any file system (-d option with ndsconfig).

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
  ```

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

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

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

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

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

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

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

3.6.9 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, and AIX systems to configure NMAS.

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

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

- "Configuring NMAS" on page 80
- "Installing Login Methods" on page 81

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*.

3.6.10 Nonroot user SNMP configuration

NICI and NOVLsubag should be installed as root user.

1 Root User Installing NICI. Refer to "Root User Installing NICI" on page 59

2 Root User Installing NOVLsubag.

   To install NOVLsubag, complete the following procedure:

   Enter the following command:

   ```
   rpm -ivh --nodeps NOVLsubag_rpm_file_name_with_path
   ```
   For example:

   ```
   rpm -ivh --nodeps novell-NOVLsubag-8.8.1-5.i386.rpm
   ```

3 Export the paths as follows:

Manually export the environment variables.

- ◆ For 32-bit

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

- ◆ For 64-bit

```
export LD_LIBRARY_PATH=custom_location/opt/novell/eDirectory/lib64:/opt/
novell/eDirectory/lib64/nds-modules:/opt/novell/lib64:$LD_LIBRARY_PATH
```

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

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

Installing or Upgrading Novell eDirectory on Solaris

<div style="text-align: right">

4

</div>

Use the following information to install or upgrade Novell® eDirectory™ 8.8 on a Solaris* server:

- Section 4.1, "System Requirements," on page 83
- Section 4.2, "Prerequisites," on page 84
- Section 4.3, "Hardware Requirements," on page 85
- Section 4.4, "Forcing the Backlink Process to Run," on page 85
- Section 4.5, "Upgrading eDirectory," on page 86
- Section 4.6, "Installing eDirectory," on page 86

4.1 System Requirements

- ❑ One of the following:
  - ◆ Solaris* 9 and 10 on Sun SPARC
- ❑ Update your system with the following libumem patches:
  - ◆ Sun OS 5.9: libumem library patch for Solaris 9 on SPARC
    - ◆ Patch Id 114370-05
  - ◆ Sun OS 5.10: libumem library patch for Solaris 10 on SPARC
    - ◆ Patch Id 121921-02

> **NOTE:** All latest recommended set of patches are 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

4.2 Prerequisites

IMPORTANT: Check the currently installed Novell and Third Party applications to determine if eDirectory 8.8 is supported before upgrading your existing eDirectory environment. You can find out the current status for Novell products in the TID - What Novell products are supported with Novell eDirectory 8.8? (http://support.novell.com/cgi-bin/search/searchtid.cgi?10099872.htm). We also highly recommend you to back up eDirectory before any upgrades.

❑ (Conditional) NICI 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 8.8eDirectory 8.8. In addition, every workstation using the management utilities, for example, iManager and ConsoleOne, must have NICI 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 NICI 2.7 is named `NOVLniu0-2.7` on Solaris.

For more information, refer to Section 4.6.3, "Installing NICI," on page 88.

❑ 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 87.

❑ 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, or AIX 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) 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.

❑ (Conditional) If you are installing a secondary server into an existing tree as a nonadministrator user, ensure that at least one of the servers in the tree has the same or higher eDirectory version as that of the secondary being added as container admin. In case the secondary being added is of later version, then the schema needs to be extended by the admin of the tree before adding the secondary using container admin.

Configuring Static IP Address

Refer to for more information on configuring static IP addresses.

4.3 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.

4.4 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.

4.5 Upgrading eDirectory

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

```
./nds-install
```

NOTE: Upgrade LUM 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` is renamed to `/etc/nds.conf_pre88` and the old log files under `/var/nds` are retained for reference.

NOTE: "ndsconfig upgrade" has to be run after nds-install, if upgrade of the DIB fails and nds-install asks to do so.

4.5.1 Upgrading Multiple Instances

For information on Upgrading Multiple Instances, refer to Section 3.5.6, "Upgrading Multiple Instances," on page 56 in the Linux chapter.

4.5.2 Upgrading the Tarball Deployment of eDirectory 8.8

For information on Upgrading the Tarball Deployment of eDirectory 8.8, refer to Section 3.5.5, "Upgrading the Tarball Deployment of eDirectory 8.8," on page 55 in the Linux chapter.

4.6 Installing eDirectory

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

- Section 4.6.1, "Server Health Checks," on page 87
- Section 4.6.2, "Using SLP with eDirectory," on page 87

4.6.1 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.

 - Section B.3.1, "Basic Server Health," on page 150
 - Section B.3.2, "Partitions and Replica Health," on page 151

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, "eDirectory Health Checks," on page 149 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, "eDirectory Health Checks," on page 149.

4.6.2 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/NDSslp.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 57 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 155.

4.6.3 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:

```
pkgadd -d NICI_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/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/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 NICI:

1 Log in as john and execute the following command:

sudo pkgadd -d *absolute_path_of_the_NICI_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

NICI gets installed in the server mode.

4.6.4 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 Section 4.6.5, "Nonroot User Installing eDirectory 8.8," on page 92.

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	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.
	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.
	For example, to install Novell eDirectory Server packages, you would enter the following command:
	`./nds-install -c server -n /var`
-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, "eDirectory Health Checks," on page 149.
-u	Specifies the option to use an unattended install mode.

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

2 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 NOVLlmgnt NOVLxis NLDAPsdk NLDAPbase NOVLsas NOVLntls NOVLnmas NOVLldif2dib NOVLncp	The eDirectory replica server is installed on the specified server.
Administration Utilities	NOVLice NDSbase NLDAPbase NLDAPsdk NOVLpkia NOVLxis NOVLlmgnt	The Novell Import Conversion Export and LDAP Tools administration utilities are installed on the specified workstation.

3 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.

Novell Modular Authentication Service™ (NMAS™) is installed as part of the server component. By default, ndsconfig configures NMAS. 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 123.

For more information on the nmasinst utility, see "Using the Nmasinst Utility to Configure NMAS" on page 96.

4 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.

4.6.5 Nonroot User Installing eDirectory 8.8

A nonroot user can install eDirectory 8.8 using the tarball.

Prerequisites

❑ Ensure that NICI is installed.

  For information on installing NICI, refer to Section 4.6.3, "Installing NICI," on page 88.

❑ 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 Section 4.2, "Prerequisites," on page 84 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/eDirectory/opt/
  novell/eDirectory/lib:custom_location/eDirectory/opt/novell/
  eDirectory/lib/nds-modules:custom_location/eDirectory/opt/
  ```

```
novell/lib:/opt/novell/lib:/opt/novell/eDirectory/
lib:$LD_LIBRARY_PATH
```

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

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

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

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

   Prefix the ndspath script to the utility if you do not want to export the paths manually.

   - ◆ Run the utility you want as follows:

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

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

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

      NOTE: Ensure that you enter the above commands from the `custom_location/`
      `eDirectory/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 76.

Follow the onscreen instructions to complete the configuration.

For more information, see Section 4.6.6, "Using the Ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 94.

4.6.6 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 123.

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 from /var/opt/novell/eDirectory/data/dsreports 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

Refer to "ndsconfig Utility Parameters" on page 72 for more information.

4.6.7 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 Section 3.6.7, "Using ndsconfig to Configure Multiple Instances of eDirectory 8.8," on page 74 in the Linux chapter.

4.6.8 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.

4.6.9 Using the Nmasinst Utility to Configure NMAS

For eDirectory 8.8, by default, ndsconfig configures NMAS. You can also use nmasinst on Linux, Solaris, and AIX systems to configure NMAS.

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

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

- ◆ "Configuring NMAS" on page 96
- ◆ "Installing Login Methods" on page 97

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*.

4.6.10 Nonroot user SNMP configuration

NICI and NOVLsubag should be installed as root user.

1 Root User Installing NICI. Refer to Section 4.6.3, "Installing NICI," on page 88.

2 Install NOVLsubag as root.

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/lib:/opt/novell/lib:/
opt/novell/eDirectory/lib:$LD_LIBRARY_PATH


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


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

Installing or Upgrading Novell eDirectory on AIX

5

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

5.1 System Requirements

- ❑ AIX 5L Version 5.3
- ❑ 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

5.2 Prerequisites

IMPORTANT: Check the currently installed Novell and Third Party applications to determine if eDirectory 8.8 is supported before upgrading your existing eDirectory environment. You can find out the current status for Novell products in the TID - What Novell products are supported with Novell eDirectory 8.8? (http://support.novell.com/cgi-bin/search/searchtid.cgi?10099872.htm). We also highly recommend you to back up eDirectory before any upgrades.

- ❑ 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) NICI 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 NICI 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 NICI 2.7 is named `NOVLniu0-2.7` on AIX. For more information, refer to Section 5.6.3, "Installing NICI," on page 104.

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

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

❑ (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) 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.

❑ (Conditional) If you are installing a secondary server into an existing tree as a nonadministrator user, ensure that at least one of the servers in the tree has the same or higher eDirectory version as that of the secondary being added as container admin. In case the secondary being added is of later version, then the schema needs to be extended by the admin of the tree before adding the secondary using container admin.

Configuring Static IP Address

Refer to "Configuring Static IP Address" on page 12 for more information on configuring static IP addresses.

5.3 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.

5.4 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.

5.5 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` is renamed to `/etc/nds.conf_pre88` and the old log files under `/var/nds` are retained for reference.

NOTE: "ndsconfuiig upgrade" has to be run after nds-install, if upgrade of the DIB fails and nds-install asks to do so.

5.5.1 Upgrading Multiple Instances

For information on Upgrading Multiple Instances, refer to Section 3.5.6, "Upgrading Multiple Instances," on page 56 in the Linux chapter.

5.5.2 Upgrading the Tarball Deployment of eDirectory 8.8

For information on Upgrading the Tarball Deployment of eDirectory 8.8, refer to Section 3.5.5, "Upgrading the Tarball Deployment of eDirectory 8.8," on page 55 in the Linux chapter.

5.6 Installing eDirectory

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

- Section 5.6.1, "Server Health Checks," on page 102
- Section 5.6.2, "Using SLP with eDirectory," on page 103
- Section 5.6.3, "Installing NICI," on page 104
- Section 5.6.4, "Using the Nds-install Utility to Install eDirectory Components," on page 105
- Section 5.6.5, "Nonroot User Installing eDirectory 8.8," on page 107
- Section 5.6.6, "Using the Ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 109
- Section 5.6.7, "Using ndsconfig to Configure Multiple Instances of eDirectory 8.8," on page 111
- Section 5.6.8, "Using Ndsconfig to Install an AIX Server into a Tree with Dotted Name Containers," on page 111
- Section 5.6.9, "Using the Nmasinst Utility to Configure NMAS," on page 111
- Section 5.6.10, "nonroot user SNMP configuration," on page 112

5.6.1 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.

- Section B.3.1, "Basic Server Health," on page 150
- Section B.3.2, "Partitions and Replica Health," on page 151

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, "eDirectory Health Checks," on page 149 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, "eDirectory Health Checks," on page 149.

5.6.2 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 57 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 155.

5.6.3 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.

5.6.4 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	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.
	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.
	For example, to install Novell eDirectory Server packages, you would enter the following command:
	`./nds-install -c server -n /var`
-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, "eDirectory Health Checks," on page 149.
-u	Specifies the option to use an unattended install mode.

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

2 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 NOVLembox NOVLlmgnt NOVLxis NLDAPsdk NLDAPbase NOVLsas NOVLntls NOVLnmas NOVLldif2dib NOVLncp	The eDirectory replica server is installed on the specified server.
Administration Utilities	NOVLice NDSbase NLDAPbase NLDAPsdk NOVLpkia NOVLxis NOVLlmgnt	The Novell Import Conversion Export and LDAP Tools administration utilities are installed on the specified workstation.

3 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.

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 123.

For more information on the nmasinst utility, see .

4 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.

5.6.5 Nonroot User Installing eDirectory 8.8

A nonroot user can install eDirectory 8.8 using the tarball.

Prerequisites

❑ Ensure that NICI is installed.

For information on installing NICI, refer to .

❑ 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 section.

Installing eDirectory

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

2 Untar the tar file as follows:

```
tar xvfp /tar_file_name
```

3 Export the paths as follows:

- ◆ **Manually export the environment variables**

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

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

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

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

  ```
  export TEXTDOMAINDIR=custom_location/eDirectory/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/eDirectory/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/eDirectory/opt/novell/eDirectory/bin/ndspath
    utility_name_with_parameters
    ```

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

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

    NOTE: Ensure that you enter the above command from the `custom_location/eDirectory/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 76.

Follow the onscreen instructions to complete the configuration.

For more information, see Section 5.6.6, "Using the Ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 109.

5.6.6 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 123.

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 from `/var/opt/novell/eDirectory/data/dsreports` 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

Refer to for more information.

5.6.7 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 in the Linux chapter.

5.6.8 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.

5.6.9 Using the Nmasinst Utility to Configure NMAS

For eDirectory 8.8, by default, ndsconfig configures NMAS. You can also use nmasinst on Linux, Solaris, and AIX systems to configure NMAS.

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

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

- "Configuring NMAS" on page 112
- "Installing Login Methods" on page 112

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*.

5.6.10 nonroot user SNMP configuration

NICI and NOVLsubag should be installed as root user.

1 Root User Installing NICI. Refer to Section 5.6.3, "Installing NICI," on page 104.

2 Install NOVLsubag as root.

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/lib:/opt/novell/lib:/
opt/novell/eDirectory/lib:$LD_LIBRARY_PATH

export   PATH=/opt/novell/eDirectory/bin:$PATH
export MANPATH=/opt/novell/:$MANPATH
```

Relocating the DIB

6

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.

6.1 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
```

6.2 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.

Upgrade Requirements of eDirectory 8.8

7

One of the unique features of eDirectory is its ability to maintain the tight referential integrity. Any object Classes derived from Top will have a reference attribute in its class definition. This is a hidden attribute added to all the referenced objects that are internally maintained by eDirectory. Background processes keep running to check the links between the referenced object and the referencing objects.

If the referenced object is from a different partition than the one held locally in the server, an external reference to that object will be created locally in the external reference partition. An external reference is a representation of an object existing in the eDirectory tree; however, it is not a copy of the object and its assigned attributes.

Though we can remove the Reference attribute from eDirectory, currently, the class definitions are untouched to maintain the backward compatibility in the tree.

Figure 7-1   *iMonitor Output showing References to an Object*

This chapter explains the changes and possible upgrade scenarios in eDirectory 8.8.

7.1 Reference Changes in 8.8 SP4

The reference attribute is a hidden attribute and is maintained on each referenced object. This is created and maintained by DS. The new referencing code in DS is based on a FLAIM index called `LocalEntryIDIndex` that DS creates. Though FLAIM maintains the index, the usage is determined by DS. FLAIM automatically updates the index when a DN value is added or deleted. Each key in the index is a compound key, i.e, DN of the object being referenced + Entry ID of the referencing object. For example, if there is an object with Entry ID 343, and it has a "member" value that points to object #899, FLAIM will automatically generate a key in the index of 899+343.

DS can now do lookups in the index to find all the objects pointing to object #899. Object #899 does not have to keep a reference attribute on itself to remember all the objects referencing it. Actually, FLAIM maintains the index without knowing how it is used, but DS has the code that knows how to use the index.

However, the new way of maintaining references requires a database upgrade when the existing eDirectory instance is upgraded to 8.8 SP4. The upgrade requires the creation of a new index; which will require traversing each entry in the database. It also requires the removal of all of the "reference" attributes from each entry in the database. In addition, some internal octet string attributes used by DS that had embedded DNs would need to generate some new DN values to store alongside the octet string value. All this would be a time consuming process on a large database. Since DS is changed to do referential integrity using new FLAIM feature, and that depends on the new index, there is no way DS can really operate until the conversion is complete - so the first time an existing database is opened, all reference attributes need to be changed to a new index. It could take hours before it actually opens and is ready for use by applications for a large database.

7.2 Upgrade Process in 8.8 SP4

As stated above, eDirectory database will be upgraded to a new format when SP4 is installed.

The appropriate upgrade utility will be called after the packages are upgraded to eDirectory 8.8. Refer to the eDirectory install and upgrade documents in *Novell eDirectory 8.8 Installation Guide* (http://www.novell.com/documentation/edir88/index.html)

A new offline database upgrade utility will be available with eDirectory 8.8.

NOTE: Incase the administrator wants to run the utility and find out the status of the upgrade, this database upgrade tool can be used with a copy of the database or with `-d` option

Unix/Linux	NetWare	Windows
`ndsdibupg`	`dsdibupg.nlm`	`ndsdibupg.exe`

Figure 7-2   *ndsdibupg Help Screen*

The following table discusses the ndsdibupg options.

Table 7-1   *ndsdibupg Options*

Option	Description
-q	Quiet mode. There will not be any messages in quiet mode. Messages will be logged to log file (if provided) even in -q mode. It is recommended that you always provide a log file name for troubleshooting purpose.
-d	Dry run. Upgrade will be performed on a copy of the actual database. This option is more useful in NetWare where the database location can not be changed. The last argument – database path - of this utility will not have any effect on NetWare platforms.
	IMPORTANT: ds.nlm should be unloaded before loading dsdibup.nlm.
	This option can be used if the administrator wants to know if the upgrade is going to be successful and also to estimate the time required to upgrade the database. It is recommended to take a copy of the DIB.
	NOTE: eDirectory service should be unloaded or stopped before taking a copy of the database. ndsdibupg utility can be run on the copied database to estimate the downtime required for the actual upgrade. During this time, eDirectory service can be loaded or restarted.
-v	Verbosity of the messages. The default value is 3 where all messages are logged. It is recommended to always leave the verbosity level to its default value.

Option	Description
-l	Provide a log file name where messages are logged during upgrade. The log file will indicate the time the upgrade started and the end time. Given below is a snapshot of log file.

```
Utility called with dir: /var/opt/novell/eDirectory/data/dib
     options
        Log File: /var/opt/novell/eDirectory/log/ndsdibupg.log
DIB upgrade starting: May 02 10:27:02
Open the dib to start upgrade process...
Total DIB size: 45 MB
Failed to open the dib, Traying limited mode...
QUERY CRITERIA:
    FLD:30 == 4278190110
  AND
    FLD:33.34 == "Reference"
  {OptInfo: UsingIX=143, KeyMatch=YES, RecMatch=NO, FromKeyLen=16, FromKey={1F F
F 00:2 1E 02 99 87 88 87 99 87 93 83 87 05}, UntilKeyLen=16, UntilExcl=Yes, Unti
lKey={1F FF 00:2 1E 02 99 87 88 87 99 87 93 83 87 07}}
  {Stats: Container=32001, Matched=1, KeysFailed=0 of 1, RefsFailed=0 of 1}

QUERY CRITERIA: (<empty>) {OptInfo: Full Container Scan}
    {Stats: Container=2, Matched=662, RecsFetched=662, RecsRejected=0, RecsNotFo
und=0}

#                                                 3
.
.
.
##################################################  100
Indexing progress: Index 210 is offline.  Last record processed = 33671.
Indexing progress: Index 210 is offline.  Last record processed = 33672.
Indexing progress: Index 210 is offline.  Last record processed = 35030.
Indexing progress: Index 210 is offline.  Last record processed = 35031.
Indexing progress: Index 210 is offline.  Last record processed = 35073.
Upgrade process completed (May 02 10:27:49 ).  Status: 0x0
```

7.3 Performing a Dry Run before Upgrading eDirectory

ndsdibupg can be used to perform a dry run before upgrading the packages. This utility alone can be used against a copied database on non-NetWare platforms. The advantage is that eDirectory services will still be available when the dry run is being performed.

It is not possible to copy of the DIB and perform the dry run on NetWare when DS.NLM is loaded. Here, -d option can be used where the upgrade utility itself takes a copy of the DIB and performs the upgrade on the copy. ds.nlm should be unloaded while copying the database to ensure the integrity of the database. Upgrade will require twice the size of the database since a copy needs to be taken.

Figure 7-3 *Upgrade Process*
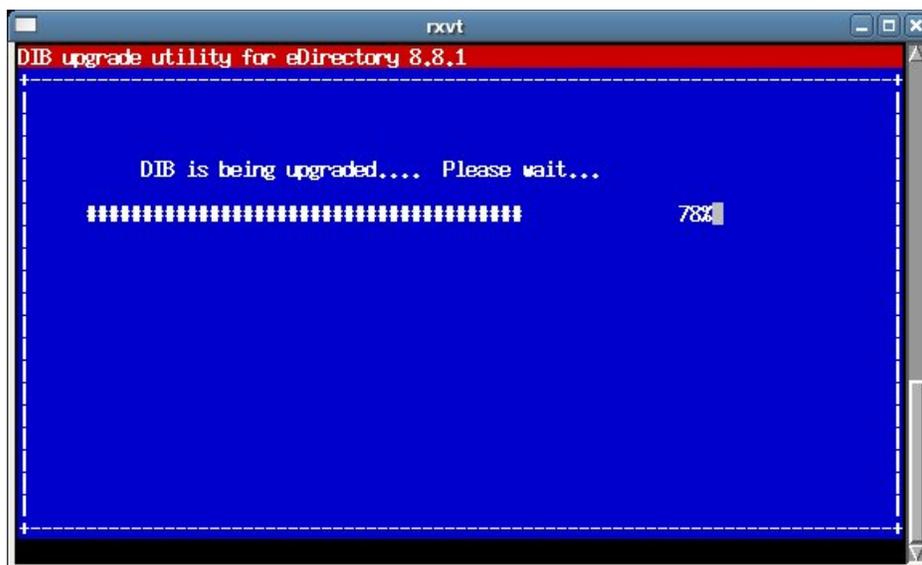
7.3.1 Common Problems Encountered during the Upgrade Process

The following FAQ section discusses the common problems faced while upgrading from the previous versions of eDirectory to eDirectory 8.8.

Question: I am upgrading from eDirectory 8.7.x to eDirectory 8.8. The upgrade process failed with an error. My eDirectory 8.7.x server no longer comes up.

Answer: While upgrading from 8.7.*x* to eDirectory 8.8, the database goes through a two phase upgrade. In the first phase, a key pair is created for encrypted attributes support which was introduced in eDirectory 8.8. In the second phase, DIB upgrade happens for reference changes. Incase the second phase fails after the first phase, the existing binaries (eDirectory 8.7.*x*) will not be able to open the database as database is already upgraded to 8.8 level and the database version is changed to reflect that. We recommend taking a backup of the database before proceeding with upgrading to eDirectory 8.8. Please refer to Section 9.2, "Migrating to eDirectory 8.8 SP4 Without Upgrading the Operating System," on page 133 for further details.

Question: The upgrade process seems to be taking a lot of time.

Answer: The upgrade scanns the entire database and checks for reference attributes on all the objects. This process might take a while depending on the number of the objects in the database. It may take hours for a database with 5 million objects with reference attributes on all the objects.

Question: The upgrade process seems to be taking a lot of space in the storage.

Answer: Since the entire reference upgrade has to be done in a single transaction and transaction rollback is required in case the upgrade fails, flaim keeps the changed blocks in its nds.db file. As a result of this, you might observe the nds.db growing during the upgrade process. This is quite normal. The file might spill over to nds.00v, nds.002, etc. The upgrade process will require as much

as 100% of existing disk space depending on the number of objects to be upgraded. For e.g, a DIB size of 15Gig might require another 15Gig free space, if all objects in the DIB has reference attributes.

Question: The eDirectory database upgrade proceeds even if I provide a wrong password and admin user.

Answer: eDirectory package upgrade and database upgrade happens based on your file system rights. The eDirectory administrator password will not be used for this. It has a side effect that the login might fail once the upgrade begins. The next attempt of "ndsconfig upgrade" will always go through.

Question: I provided a wrong password for administrator. My upgrade failed, and I started the upgrade again with the correct password. The upgrade is again taking long time (as long as 1 hour for a 5 million objects with reference attributes on all) to bring up the initial display.

Answer: eDirectory maintains the reference attributes in a separate container in the database. The delay in the initial display is due to the time it takes FLAIM to delete the database container that holds the "Reference" attribute records.

Configuring Novell eDirectory on Linux, Solaris, or AIX Systems

8

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

- Section 8.1, "Configuration Utilities," on page 123
- Section 8.2, "Configuration Parameters," on page 124
- Section 8.3, "Security Considerations," on page 129

8.1 Configuration Utilities

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

- "The ndsconfig Utility" on page 123
- "Using the ldapconfig Utility to Configure the LDAP Server and LDAP Group Objects" on page 123
- "Using the nmasinst Utility to Configure Novell Modular Authentication Service" on page 124

8.1.1 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 Section 3.6.6, "Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 70.

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 Section 8.2, "Configuration Parameters," on page 124 for a description of `ndsconfig` parameters.

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

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

For more information, see Using the ldapUtility on Linux and UNIX (http://www.novell.com/documentation/edir88/edir88/data/h0000007.html) in the *Novell eDirectory 8.8 Administration Guide*.

8.1.3 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, and AIX systems to configure NMAS.

ndsconfig only configures NMAS and does not install the login methods. To install these login methods, you can use nmasinst. For more information, see "Using the nmasinst Utility to Configure NMAS" on page 80.

8.2 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 .
n4u.base.dclient.use-udp	DClient can use UDP in addition to TCP for communicating with the eDirectory servers. This parameter enables the UDP transport feature. Default=0 Range=0, 1
n4u.base.slp.max-wait	The Service Location Protocol (SLP) API calls timeout. Default=30 Range=3 to 100 This value is in seconds.

Parameter	Description
n4u.nds.advertise-life-time	eDirectory reregisters itself with the Directory Agent after this time period. Default=3600 Range=1 to 65535 This value is in seconds.
n4u.server.signature-level	Determines the level of enhanced security support. Increasing this value increases security, but decreases performance. Default=1 Range=0 to3
n4u.nds.dibdir	The eDirectory directory information database. Default: `/var/opt/novell/eDirectory/data/dib` This parameter cannot be set using the ndsconfig set command. You can manually change this parameter if you want to relocate your DIB. However, we do not recommend you to do so.
n4u.nds.server-guid	A globally unique identifier for the 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 the eDirectory on the server. Default=60 Range=2 to 1440
n4u.nds.synchronization-restrictions	The Off value allows synchronization with any version of the eDirectory. The On value restricts synchronization to version numbers you specify as parameters (for example, ON,420,421). Default=Off

Parameter	Description
n4u.nds.janitor-interval	The interval (in minutes) after which the eDirectory Janitor process is executed.
	Default=2 Range=1 to 10080
n4u.nds.backlink-interval	The interval (in minutes) after which the eDirectory backlink consistency is checked.
	Default=780 Range=2 to 10080
n4u.nds.drl-interval	The interval (in minutes) after which the eDirectory distributed reference link consistency is checked.
	Default=780 Range=2 to 10080
n4u.nds.flatcleaning-interval	The interval (in minutes) after which the flatcleaner process automatically begins purging and deleting entries from the database.
	Default=720 Range=1 to 720
n4u.nds.server-state-up-threshold	The server state up threshold, in minutes. This is the time after which the eDirectory checks the server state before returning -625 errors.
	Default=30 Range=1 to 720
n4u.nds.heartbeat-schema	The heartbeat base schema synchronization interval in minutes.
	Default=240 Range=2 to 1440
n4u.nds.heartbeat-data	The heartbeat synchronization interval in minutes.
	Default=60 Range=2 to 1440
n4u.nds.dofsync	Setting this parameter to 0 increases update performance significantly for large databases, but there is a risk of database corruption if the system crashes.
n4u.server.configdir	The eDirectory configuration files are placed here.
	Default=/etc
n4u.server.vardir	The eDirectory and utilities log files are placed here.
	Default=/var/opt/novell/eDirectory/log
n4u.server.libdir	The eDirectory specific libraries are placed here in the nds-modules directory.
	Default=/opt/novell/eDirectory/lib

Parameter	Description
n4u.server.sid-caching	Enables SSL session ID caching. Refer to the SSL v3.0 RFC for more details about session ID caching in SSL.
n4u.server.tcp-port	The default port used if the port number is not specified in the n4u.server.interfaces parameter.
n4u.server.interfaces	The IP address and port number that eDirectory server should listen on for client connections. The value can be a comma-separated list specifying more than one combination of possible settings. For example: n4u.server.interfaces=101.1.2.3@524,100.1.2.3@1524
n4u.server.max-interfaces	This parameter specifies maximum number of interfaces that eDirectory will use. Default =128. Range =1 to 2048.
n4u.server.max-openfiles	This parameter specifies the maximum number of file descriptors that eDirectory can use. Default=maximum allowed by the administrator
n4u.server.max-threads	The maximum number of threads that will be started by the eDirectory server. This is the number of concurrent operations that can be done within the eDirectory server. Default=64 Range=32 to 512 Refer to the eDirectory tuning guide to set an optimum value.
n4u.server.idle-threads	The maximum number of idle threads that are allowed in the eDirectory server. Default=8 Range=1 to 128
n4u.server.start-threads	Initial number of threads to be started up. Default=8
n4u.server.log-levels	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.
n4u.server.log-file	This parameter specifies the log file location where the messages would be logged. By default, the messages are logged into the `ndsd.log` file.

Parameter	Description
n4u.ldap.lburp.transize	Number of records that are sent from the Novell Import/ Export client to the LDAP server in a single LBURP packet. You can increase the transaction size to ensure that multiple add operations can be performed in a single request. Default=25 Range=1 to 250
n4u.server.listen-on-loopback	It is a boolean parameter, and enabled by default. In a few recent Linux distributions, the hostname in /etc/ hosts file is associated with the loopback address. Though the common address given in the SLES systems is 127.0.0.2, it can be anything from 127.0.0.0 to 127.255.255.255 (valid loopback addresses).
http.server.interfaces	Comma-separated list of interfaces that HTTP server should use.
http.server.request-io-buffer-size	Default IO buffer size.
http.server.request_timeout-seconds	Server request timeout.
http.server.keep-timeout-seconds	Number of seconds to wait for the next request from the same client on the same connection.
http.server.threads-per-processor	HTTP thread pool size per processor.
http.server.session-exp-seconds	Session expiration time in seconds.
http.server.sadmin-passwd	Session administrator password.
http.server.module-base	HTTP server webroot.
https.server.cached-cert-dn	HTTPS server cached certificate DN.
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.

NOTE: For more details information on the eDirectory configuration parameters, refer nds.conf man page.

8.3 Security Considerations

We recommend the following security considerations:

- Make sure that only authenticated users have browse rights to the tree. To limit this, do the following:

    - Remove browse rights of [Public] on tree root.

    - Assign [Root] browse rights on tree root.

- Set ldapBindRestrictions attribute on the LDAP server object to "Disallow anonymous Simple Bind". This prevents the clients from doing anonymous binds.

- By default, the cipher is set to Export. Make LDAP more secure by setting the cipher to HIGH. To do this, change the bind restrictions attribute of LDAP Server object to "Use Higher Cipher (greater than 128 bit)".

Migrating to eDirectory 8.8 SP4

<div style="text-align: right; font-size: 2em;">9</div>

This document guides you to migrate your Novell® eDirectory™ 8.7.3.*x* server to eDirectory 8.8 SP4 when you have to upgrade your operating system also.

eDirectory 8.8 SP4 supports the following platforms:

Platform	Supported Versions
Linux*	◆ SUSE® Linux Enterprise Server 9.1 (OES) or SUSE Linux Enterprise Server 9 ◆ Red Hat* Advanced Server 3
Solaris*	◆ Solaris 10 on Sun* SPARC ◆ Solaris 9 on Sun SPARC
AIX*	◆ AIX 5L Version 5.2
NetWare®	◆ NetWare 6.5 with Support Pack 4 or later
Windows*	◆ Windows 2000 Server with Service Pack 4 or later, Windows 2000 Advanced Server with Service Pack 4 or later ◆ Windows Server 2003

With the change in the operating systems supported in eDirectory 8.8 SP4, there are certain versions that eDirectory 8.8 SP4 does not support that were earlier supported with eDirectory 8.7.3.*x*.

There are two scenarios while migrating to eDirectory 8.8 SP4:

◆ **Migrating to eDirectory 8.8 SP4 when platform upgrade is possible**

In this scenario, you upgrade your operating system to a supported version and then upgrade eDirectory to eDirectory 8.8 SP4.

◆ **Migrating to eDirectory 8.8 SP4 when platform upgrade is not possible**

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

9.1 Migrating to eDirectory 8.8 SP4 While Upgrading the Operating System

In this scenario, you can migrate to eDirectory 8.8 SP4 after upgrading the operating system. The table below describes the migration path.

IMPORTANT: Ensure that you have upgraded eDirectory 8.7.3 with the latest set of patches.

Table 9-1 *Migration Path*

Operating System	Starting State	Intermediate State	Desired State
NetWare	NetWare 5.1 SP6	NetWare 6.5 SP3	eDirectory 8.8 SP1
	NetWare 6 SP3	NetWare 6.5 SP3	eDirectory 8.8 SP1
Windows	Windows NT* 4.0 SP6 + eDirectory 8.7.3.x	Windows 2000 SP4 + eDirectory 8.7.3.x	Windows 2000 SP4 + eDirectory 8.8 SP1
	Windows NT 4.0 SP6 + eDirectory 8.7.3.x	Windows 2003 + eDirectory 8.7.3.x	Windows 2003 + eDirectory 8.8 SP1
	Windows NT 4.0 SP6 + eDirectory 8.7.3.x	Windows 2000 AS SP4 + eDirectory 8.7.3.x	Windows 2000 AS SP4 + eDirectory 8.8 SP1
	Precautions: Before upgrading eDirectory on UNIX and Linux, ensure that the hostname is configured to a valid IP address and not to loopback address in /etc/hosts.		
Linux	eDirectory 8.7.3.x	SLES 9 + eDirectory 8.7.3.x	SLES 9 + eDirectory 8.8 SP1
	eDirectory 8.7.3.x	eDirectory 8.7.3.x	eDirectory 8.8 SP1
	RedHat AS 2.1 + eDirectory 8.7.3.x	RedHat AS 3.0 + eDirectory 8.7.3.x	RedHat AS 3.0 + eDirectory 8.8 SP1
Solaris	Solaris 8 + eDirectory 8.7.3.x	Solaris 9 + eDirectory 8.7.3.x	Solaris 9 + eDirectory 8.8 SP1
	Solaris 8 + eDirectory 8.7.3.x	Solaris 10 + eDirectory 8.7.3.x	Solaris 10 + eDirectory 8.8 SP1
AIX	AIX 5.1 + eDirectory 8.7.3.x	AIX 5.2 + eDirectory 8.7.3.x	AIX 5.2 + eDirectory 8.8 SP1

Recommendations

1. Backup your eDirectory 8.7.3.*x* files before upgrading the operating system. Stop eDirectory and backup the following files:
   - `dib` directory
   - `nds.rfl` directory (by default this directory is present under the `dib` directory)
   - `nds.conf` file
   - `nici` directory
   - log files

2. Do not perform any operations on the intermediate state other than upgrading eDirectory, if the eDirectory version is not supported on a particular operating system in the intermediate state. For example, eDirectory 8.7.3.*x* on Solaris 10.

9.2 Migrating to eDirectory 8.8 SP4 Without Upgrading the Operating System

This method is used in scenarios where there is no operating system upgrade path to supported eDirectory 8.8 SP4 version.

For example, eDirectory 8.7.3.*x* is installed on Red Hat 7.3. A customer using Red Hat 7.3 wants to upgrade to eDirectory 8.8 SP4. eDirectory 8.8 SP4 is supported on Red Hat AS 3.0 and there is no upgrade path from Red Hat 7.3 to Red Hat AS 3.0.

Complete the following steps to migrate to eDirectory 8.8 SP4:

1 Stop the eDirectory server

2 Take a backup of the following eDirectory 8.7.3.x files:

- `dib` directory
- `nds.rfl` directory (by default, this directory is present under the `dib` directory)
- `nds.conf` file
- `nici` directory
- log files

3 Install the operating system

4 Remove the nici folder from `/var/novell` and restore the `nici` folder to `/var/opt/novell`

5 Ensure that `/var/novell/nici` is pointing to `/var/opt/novell/nici`

6 Install eDirectory 8.8 SP4 on the server (a new install)

7 Restore the `dib` and `nds.rfl` directories

8 Restore the nds.conf to the user specified location

9 Edit `/etc/opt/novell/eDirectory/conf/.edir/instances.0` and put the absolute path to `nds.conf file`.

10 Edit nds.conf file and add the following.

```
n4u.nds.dibdir=dib_file_location
n4u.server.libdir=/opt/novell/eDirectory/lib
n4u.server.vardir=var_directory
n4u.server.configdir=/etc/opt/novell/eDirectory/conf
http.server.module-base=http_server_module_base_directory
```

11 Set the path as follows:

- For 32-bit

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

- For 64-bit

  Use `/opt/novell/eDirectory/lib64/bin/ndspath` utility.

12 Run ndsconfig upgrade after setting the path.

Migrating eDirectory from NetWare to OES 2 Linux

10

eDirectory™ migration from NetWare® requires the migration of eDirectory data and server identity to provide seamless accessibility after migration.The eDirectory migration utility performs all of the pre-migration tasks, health validations and server backups; server migration, and post-migration tasks for you.

The following sections give you more details on the migration procedure for eDirectory. For more information, see the *OES Migration Guide* (http://www.novell.com/products/openenterpriseserver/migrate.html).

- Section 10.1, "Planning Your Migration," on page 135
- Section 10.2, "Migration Tools," on page 136
- Section 10.3, "Migration Procedure," on page 136
- Section 10.4, "After the Migration," on page 138

10.1 Planning Your Migration

This section lists the important requirements that must be verified before attempting eDirectory migration.

- Section 10.1.1, "System Requirements," on page 135
- Section 10.1.2, "Prerequisites," on page 135
- Section 10.1.3, "Supported Platforms," on page 136

10.1.1 System Requirements

❑ The target server must run OES 2 and should have the eDirectory 8.8 SP3 RPMs already installed.

❑ If the target OES 2 server has a default eDirectory 8.8 SP3 instance already configured, this instance should be active. This instance will be overwritten after the migration.

❑ OES 2 does not support multiple instances of eDirectory on the same server, so any non-default instances should not be running during migration.

❑ The source NetWare server should be running and should not be part of any partition operation. For more information on supported source NetWare server versions, refer to *eDirectory Coexistence and Migration* (http://www.novell.com/documentation/oes2/oes_implement_lx_nw/index.html?page=/documentation/oes2/oes_implement_lx_nw/data/edir.html#edir-coexistnmig).

10.1.2 Prerequisites

❑ The eDirectory migration utility will run only on the target server and must be able to access the NetWare server remotely.

10.1.3 Supported Platforms

The eDirectory migration utility is designed to run on the Linux version of OES 2, which is the target platform for migration. The following table lists the compatible eDirectory versions at source and the corresponding target servers:

Table 10-1   *eDirectory Versions at Source and Target Servers*

Source Server	Target Server
NetWare 5.1 SP8 + eDirectory 8.7.3.6	Physical or Virtualized OES2 Linux 32 or 64
NetWare 5.1 SP8 + eDirectory 8.7.3.7	Physical or Virtualized OES2 Linux 32 or 64
NetWare 6.5 SP6 + eDirectory 8.7.3.9	Physical or Virtualized OES2 Linux 32 or 64
NetWare 6.5 SP6 + eDirectory 8.8	Physical or Virtualized OES2 Linux 32 or 64
NetWare 6.5 SP6 + eDirectory 8.8 SP1	Physical or Virtualized OES2 Linux 32 or 64
NetWare 6.5 SP6 + eDirectory 8.8 SP3	Physical or Virtualized OES2 Linux 32 or 64

10.1.4 Considerations

- IP address and DNS migrations are not performed by this migration utility.
- Only the eDirectory instance will be migrated. Applications depending on eDirectory will not be migrated.
- You should not use this migration methodology if you want both the servers to be available during the migration operation.

NOTE: Only the target server will be available after the migration. The source server will be locked. Other service migrations cannot be performed after completing eDirectory migration.

10.2 Migration Tools

The eDirectory migration is performed independently of the OES migration framework. The complete migration task is performed by invoking the migedir command line utility.

10.3 Migration Procedure

1 Run the migedir utility by entering the following command on the target server:

```
migedir -s <IP address> [-A <log directory name>] [-t] [-v] [-h]
```

The utility takes the following command line options:

Option	Description
-s *IP address*	Specifies the IP address of the source server containing the eDirectory instance to be migrated.
	IMPORTANT: -*s* is a mandatory parameter.
-A *directory name*	Enables auditing. *directory name* specifies the directory in which log files should be created.
-t	Tests the validity of the input parameters.
	NOTE: This option verifies the IP address; however, it does not perform the actual migration.
-v	Enables the verbose mode.
-h	Prints help about using this utility.

2 Follow the on-screen instructions as the utility performs the migration.

The migration utility does some pre-migration checks, performs the migration, then does some post-migration tasks.

- ◆ "Pre-migration" on page 137
- ◆ "Migration" on page 137
- ◆ "Post-migration" on page 138
- ◆ "Handling Failures" on page 138

Pre-migration

The utility performs the following checks:

- ◆ The health and state of the replicas in the ring are verified.
- ◆ Configuration information for the server being migrated is collected and written to a configuration file to be used by other operations during the migration.
- ◆ Time synchronization is verified between the source and target servers.
- ◆ The target server is checked for any existing eDirectory instances.
  - ◆ If the instance exists, the user is prompted and the existing instance is removed before proceeding with the migration.
  - ◆ If the instance doesn't exist, a new instance is configured and used.

Migration

The utility performs the migration of the eDirectory instance from the collected configuration information. This involves backing up the source server data, locking the eDirectory instance in the source server, migrating data to the target server, and restoring the eDirectory instance on the target server. The dependent NICI files are also migrated.

The utility also configures the local instance in the target server with the source server details obtained during the previous checks.

Post-migration

After migration, the following tasks are performed by the utility:

- The `nds.conf` configuration file is modified with the source server eDirectory instance information, such as tree name and server name.
- The eDirectory instance in the target server is restarted so it can use the new data.
- Network address repair is performed to start the synchronization of the new IP address in the replica ring.

Handling Failures

During migration, the database in the source server is locked to avoid multiple copies of the instance running on the source and target servers. Multiple copies of the same instance can lead to data inconsistency. If the process fails and if you intend to bring up the source server again, you need to perform the following tasks:

1 Remove the partially migrated eDirectory instance on the target server.

   Refer to Removing a Server Object And Directory Services From a Tree (http://www.novell.com/documentation/edir88/edirin88/data/a79kg0w.html#bxm6fn9) for more information on how to remove the eDirectory instance from a server.

2 Restore and unlock the database in the source server.

   Refer to Backup and Restore Command Line Options (http://www.novell.com/documentation/edir88/edir88/data/agatd4y.html) for more information on how to unlock and restore the database.

   The database backup is saved in the `sys:ni/data` folder.

10.4 After the Migration

After migration, the target eDirectory instance listens on the IP address of the target server and not on the source server's address. It requires additional time after migration for the eDirectory instance to synchronize the new IP address in the replica ring. Successful eDirectory migration can be verified by performing eDirectory operations on the new IP address.

IMPORTANT: If you want to use the existing security certificates, you must change the IP address of the target server to that of the source server. If you don't want to do this, you must issue new certificates.

NOTE: If you change the IP address of the target server after migration, you must modify the `nds.conf` file, restart the eDirectory instance, and repair the network address and partitions replica manually. For more infomation on repairing eDirectory instance, refer to Advanced DSRepair Options (http://www.novell.com/documentation/edir88/edir88/data/aflm3p7.html).

Uninstalling Novell eDirectory

<div style="text-align: right">11</div>

This chapter contains the following information:

11.1 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 (http://www.novell.com/documentation/edir88/edir88/data/agavcur.html) 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.

NOTE: The HTML files created using iMonitor will not be removed. You must manually remove these files from `sys:/system/ndsimon/dsreports` before removing eDirectory.

11.1.1 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 15 for more information.

11.2 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 140
- ◆ "Uninstalling NICI" on page 143

NOTE: The HTML files created using iMonitor will not be removed. You must manually remove these files from `<install directory>\novell\NDS\ndsimon\dsreports` before removing eDirectory.

11.2.1 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.

11.2.2 Unattended Uninstallation of eDirectory

On Windows, the unattended uninstallation of eDirectory uses predefined text files that facilitate the unattended uninstallation.The following sections discuss various features of unattended eDirectory uninstallation:

- ◆ "Response Files" on page 140
- ◆ "remove.rsp File Sections and Keys" on page 141
- ◆ "Add Features to the Automated Uninstallation" on page 141
- ◆ "Remove Configuration File Changes" on page 142
- ◆ "Unattended Uninstallation of eDirectory using Response File" on page 142

Response Files

Uninstalling eDirectory on Windows operating system can be made silent and more flexible by using a response file (`remove.rsp`) to complete the following tasks:

- ◆ Complete unattended uninstallation with all required user inputs
- ◆ Default configuration of components
- ◆ Bypass all prompts during the installation

A response file is a text file containing sections and keys, similar to a Windows.ini file. You can create and edit a response file using any ASCII text editor. The eDirectory reads the uninstallation parameters directly from the response file and replaces the default uninstallation values with response file values. The uninstallation program accepts the values from the response file and continues to uninstall without prompts.

remove.rsp File Sections and Keys

The eDirectory uninstallation requires changes to the sections in the response file to add information about including the tree name, administrator context, administrator credentials (including user name and passwords), etc. A full list of the keys and their default values is available in the sample `remove.rsp` file that is delivered with the eDirectory installation.

NOTE: You should use the provided `remove.rsp` file available at `eDirectory\nt\i386\NDSonNT\remove.rsp` in the eDirectory installation. Essential parameters are set by default in this file. When editing the `remove.rsp` file, ensure there are no blank spaces between the key and the values along with the equals sign ("=") in each key-value pair.

You provide the administrator user credentials in the `remove.rsp` file for an unattended uninstallation. Therefore, you must permanently delete the file after the uninstallation to prevent the administrator credentials from being compromised.

Add Features to the Automated Uninstallation

Most details for configuring the eDirectory Uninstaller have default setting for the manual uninstallation. However, during unattended uninstallation, each configuration parameter must be explicitly configured. This section discusses the basic settings to be unconfigured.

eDirectory Server Details

The details of the server being uninstalled must be provided to the Uninstaller. Most of this information is configured in three tags, `[Novell:NDSforNT:1.0.0]`, `[Initialization]`, and `[Selected Nodes]`.

Take all the values mentioned in `[Initialization]` and `[Selected Nodes]` in `remove.rsp` as it they are.

[Novell:NDSforNT:1.0.0]

Tree Name: The name of the tree from which the server will be uninstalled.

Admin Login Name: The name (RDN) of the Administrator object in the tree that has full rights, at least to the context to which this server is added. All operations in the tree will be performed as this user.

Admin Context: Any user added to a tree has a user object that contains all the user-specific details. This parameter is the container object in the tree to which the Administrator object will be added. For primary server installations, this container will be created with the server object.

Admin Password: The password for the Administrator object created in the previous parameters. This password will be configured to the Administrator object during primary server installations. For secondary server installations, this needs to be the password of the Administrator object in the primary server that has rights to the context to which the new server is added.

Prompt: The type of the uninstallation mode should be mentioned in this variable. It will be set by default to 'silent' for unattended uninstallation. If any value other than 'silent' is set then it will do normal uninstallation

The following is a sample of text in the response file for all the basic parameters described above:

```
[Novell:NDSforNT:1.0.0]

  Tree Name=SILENTCORP-TREE

  Admin Context=Novell

  Admin Login Name=Admin

  Admin Password=novell

  prompt=silent
```

Remove Configuration File Changes

In `remove.cfg` file residing in `<Windows Install Drive>\Program Files\Common Files\novell\ni\bin,` change

```
[PARAMETERS]0/OUTPUT_TO_FILE
```

to

```
[PARAMETERS]0/OUTPUT_TO_FILE /SILENT
```

Unattended Uninstallation of eDirectory using Response File

Copy the above edited file `remove.rsp` into `<Windows Install Drive>\Program Files\Common Files\novell\ni\data.`

The `install.exe` installed in the eDirectory is invoked in the command line with a few additional parameters, the command is:

```
<Windows Install Drive>\Program Files\Common
Files\novell\ni\bin>install.exe -remove ..\data\ip.db
..\data\remove.rsp Novell:NDSforNT:1.0.0 0 NDSonNT
```

This performs an unattended uninstallation of eDirectory on the Windows server.

Delete the following folders after uninstalling eDirectory:

- `C:\Novell\NDS`
- `C:\Program Files\Novell\ni`
- `<Windows Installed Drive>:\Program Files\Novell\ni`
- `<Windows Installed Drive>:\Windows\system32\NDScpa.cpl`

11.2.3 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.

11.2.4 Uninstalling Microsoft Visual C++ 2005 Runtime Libraries

If Microsoft Visual C++ 2005 Runtime Libraries are not used by any other products other than eDirectory, uninstall them using the following procedure:

1 Click *Start > Settings > Control Panel > Add/Remove Programs* on the Windows server where eDirectory is installed.

2 Select Microsoft Visual C++ 2005 Redistributable from the list, then click *Add/Remove*.

3 Click Yes to confirm that you want to remove the Microsoft Visual C++ 2005 Redistributable.

The Installation Wizard removes the Microsoft Visual C++ 2005 Redistributable from the server.

11.3 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. You must deconfigure eDirectory server before running `nds-uninstall`. Run `ndsconfig rm -a <admin FDN>` to remove the eDirectory server.

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]...][-s][-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.
-s	Skips the removal of DIBs while the eDirectory is uninstalled. This option facilitates the removal of the eDirectory packages without interrupting the DIBs.
	The 'nds-install' script must be executed to perform an eDirectory upgrade. This option is best suited when the eDirectory packages are required to be replaced for some reason with the same version, usually in the testing scenarios.
	NOTE: The DIBs without the eDirectory binaries cannot be used and are insignificant.

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:
	◆ 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:
	◆ eDirectory installed in a custom location
	◆ eDirectory installed by a nonroot user

Linux, Solaris, and AIX Packages for Novell eDirectory

A

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

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

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 NOVLlmgnt, NOVLxis, and NLDAPbase packages.
NDSbase	Represents the Directory User Agent. This package is dependent on the NICI package.
	The NDSbase package contains the following:
	◆ 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	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.

The NDSserv package contains the following:

- 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, NDSD, and NLDAP
- Man pages

Package	Description
NDSimon	Contains the runtime libraries and utilities used to search and retrieve data from eDirectory services. This package is dependent on the NDSbase package.
NDSrepair	Contains the runtime libraries and the utility that corrects problems in the eDirectory database. This package is dependent on the NDSbase package.
NLDAPbase	Contains LDAP libraries, extensions to LDAP libraries, and the following LDAP tools:

- ldapdelete
- ldapmodify
- ldapmodrdn
- ldapsearch

This package is dependent on the NLDAPsdk package.

Package	Description
NOVLnmas	Contains all the NMAS libraries and the nmasinst binaries needed for NMAS server. This package is dependent on the NICI and NDSmasv packages.
NLDAPsdk	Contains Novell extensions to LDAP runtime and Security libraries (Client NICI).
NOVLsubag	Contains the runtime libraries and utilities for the eDirectory SNMP subagent. This package is dependent on the NICI, NDSbase, and NLDAPbase packages.
NOVLpkit	Provides PKI Services which do not require eDirectory. This package is dependent on the NICI and NLDAPsdk packages.
NOVLpkis	Provides PKI Server Service. This package is dependent on the NICI, NDSbase, and NLDAPsdk packages.
NOVLsnmp	The runtime libraries and utilities for SNMP. This package is dependent on the NICI package.
NDSdexvnt	Contains the library that manages events generated in Novell eDirectory to other databases.
NOVLpkia	Provides PKI services. This package is dependent on the NICI, NDSbase, and NLDAPsdk packages.
NOVLembox	Provides the eMBox infrastructure and eMTools.

Package	Description
NOVLlmgnt	Contains runtime libraries for Novell Language Management.
NOVLxis	Contains the runtime libraries for Novell XIS.
NOVLsas	Contains the Novell SAS libraries.
NOVLntls	Contains Novell TLS library. This package is identified as: ◆ NOVLntls on Solaris, and AIX ◆ ntls on Linux
NOVLldif2dib	Contains the Novell Offline Bulkload utility and is dependent on the NDSbase, NDSserv, NOVLntls, NOVLlmgnt and NICI packages.
NOVLncp	Contains the Novell Encrypted NCP Services for Unix. This package is dependent on the NDScommon package.

eDirectory Health Checks

<div style="text-align: right; font-size: 3em;">B</div>

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

eDirectory health checks are 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.

B.1 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 heath 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.

B.2 Performing Health Checks

You can perform eDirectory health checks in two ways:

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

B.2.1 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 eDirectory health checks happen as part of the installation wizard. You can enable or disable the health checks when prompted to do so.

B.2.2 As a Standalone Utility

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

Table B-1   *Health Check Utilities*

Platform	Utility Name
Linux and UNIX	`ndscheck` Syntax: `ndscheck [--help	-?] Display command usage ndscheck [--version	-v] Display version information ndscheck [-h <hostname port]>] [-a <admin FDN>] [-F <log file>] [-D] [-q] [--config-file <file name>]`
NetWare®	`dscheck` Syntax: `dscheck [--help	-?] Display command usage dscheck [--version	-v] Display version information dscheck [-h <hostname port]>] [-a <admin FDN>] [-F <log file>] [-D] [-q] [--config-file <file name>]`
Windows	`ndscheck` Syntax: `ndscheck [--help	-?] Display command usage ndscheck [--version	-v] Display version information ndscheck [-h <hostname port]>] [-a <admin FDN>] [-F <log file>] [-D] [-q] [--config-file <file name>]`

B.3 Types of Health Checks

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

- Basic Server Health
- Partitions and Replica Health

When you run the `ndscheck` utility, the results are displayed on the screen and logged in `ndscheck.log`. For more information on log files, refer to Section B.5, "Log Files," on page 153.

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). Error types are described in Section B.4, "Categorization of Health," on page 151.

B.3.1 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.

B.3.2 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.

B.4 Categorization of Health

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

- Normal (page 151)
- Warning (page 151)
- Critical (page 152)

The status of the health checks is logged into a logfile. For more information, refer to Section B.5, "Log Files," on page 153.

B.4.1 Normal

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

The upgrade proceeds without an interruption.

B.4.2 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 B-1 on page 152.

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 B-1 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.SOLT
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.O=org.T=SOLT0
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=SOLT0615." ...  [OK]
Checking the status of the replica ring...
 Number of replicas = 2
+---------------------------------------+---------+------------+------------------+------------
----+
 Server Name                             Status   Time Sync   Time Delta         Replica S
tate
+---------------------------------------+---------+------------+------------------+------------
----+

.CN=osg-dt-srv27.O=org.T=SOLT0615.      UP        YES         0 m:0 s            ON

.CN=osg-dt-srv9.O=org.T=SOLT0615.        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/no
vell/eDirectory/data/../log/ndscheck.log" for more details.

For a possible solution refer the following locations -
    1. Cool solutions: http://www.novell.com/coolsolutions/nds/
    2. Support forums: http://support.novell.com/forums/2ed.html
    3. Documentation (trouble shooting section): http://www.novell.com/documentati
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)? _
```

B.4.3 Critical

Critical errors were found while checking the eDirectory health.

If the health check is run as part of the eDirectory upgrade, the upgrade operation is aborted. For more information, see Figure B-2 on page 153.

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 B-2   *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.SOLT
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.O=org.T=SOLT0
615." ...
-----------------------------------------------------------------------------------
-----------
Checking the LDAP and HTTP configuration... [OK]

Checking health of partitions ...

Status of partition ".T=SOLT0615." ...  [OK]
Checking the status of the replica ring...
 Number of replicas = 2
+-----------------------------------------+---------+-------------+----------------+------------+
-----+
 Server Name                               Status   Time Sync    Time Delta      Replica S
tate
+-----------------------------------------+---------+-------------+----------------+------------+
-----+

.CN=osg-dt-srv27.O=org.T=SOLT0615.    UP       YES          0 m:0 s          ON

.CN=osg-dt-srv9.O=org.T=SOLT0615.     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/no
vell/eDirectory/data/../log/ndscheck.log" for more details.

For a possible solution refer the following locations -
  1. Cool solutions: http://www.novell.com/coolsolutions/nds/
  2. Support forums: http://support.novell.com/forums/2ed.html
  3. Documentation (trouble shooting section): http://www.novell.com/documentati
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</>_
```

B.5 Log Files

Every eDirectory 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 B-1 on page 152 and Figure B-2 on page 153.

The health check log file contains the following:

- Status of the health checks (normal, warning, or critical).
- URLs where possible solutions can be found.
  - Support forums (http://support.novell.com/forums/2ed.html)
  - Troubleshooting Documentation (http://www.novell.com/documentation/edir88/edir88tshoot/data/front.html)

- Error Codes (http://www.novell.com/documentation/lg/nwec/index.html)
- Patches (http://support.novell.com/filefinder/5069/index.html)
- Cool Solutions (http://www.novell.com/coolsolutions/nds/)

The following table gives the default log file location on various platforms:

Table B-2 *Health Check Log File Location*

Platform	Log Filename	Location
Linux and UNIX	`ndscheck.log`	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`	1. During eDirectory upgrade, the log messages would be saved at `sys:\system\dscheck.upg`. This file would be recreated each time during upgrade. 2. When health check is performed manually using `dscheck.nlm`, the default log messages would be saved at `sys:\system\dscheck.log`.
Windows	`nsdcheck.log`	The log file will be saved at *install_directory*`\novell nds\`. **NOTE:** *install_directory* is user specified.

Configuring OpenSLP for eDirectory

C

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

C.1 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.

C.2 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.

C.2.1 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.

C.2.2 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.

C.2.3 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 .).

C.3 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.DAActiveDiscoveryInterval = <0, 1, or a number of seconds>
```

The useScopes option indicates which scopes the SA will advertise into, and which scopes queries will be made to in the absence of a specific scope on the registration or query made by the service or client application. Because eDirectory always advertises into and queries from the default scope, this list will become the default scope list for all eDirectory registrations and queries.

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

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

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

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

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