Installation Guide

eDirectory™ 8.8 SP7

April 27, 2012

Novell®

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 and enter your comments there.

Documentation Updates

For the most recent version of the *Novell eDirectory 8.8 SP7 Installation Guide*, see the Novell eDirectory online 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 SP7 Administration Guide* (http://www.novell.com/documentation/edir88/edir88/data/a2iii88.html).

1 Installing or Upgrading Novell eDirectory on Linux

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

-
-
-
-
-
-

1.1 System Requirements

You must install eDirectory on one of the following platforms.

For a 32-bit eDirectory installation:

- 32-bit (x86_32)
  - SUSE Linux Enterprise Server (SLES) 11 SP1 and later Support Packs
  - SLES 10 SP4 and later Support Packs

    NOTE: You might get a warning message while installing eDirectory 8.8 SP7 on SLES 10 SP3. Ignore this warning message. For more information, see TID 7005524 (http://www.novell.com/support/kb/doc.php?id=7005524).

  - Red Hat Enterprise Linux (RHEL) AP 5.4 and later Support Packs
  - RHEL 6 AP and its Support Packs
  - RHEL 6 AP virtualization
  - Xen (on SLES 10 and SLES 11 and their Support Packs)
  - VMware ESX
- 64-bit (x86_64)
  - SLES 11 SP1 and later Support Packs
  - SLES 10 SP4 and later Support Packs
  - RHEL AP 5.4 and later Support Packs
  - RHEL 6 AP and its Support Packs
  - RHEL 6 AP virtualization
  - VMware ESX
  - Xen (on SLES 10 and SLES 11 and their Support Packs)

NOTE: eDirectory 8.8 SP7 is supported on SLES 10 XEN virtualization service that runs the SLES 10 guest OS. The following updates are available at the Novell Update Web site (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 with the Novell Customer Center (http://www.suse.com/products/register.html). After installing 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.

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.

For a 64-bit eDirectory installation:

- SLES 11 SP1 64-bit and later Support Packs
- SLES 10 SP4 64-bit and later Support Packs
- RHEL 5 and its Support Packs
- RHEL 6 and its Support Packs
- VMware ESX
- RHEL virtualization (5.0 and 6.0)
- XEN (on SLES 10 and SLES 11 and their Support Packs)

NOTE: If you install eDirectory on a SLES 11 SP2 server within a BTRFS filesystem, you may experience performance issues when performing LDAP operations or using the Novell Import Conversion Export Utility (ICE). For performance reasons, it is recommended that you use the ext3 filesystem for your eDirectory server.

eDirectory also requires the following:

- A minimum of 512 MB RAM for eDirectory
- 162 MB of disk space for the eDirectory server
- 30 MB of disk space for the eDirectory administration utilities
- 150 MB of disk space for every 50,000 users
- Ensure that gettext is installed

  NOTE: By default, gettext is not installed. Ensure that you install it before you run nds-install, or the installer displays messages about it being missing. On SLES, gettext is available in install CDs.

- Ensure that the `net-snmp-32bit` RPM is installed on 64-bit SLES or OES Linux. The RPM is available in the SLES 10 64-bit install CD.
- If you use ZLM for patch management, apply the hotpatch ZLM6.6.2 HP4 before upgrading to eDirectory 8.8 SP7. On servers such as Vanilla SLES10 or SLES10 SP1, libredcarpet should be upgraded to the latest patch level using YaST Online Update.

1.2 Prerequisites

IMPORTANT: Check the currently installed Novell and Third Party applications to determine if those products are supported on eDirectory 8.8 before upgrading your existing eDirectory environment. The prerequisites for other Novell products can be found on the Novell Documentation site (http://www.novell.com/documentation/). We also recommend you back up an eDirectory instance before performing any upgrades on that instance.

❏ (Conditional) Novell International Cryptographic Infrastructure (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 but will still 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.

When you install eDirectory, the nds-install utility automatically installs NICI. For more information about installing eDirectory, see Section 1.6.2, "Using the nds-install Utility to Install eDirectory Components," on page 20. However, if you need to install only NICI, and not eDirectory itself, on a workstation that has the management utilities installed, you must install NICI manually. For more information about manually installing NICI, see "Installing NICI" on page 23.

❏ Service Location Protocol (SLP) installed and configured

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

Only a root user can install SLP.

For more information on installing SLP, refer to "Using SLP with eDirectory" on page 19.

❏ 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.

For more information on multicast and broadcast routes, refer to the OpenSLP Web site (http://www.openslp.org/doc/html/UsersGuide/Installation.html).

❏ Network server time synchronized

Use Network Time Protocol's (NTP) xntpd to synchronize time across all network servers.

❏ `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 RHEL 5.4, 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 or the `ncurses` RPM contains `libncurses.so.4.`*x* or `libncurses.so.5.`*x*. eDirectory 8.8 supports `libncurses.so.4.`*x* and `libncurses.so.5.`*x*.

❑ 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 non-administrator 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 non-administrator 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 administrator of the tree before adding the secondary using container admin.

❑ While configuring eDirectory, you must enable SLP services and a NetWare Core Protocol™ (NCP) port (the default is 524) in the firewall to allow the secondary server addition. Additionally, you can enable the following service ports based on your requirements:

  ◆ LDAP clear text - 389

  ◆ LDAP secured - 636

  ◆ HTTP clear text - 8028

  ◆ HTTP secured - 8030

In case, if you have enabled user-defined ports, you must mention these ports while configuring eDirectory.

❑ Do not set the user-defined ports to 8008 and 8010 while upgrading eDirectory 8.8 SP2 or later versions to 8.8 SP7. If the ports are set to 8008 or 8010, `ndsconfig` assumes that the server is a pre-eDirectory 8.8*x* server and automatically resets them to 8028 and 8030 respectively.

❑ During eDirectory upgrade, if SecretStore has not already been configured with the previous versions, or you do not want to configure SecretStore, use the `-m no_ss` option with the `nds-install` utility.

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. Two factors increase performance: more cache memory and faster processors. For best results, cache as much of the Directory Information Base (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.

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, start the DSTrace process by issuing the `ndstrace -l>log&` command, which runs the process at the background. This allows you to properly analyze the results of the backlinker process, which takes 4 to 10 minutes. Then force the backlink process to run by issuing the `ndstrace -c 'set ndstrace=*B'` command from the DSTrace OS command prompt. Review the results of the log file created in the first step. Then you can unload the DSTrace process by issuing the `ndstrace -u` command. Running the backlink process is especially important on servers that do not contain a replica.

1.5 Upgrading eDirectory

IMPORTANT: Ensure that supported version of SSP is installed on eDirectory 8.7.3 SP*x* before upgrading to eDirectory 8.8 SP7.

- For eDirectory 8.7.3 SP9, ensure that SSP 203 is installed.
- For eDirectory 8.7.3 SP10, ensure that SSP 206 is installed.

NOTE: The `ndsconfig upgrade` command is used to upgrade the necessary configuration of the individual components such as HTTP, LDAP, SNMP, SAS, and Novell Modular Authentication Service (NMAS). eDirectory database is upgraded to a new format if eDirectory versions prior to eDirectory 8.8 SP1 are upgraded to eDirectory 8.8 SP7.

1.5.1 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 153

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 151 for a list of minor and critical error conditions.

Skipping Server Health Checks

To skip server health checks, run `nds-install -j` or `ndsconfig upgrade -j` from the installation folder.

For more information, see Appendix B, "eDirectory Health Checks," on page 151.

1.5.2 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 the nds-install utility. This utility is located in the `Setup` directory of the downloaded file for Linux platform. Enter the following command from the `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: Run `ndsconfig upgrade` after nds-install, if the upgrade of the DIB fails and nds-install asks to do so.

NOTE: Health check fails due to time sync. To resolve this issue, perform a time sync between the instances. You can ignore this warning message during upgrade.

1.5.3 Unattended Upgrade of eDirectory on UNIX

On UNIX platform, eDirectory provides switches and options along with the install script and configuration utility that facilitates the unattended upgrade. The following sections discuss various steps for unattended eDirectory upgrade on UNIX:

1 Perform the health check of eDirectory:

Health check of all the root instances planned for upgrade is manually done by using `ndscheck` utility.

`export LD_LIBRARY_PATH, SHLIB_PATH and LIBPATH to the <untarred location of eDirectory>/eDirectory/setup/utils`

   1a Run ndscheck using one of the below commands:

       `<untarred location of eDirectory>/eDirectory/setup/utils/ndscheck -a <user name> -w passwd --config-file <nds.conf with absolute path>`

       Passing the password through environment variable: `<untarred location of 88SP7>/eDirectory/setup/utils/ndscheck -a <user name> -w env:<environment variable> --config-file <nds.conf with absolute path>`

       Passing the password through file: `<untarred location of 88SP7>/eDirectory/setup/utils/ndscheck -a <user name> -w file:<filename> --config-file <nds.conf with absolute path>`

       Any one of the above can be used in the automated script for the health check. For example:

```
/Builds/eDirectory/utils/ndscheck -a admin.novell -w n
/Builds/eDirectory/utils/ndscheck -a admin.novell -w env:ADM_PASWD
/Builds/eDirectory/utils/ndscheck -a admin.novell -w file:adm_paswd
```

2 Upgrade the eDirectory 8.8 packages:

   2a Run the nds-install script to upgrade the packages as below:

       `nds-install -u -i -j`

3 Update the following environment variables:

```
PATH=/opt/novell/eDirectory/bin:/opt/novell/eDirectory/sbin:$PATH
LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/opt/novell/eDirectory/lib/nds-
modules:/opt/novell/lib:$LD_LIBRARY_PATH
MANPATH=/opt/novell/man:/opt/novell/eDirectory/man:$MANPATH
TEXTDOMAINDIR=/opt/novell/eDirectory/share/locale
```

4 Upgrade eDirectory by using the `ndsconfig` utility for all the root instances by using the following commands:

`ndsconfig upgrade -a <user name> -w passwd -c --config-file <nds.conf with absolute path>`

Passing the password through environment variable: `ndsconfig upgrade -a <user name>` `-w env:<environment variable> -c --config-file <nds.conf with absolute path>`

Passing the password through file: `ndsconfig upgrade -a <user name> -w` `file:<filename with absolute/relative path> -c --config-file <nds.conf with` `absolute path>`

Any of the above can be used in the automated script for the eDirectory upgrade. For example:

```
ndsconfig upgrade -a admin.novell -w n -c --config-file /etc/opt/novell/
eDirectory/conf/nds.conf
```

```
ndsconfig upgrade -a admin.novell -w env:ADM_PASWD -c --config-file /etc/opt/
novell/eDirectory/conf/nds.conf
```

```
ndsconfig upgrade -a admin.novell -w file:/Builds/88SP7/adm_paswd -c --config-
file /etc/opt/novell/eDirectory/conf/nds.conf
```

1.5.4 Upgrading eDirectory on Existing OES

For more information on upgrading eDirectory on an existing OES installation, refer to the "Updating (Patching) an OES 2 SP3 Server" (http://www.novell.com/documentation/oes2/inst_oes_lx/data/bxlu3xc.html) section in the *OES Installation Guide*.

1.5.5 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 the *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 151. You can use the applicable tools for verification:

  - Use iMonitor for eDirectory version prior to 8.8, see "Using Novell iMonitor" in the *Novell eDirectory 8.8 SP7 Administration Guide*.
  - Use ndscheck utility for eDirectory version 8.8 or later, see "General Utilities" in the *Novell eDirectory 8.8 SP7 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 at least equals the DIB size. For example, 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 155.

1.5.6 Upgrading the Tarball Deployment of eDirectory 8.8

If you want to upgrade the tarball deployment from eDirectory 8.8 to eDirectory 8.8 SP7, 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 ndsmanage.

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

7 Upgrade the following packages if necessary.

Platform	Command	Packages
Linux 32-bit	rpm -Uvh *<rpm name>*	◆ novell-NOVLsubag-8.8.6-1.i586.rpm ◆ novell-NDSslp-8.8.2-1.i386.rpm ◆ nici-2.7.0-0.01.i386.rpm ◆ novell-NDSslp-8.8-1.i386.rpm
Linux 64-bit		◆ novell-NOVLsubag-8.8.6-1.x86_64.rpm ◆ nici64-2.7.6-0.01.x86_64.rpm **NOTE:** For more information on installing 32 and 64-bit NICI, refer to the "Installing NICI" on page 23.
Solaris 32-bit	◆ Remove the older version using the command pkgrm *<pkg name>*. ◆ Install new version using the command pkgadd -d *<pkg name>*.	◆ NOVLsubag.pkg ◆ NOVLniu0.pkg ◆ NDSslp.pkg
Solaris 64-bit		◆ NOVLsubagx.pkg ◆ NOVLniu64.pkg
AIX	installp -acgXd *<pkg name with full path> <pkg name>* all	◆ NDS.NOVLsubag.8.8.6.0 ◆ NOVLniu0.2.7.6.0 ◆ NDS.NDSslp.8.8.2.0

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 Read/Write and others.

1.5.7 Upgrading Multiple Instances

This section contains the following information:

Root User has Multiple Instances

If you run nds-install after upgrading the package, it prompts you to upgrade the DIB files of all the eDirectory server instances, which might take a long time to complete. If you wish to perform the DIB upgrade in parallel, you can do it manually. For information about manually upgrading the DIB, refer to the eDirectory Readme (http://www.novell.com/documentation/edir88/edir887_unix_readme/data/edir887_unix_readme.html). If you upgrade the DIB for all the active instances one by one, it runs the `ndsconfig upgrade` command separately for each instance. If you have a larger DIB, you can select *No* and run the `ndsconfig upgrade` in parallel in separate shells, which can reduce the upgrade time of each instance.

Non Root User's Instances

If you have non root users' instances which are using root users' binaries, before doing the package upgrade you need to run ndscheck for such instances and make sure that their health is proper by referring the `ndscheck.log` file. If you run nds-install, it stops all the instances, including the non root user's instances. After doing the package upgrade, the `nds-install` command does not call `ndsconfig upgrade` for nonroot user's instances. You need to manually run `ndsconfig upgrade` for all nonroot user's instances to start these instances.

Order of Upgrade

While running `ndsconfig upgrade`, it is recommended to follow the order in which master replica comes first and then Read/Write or other replicas.

1.5.8 Disk Space Check on Upgrading to eDirectory 8.8 SP7

When eDirectory server is upgraded from previous versions to eDirectory 8.8 SP7, 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 6, "Upgrade Requirements of eDirectory 8.8," on page 95.

1.6 Installing eDirectory

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

1.6.1 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, you should install and configure the protocol, and the SLP directory agents (DAs) should be stable.

1 Install OpenSLP, if it is not already installed.

2 Follow the on-screen instructions to complete the SLP installation.

3 Start SLP manually as follows:

   /etc/init.d/slpd start

For more information, refer to Appendix C, "Configuring OpenSLP for eDirectory," on page 157.

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

/etc/init.d/slpd 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.

Local server need not have an entry in this file unless it is listening on non-default NCP port.

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/DNS Resolvable Name
  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/slptool findattrs services: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/slptool findattrs services: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 157.

1.6.2 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 the command `/etc/init.d/rcd stop`.

---

1 Enter the following command at the setup directory:

`./nds-install`

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
-h or --help	Displays help for nds-install.
-i	Prevents the nds-install script from invoking the `ndsconfig upgrade` command 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 151.

nds-install Parameter	Description
-m	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.
-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 installs the following RPMs:

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.

eDirectory Component	Packages Installed	Description
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.

2 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. The default location is the `/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.

3 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 by entering the following commands:**

  - For 32-bit

    ```
    export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/opt/novell/
    eDirectory/lidirb/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 by performing the following steps:**

  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
  ```

  NOTE: When you prefix the ndspath script to the commands with arguments, specify the arguments in double quotes.

  For example:

  ```
  /opt/novell/eDirectory/bin/ndspath ldapconfig "-s ldapTLSRequired=yes"
  ```

  - 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 101.

For more information on the nmasinst utility, see "Using the nmasinst Utility to Configure NMAS" on page 37.

NOTE: After you install eDirectory, we recommend you exclude the DIB directory on your eDirectory server from any antivirus or backup software processes. Use the eDirectory Backup Tool to back up your DIB directory.

For more information about backing up eDirectory, see "Backing Up and Restoring Novell eDirectory," in the *Novell eDirectory 8.8 SP7 Administration Guide*.

1.6.3   Nonroot User Installing eDirectory 8.8

A nonroot user can install eDirectory 8.8 using the tarball.

Prerequisites

❒ If you want to install eDirectory using the tarball and not the nds-install utility, ensure that NICI is installed. For information on installing NICI, refer to "Installing NICI" on page 23.

❒ 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 non-administrator user, ensure that you have the appropriate rights as mentioned in the Section 1.2, "Prerequisites," on page 11 section.

Installing NICI

NICI should be installed before you proceed with the eDirectory installation. Because the required NICI packages are used system-wide, we recommend you use the root user to install the necessary packages. However, if necessary you can delegate access to a different account using sudo and use that account to install the NICI packages.

With eDirectory 8.8 SP3 or later versions, 32 and 64-bit applications can coexist in a single system. This requires installing both the 32 and 64-bit versions of NICI.

Root User Installing NICI

To install NICI, enter both of the following commands:

32-bit: rpm -ivh *NICI_rpm_absolute_path*/nici-2.7.4-0.01.i386_64.rpm

64-bit: rpm -ivh *NICI_rpm_absolute_path*/nici64-2.7.4-0.01.x86.rpm

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, you must 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 user "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 this 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.

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 by entering the following commands:**
  - 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 by performing the following steps:**

   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 32.

Follow the on-screen instructions to complete the configuration.

For more information, see Section 1.6.4, "Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 26.

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.

NOTE: After you install eDirectory, we recommend you exclude the DIB directory on your eDirectory server from any antivirus or backup software processes. Use the eDirectory Backup Tool to back up your DIB directory.

For more information about backing up eDirectory, see "Backing Up and Restoring Novell eDirectory," in the *Novell eDirectory 8.8 SP7 Administration Guide*.

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

After installing eDirectory, configure the eDirectory replica server using the ndsconfig utility. 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 101.

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 FDN` variables. The maximum number of characters allowed for these variables is as follows:

- `tree_name`: 32 characters
- `admin FDN`: 255 characters
- `server FDN`: 255 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, see "Encrypted Replication" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

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. **NOTE:** This option does not remove the key material objects. These objects must be removed manually.
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`.

ndsconfig Parameter	Description
-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.
-r	This option forcefully adds the replica of the server regardless of the number of servers already added to the server.
-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.
-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. **NOTE:** If you do not want to configure Novell SecretStore during eDirectory upgrade through nds-install, pass the no_ss value to this option. For example, nds-install '-m no_ss'.
-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 recommended 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.

ndsconfig Parameter	Description
`-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 parameters 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.

`--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_data*	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 parameters, ndsd need not be restarted.
	
	These parameters are listed below:
	
	  ♦ `n4u.nds.inactivity-synchronization-interval`
	  ♦ `n4u.nds.synchronization-restrictions`
	  ♦ `n4u.nds.janitor-interval`
	  ♦ `n4u.nds.backlink-interval`
	  ♦ `n4u.nds.drl-interval`
	  ♦ `n4u.nds.flatcleaning-interval`
	  ♦ `n4u.nds.server-state-up-threshold`
	  ♦ `n4u.nds.heartbeat-schema`
	  ♦ `n4u.nds.heartbeat-data`

`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.

ndsconfig Parameter	Description
`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.

1.6.5 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 Instances" in the *Novell eDirectory 8.8 SP7 What's New Guide*.

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 port number 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.

    When configuring multiple instances, either on the same tree or on different trees, the NCP server name should be unique.

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 32.

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 32
- "Listing the Instances" on page 32
- "Creating an Instance through ndsmanage" on page 32
- "Performing Operations for a Specific Instance" on page 33

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 DSTrace for the instance
  - Deconfigure the instance
- Start and Stop all instances

Listing the Instances

The following table describes how to list the eDirectory instances.

Table 1-1 *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 fully distinguished name (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 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 1-1 *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:

- "Starting a Specific Instance" on page 33
- "Stopping a Specific Instance" on page 34
- "Deconfiguring an Instance" on page 34

Other than the ones listed above, you can also run DSTrace 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 1-2 *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 Figure 1-2, "ndsmanage Utility Output Screen with Instance Options," on page 34.

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 Figure 1-2, "ndsmanage Utility Output Screen with Instance Options," on page 34.

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 33.

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 34.

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
var directory	/home/mary/inst1/var

- **Instance 2:**

Port number the instance should listen on	2524
Configuration file path	/home/mary/inst2/nds.conf
var 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. With eDirectory, it is recommended to have the `var` directory on the local file system (`-D` option with `ndsconfig`) and the DIB directory can be of any file system (`-d` option with `ndsconfig`).

Invoking a Utility for an Instance

If Mary wants to run the DSTrace 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 (user name is `john`):

  ```
  ndsmanage john
  ```
* To display all instances of all users that are using a particular installation of eDirectory:

  ```
  ndsmanage -a
  ```

1.6.6 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 DSRepair, Backup, DSMerge, DSLogin, and ldapconfig.

1.6.7 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 37
- ◆ "Installing Login Methods" on page 37

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/nmas33/admin/data/a53vj9a.html) in the *Novell Modular Authentication Services 3.3 Administration Guide*.

1.6.8 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 23

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
```

2 Installing or Upgrading Novell eDirectory on Solaris

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

2.1 System Requirements

You must install eDirectory on one of the following platforms.

For a 32-bit eDirectory installation:

- Solaris 10 on Sun SPARC

For a 64-bit eDirectory installation:

- Solaris 10 on Sun SPARC
- Solaris 10 Zones (Small Zone and Big Zone)

  NOTE: Installation on Solaris 10 Zones is supported on eDirectory 8.8 SP5 or later. Regardless of the type of a zone, either a 32-bit eDirectory or a 64-bit eDirectory can be installed in each of the zones present in a system. In a zone only one type of eDirectory should be installed.

Update your system with the following libumem patches:

- 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 My Oracle Support* Web page (https://support.oracle.com). If you do not update your system with the latest patches before installing eDirectory, you will get the patchadd error.

eDirectory also requires the following:

- A minimum of 512 MB RAM
- 184 MB of disk space for the eDirectory server

- 43 MB of disk space for the eDirectory administration utilities
- 150 MB of disk space for every 50,000 users

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 TID 7003446 (http://www.novell.com/support/kb/doc.php?id=7003446). You are highly recommended 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 but will still 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.

When you install eDirectory, the nds-install utility automatically installs NICI. For more information about installing eDirectory, see Section 2.6.3, "Using the nds-install Utility to Install eDirectory Components," on page 45. However, if you need to install only NICI, and not eDirectory itself, on a workstation that has the management utilities installed, you must install NICI manually. For more information about manually installing NICI, see "Installing NICI" on page 48. The package containing NICI 2.7 is named NOVLniu0-2.7 on Solaris.

❒ 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 44.

❒ 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
```

For more information on multicast and broadcast routes, refer to the OpenSLP Web site (http://www.openslp.org/doc/html/UsersGuide/Installation.html).

❒ 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.

❏ To avail all the functionality of eMBox such as DSMerge, you need to install the latest Solaris patch - 12 March 2009 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 non-administrator 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 non-administrator 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.

❏ While configuring eDirectory, you must enable SLP services and an NCP™ port (the default is 524) in the firewall to allow the secondary server addition. Additionally, you can enable the following service ports based on your requirements:

- LDAP clear text - 389
- LDAP secured - 636
- HTTP clear text - 8028
- HTTP secured - 8030

In case, if you have enabled user-defined ports, you must mention these ports while configuring eDirectory.

❏ During eDirectory upgrade, if SecretStore has not already been configured with the previous versions, or you do not want to configure SecretStore, use the `-m no_ss` option with the `nds-install` utility.

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.

2.3 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.

2.4 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 DSTrace 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 DSTrace command prompt. Then you can unload the DSTrace process by issuing the `ndstrace -u` command. Running the backlink process is especially important on servers that do not contain a replica.

2.5 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: The `ndsconfig upgrade` command has to be run after nds-install, if upgrade of the DIB fails and nds-install asks to do so.

NOTE: Health check fails due to time sync. To resolve this issue, perform a time sync between the instances. You can ignore this warning message during upgrade.

2.5.1 Upgrading Multiple Instances

For information on Upgrading Multiple Instances, refer to Section 1.5.7, "Upgrading Multiple Instances," on page 18 in the Linux chapter.

2.5.2 Upgrading the Tarball Deployment of eDirectory 8.8

For information on upgrading the tarball deployment of eDirectory 8.8, refer to Section 1.5.6, "Upgrading the Tarball Deployment of eDirectory 8.8," on page 16 in the Linux chapter.

2.6 Installing eDirectory

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

- Section 2.6.1, "Server Health Checks," on page 43
- Section 2.6.2, "Using SLP with eDirectory," on page 44
- Section 2.6.3, "Using the nds-install Utility to Install eDirectory Components," on page 45
- Section 2.6.4, "Nonroot User Installing eDirectory 8.8," on page 47
- Section 2.6.5, "Installing eDirectory 8.8 on Solaris 10 Zones," on page 50
- Section 2.6.6, "Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 51
- Section 2.6.7, "Using ndsconfig to Configure Multiple Instances of eDirectory 8.8," on page 53
- Section 2.6.8, "Using ndsconfig to Install a Solaris Server into a Tree with Dotted Name Containers," on page 53
- Section 2.6.9, "Using the nmasinst Utility to Configure NMAS," on page 54
- Section 2.6.10, "Nonroot user SNMP configuration," on page 55

2.6.1 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 152
- Section B.3.2, "Partitions and Replica Health," on page 153

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 151 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 151.

2.6.2 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 on-screen 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 19 and the `hosts.nds` man page.

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 157.

2.6.3 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 2.6.4, "Nonroot User Installing eDirectory 8.8," on page 47.

1 Enter the following command from the setup directory:

```
./nds-install
```

To install eDirectory components, use the following syntax:

```
nds-install [-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
-h	Displays help for nds-install.
-i	Prevents the nds-install script from invoking the `ndsconfig upgrade` command 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 151.
-m	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.
-u	Specifies the option to use an unattended install mode.

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.

2 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. The default location is the /var directory, 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 101.

For more information on the nmasinst utility, see "Using the nmasinst Utility to Configure NMAS" on page 54.

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

- ◆ **Manually export the environment variables**

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

  64-bit: export `LD_LIBRARY_PATH=/opt/novell/eDirectory/lib/sparcv9:/opt/novell/eDirectory/lib/sparcv9/nds-modules:/opt/novell/lib/sparcv9:$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.

NOTE: After you install eDirectory, we recommend you exclude the DIB directory on your eDirectory server from any antivirus or backup software processes. Use the eDirectory Backup Tool to back up your DIB directory.

For more information about backing up eDirectory, see "Backing Up and Restoring Novell eDirectory," in the *Novell eDirectory 8.8 SP7 Administration Guide*.

2.6.4 Nonroot User Installing eDirectory 8.8

A nonroot user can install eDirectory 8.8 using the tarball.

Prerequisites

❑ If you want to install eDirectory using the tarball and not the nds-install utility, ensure that NICI is installed. For information on installing NICI, refer to "Installing NICI" on page 23.

❑ 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 non-administrator user, ensure that you have the appropriate rights as mentioned in the Section 2.2, "Prerequisites," on page 40 section.

Installing NICI

NICI should be installed before you proceed with the eDirectory installation. Because the required NICI packages are used system-wide, we recommend you use the root user to install the necessary packages. However, if necessary you can delegate access to a different account using sudo and use that account to install the NICI packages.

Root User Installing NICI

To install NICI, enter one of the following commands:

32-bit: `pkgadd -d NICI_package_absolute_path_and_filename NOVLniu0`

For example:

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

64-bit: `pkgadd -d NICI_package_absolute_path_and_filename NOVLniu64`

For example:

`pkgadd -d /home/build/Solaris/Solaris/setup/NOVLniu64.pkg NOVLniu64`

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, you must 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.

---

3 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.

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**

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

    64-bit: export LD_LIBRARY_PATH=*custom_location*/eDirectory/opt/novell/
    eDirectory/lib/sparcv9:*custom_location*/eDirectory/opt/novell/eDirectory/lib/
    sparcv9/nds-modules:*custom_location*/eDirectory/opt/novell/lib/sparcv9:/opt/novell/
    lib/sparcv9:/opt/novell/eDirectory/lib/sparcv9:$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 32.

Follow the on-screen instructions to complete the configuration.

For more information, see Section 2.6.6, "Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 51.

NOTE: After you install eDirectory, we recommend you exclude the DIB directory on your eDirectory server from any antivirus or backup software processes. Use the eDirectory Backup Tool to back up your DIB directory.

For more information about backing up eDirectory, see "Backing Up and Restoring Novell eDirectory," in the *Novell eDirectory 8.8 SP7 Administration Guide*.

2.6.5 Installing eDirectory 8.8 on Solaris 10 Zones

eDirectory 8.8 SP5 or later versions can be installed on Solaris* 10 Zones.

An Introduction to Zones

A zone is a virtual instance of Solaris. It is also one of the software partitions of the operating system. A large Sun Fire server with hardware domains allows the creation of several isolated systems. It is easy to move individual CPUs between the zones as needed, or to configure the sharing of CPUs and memory.

Types of Zones

There are two types of zones, a global zone and a non-global zone.

Global Zone

The global zone is the original Solaris OS instance, which has access to the physical hardware and can control all the processes. Global zones create non-global zones that are authorized to create and control new zones in which the applications run.

Non-Global Zone

A non-global zone is aligned with the global zones, but does not run inside them. Global zones can monitor the configuration of the non-global zones and control them. You can choose two general non-global zone types during the zone creation, a Small Zone and a Big Zone.

Small Zone (Sparse Root Zone)

A small zone is the default zone that consumes the least disk space. It is high performing and highly secure.

NOTE: Before installing eDirectory on a small zone, NICI should be installed on the global zone. For information on installing NICI, refer to "Installing NICI" on page 23

Big Zone (Whole Root Zone)

A big zone has its own /usr files, which can be modified independently.

For more information on Solaris* Zones refer to the following links:

Information on Zones (http://www.solarisinternals.com/wiki/index.php/Zones#Zones)

Information on the Solaris Operating System (http://www.oracle.com/us/products/servers-storage/solaris/overview/index.html)

Installing eDirectory 8.8 on a Global or Non-Global Zone

Use the nds-install utility to install eDirectory components on a Solaris* 10 Zones system. This utility is present in the setup directory, in the CD provided for eDirectory installation on a Solaris platform. This utility adds the required packages, based on the components you choose to install.

To run the nds-install utility, enter the following command from the setup directory:

```
./nds-install
```

After installation, use the ndsconfig utility for configuring the eDirectory installed on the Solaris* 10 Zones system. For more information on the ndsconfig utility refer to the Novell Documentation Website (http://www.novell.com/documentation/edir88/edirin88/data/a7f5t0z.html#a7f7ods)

2.6.6 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 101.

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 FDN variables. The maximum number of characters allowed for these variables is as follows:

- ◆ tree_name: 32 characters
- ◆ admin FDN: 255 characters
- ◆ server FDN: 255 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, see "Encrypted Replication" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

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 28 for more information.

2.6.7 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 1.6.5, "Using ndsconfig to Configure Multiple Instances of eDirectory 8.8," on page 31 in the Linux chapter.

2.6.8 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 DSRepair, Backup, DSMerge, DSLogin, and ldapconfig.

2.6.9 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

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/nmas33/admin/data/a53vj9a.html) in the *Novell Modular Authentication Services 3.3 Administration Guide*.

2.6.10 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 23.

2 Install `NOVLsubag` as root.

3 Export the paths as follows:

Manually export the environment variables.

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`

64-bit: export `LD_LIBRARY_PATH=`*custom_location/opt/novell/* `eDirectory/lib/`
`sparcv9:`*custom*`_location/opt/novell/lib/sparcv9:/opt/novell/lib/sparcv9:/ opt/`
`novell/eDirectory/lib/sparcv9:$LD_LIBRARY_PATH`

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

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

3 Installing or Upgrading Novell eDirectory on AIX

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

3.1 System Requirements

You can install eDirectory 8.8 SP7 (32-bit installation only) on servers running AIX Version 6.1.x.

eDirectory also requires the following:

- All recommended AIX OS patches, available at the IBM* Fix Central (http://www-933.ibm.com/support/fixcentral/) Web site
- A minimum of 512 MB RAM
- 215 MB of disk space for the eDirectory server
- 38 MB of disk space for the eDirectory administration utilities
- 150 MB of disk space for every 50,000 users

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 7003446 (http://www.novell.com/support/kb/doc.php?id=7003446). You are highly recommended 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 on the AIX Documentation Web site (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 but will still 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.

When you install eDirectory, the nds-install utility automatically installs NICI. For more information about installing eDirectory, see Section 3.6.3, "Using the nds-install Utility to Install eDirectory Components," on page 62. However, if you need to install only NICI, and not eDirectory itself, on a workstation that has the management utilities installed, you must install NICI manually. For more information about manually installing NICI, see "Installing NICI" on page 65. The package containing NICI 2.7 is named NOVLniu0-2.7 on AIX.

❑ 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.

❑ (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 non-administrator 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 non-administrator 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.

❑ While configuring eDirectory, you must enable SLP services and an NCP™ port (the default is 524) in the firewall to allow the secondary server addition. Additionally, you can enable the following service ports based on your requirements:

  ◆ LDAP clear text - 389
  ◆ LDAP secured - 636
  ◆ HTTP clear text - 8028
  ◆ HTTP secured - 8030

In case, if you have enabled user-defined ports, you must mention these ports while configuring eDirectory.

❑ During eDirectory upgrade, if SecretStore has not already been configured with the previous versions, or you do not want to configure SecretStore, use the -m no_ss option with the nds-install utility.

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.

3.3 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.

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 DSTrace 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 DSTrace command prompt. Then you can unload the DSTrace 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

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

NOTE: Health check fails due to time sync. To resolve this issue, perform a time sync between the instances. You can ignore this warning message during upgrade.

3.5.1 Upgrading Multiple Instances

For information on Upgrading Multiple Instances, refer to Section 1.5.7, "Upgrading Multiple Instances," on page 18 in the Linux chapter.

3.5.2 Upgrading the Tarball Deployment of eDirectory 8.8

For information on upgrading the tarball deployment of eDirectory 8.8, refer to Section 1.5.6, "Upgrading the Tarball Deployment of eDirectory 8.8," on page 16 in the Linux chapter.

3.6 Installing eDirectory

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

- Section 3.6.1, "Server Health Checks," on page 61
- Section 3.6.2, "Using SLP with eDirectory," on page 61
- Section 3.6.3, "Using the nds-install Utility to Install eDirectory Components," on page 62
- Section 3.6.4, "Nonroot User Installing eDirectory 8.8," on page 64
- Section 3.6.5, "Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 67
- Section 3.6.6, "Using ndsconfig to Configure Multiple Instances of eDirectory 8.8," on page 69
- Section 3.6.7, "Using ndsconfig to Install an AIX Server into a Tree with Dotted Name Containers," on page 69
- Section 3.6.8, "Using the nmasinst Utility to Configure NMAS," on page 69
- Section 3.6.9, "Nonroot user SNMP configuration," on page 70

3.6.1 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 152
- Section B.3.2, "Partitions and Replica Health," on page 153

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 151 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 151.

3.6.2 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 on-screen 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. The `hosts.nds` file should be created in `/etc/opt/novell/eDirectory/conf/hosts.nds` or `<custom_location>/etc/opt/novell/eDirectory/conf/hosts.nds`. For more information on `hosts.nds`, refer to "Using SLP with eDirectory" on page 19 and the `hosts.nds` man page.

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 157.

3.6.3 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 [-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
-h	Displays help for nds-install.
-i	Prevents the nds-install script from invoking the ndsconfig upgrade command 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 151.
-m	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.
-u	Specifies the option to use an unattended install mode.

The installation program installs the following depots:

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 NOVLldif2 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.

2 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. The default location is the /var directory, 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 101.

For more information on the nmasinst utility, see "Using the nmasinst Utility to Configure NMAS" on page 69.

3 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.

NOTE: After you install eDirectory, we recommend you exclude the DIB directory on your eDirectory server from any antivirus or backup software processes. Use the eDirectory Backup Tool to back up your DIB directory.

For more information about backing up eDirectory, see "Backing Up and Restoring Novell eDirectory," in the *Novell eDirectory 8.8 SP7 Administration Guide*.

3.6.4 Nonroot User Installing eDirectory 8.8

A nonroot user can install eDirectory 8.8 using the tarball.

Prerequisites

❒ If you want to install eDirectory using the tarball and not the nds-install utility, ensure that NICI is installed. For information on installing NICI, refer to "Installing NICI" on page 65.

❒ 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 non-administrator user, ensure that you have the appropriate rights as mentioned in the Section 3.2, "Prerequisites," on page 57 section.

Installing NICI

NICI should be installed before you proceed with the eDirectory installation. Because the required NICI packages are used system-wide, we recommend you use the root user to install the necessary packages. However, if necessary you can delegate access to a different account using sudo and use that account to install the NICI packages.

Root User Installing NICI

To install NICI, 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
```

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, you must 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.

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_] [-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 32.

Follow the on-screen instructions to complete the configuration.

For more information, see Section 3.6.5, "Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 67.

NOTE: After you install eDirectory, we recommend you exclude the DIB directory on your eDirectory server from any antivirus or backup software processes. Use the eDirectory Backup Tool to back up your DIB directory.

For more information about backing up eDirectory, see "Backing Up and Restoring Novell eDirectory," in the *Novell eDirectory 8.8 SP7 Administration Guide*.

3.6.5 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 101.

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 ] [-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 FDN* variables. The maximum number of characters allowed for these variables is as follows:

- ◆ *tree_name*: 32 characters
- ◆ *admin FDN*: 255 characters
- ◆ *server FDN*: 255 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 ] [-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 ] [-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, see "Encrypted Replication" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

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 28 for more information.

3.6.6 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 1.6.5, "Using ndsconfig to Configure Multiple Instances of eDirectory 8.8," on page 31 in the Linux chapter.

3.6.7 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 DSRepair, Backup, DSMerge, DSLogin, and ldapconfig.

3.6.8 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 69
- "Installing Login Methods" on page 70

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/nmas33/admin/data/a53vj9a.html) in the *Novell Modular Authentication Services 3.3 Administration Guide*.

3.6.9 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 65.

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
```

4 Installing or Upgrading Novell eDirectory on Windows

Use the following information to install or upgrade Novell eDirectory 8.8 on a Windows platform:

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 a Windows Server" on page 75.

4.1 System Requirements

You must install eDirectory on one of the following platforms.

For a 32-bit eDirectory installation:

- 32-bit Windows Server 2003 Enterprise Edition with latest Service Pack
- 32-bit Windows Server 2008 (Standard/Enterprise/Data Center Edition)

For a 64-bit eDirectory installation:

- 64-bit Windows Server 2008 (Standard/Enterprise/Data Center Edition)
- Windows Server 2008 R2 (Standard/Enterprise/Data Center Edition)

IMPORTANT

- You must use an account that has administrative rights to install eDirectory 8.8 SP7 on Windows Server 2008 R2.
- You should apply the latest available patch for eDirectory.
- Windows XP is not a supported eDirectory 8.8 platform.

eDirectory also requires the following:

- An assigned IP address

- 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.

- (Optional) One or more workstations running one of the following:
  - Novell Client for Windows 2000 version 4.9
  - Novell Client for Windows XP version 4.9

Refer to the OS recommended hardware requirements for your Windows server.

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 7003446 (http://www.novell.com/support/kb/doc.php?id=7003446) It is also highly recommended to back up 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 the Windows Server documentation for more information.

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

  Refer to the Windows Server documentation 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 but will still 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 NICI installed on the system.

❏ If you are upgrading to eDirectory 8.8, make sure you have the latest eDirectory patches installed on all non-eDirectory 8.8 servers in the tree. You can get eDirectory patches from the Novell Support (http://support.novell.com) Web site.

❏ Make sure you have the latest Windows 2003 or 2008 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 8.7.3 or later.

❏ (Conditional) If you are installing a secondary server into an existing tree as a non-administrator 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 non-administrator 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.

❑ While configuring eDirectory, you must enable SLP services and an NCP port (the default is 524) in the firewall to allow the secondary server addition. The NCP port must be configured to allow both inbound and outbound traffic.

Additionally, you can enable the following service ports, based on your requirements:

- ◆ LDAP clear text - 389
- ◆ LDAP secured - 636
- ◆ HTTP clear text - 8028
- ◆ HTTP secured - 8030

If you have enabled user-defined ports, you must specify these ports while configuring eDirectory.

❑ If you are installing eDirectory on a virtual machine having a DHCP address or on a physical or virtual machine in which SLP is not broadcast, ensure that the Directory Agent is configured in your network.

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.

4.3 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:

Objects	Memory	Hard Disk
10,000	384 MB	144 MB
1 million	2 GB	1.5 GB
10 million	2+ GB	15 GB

Requirements for processors depend on 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 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, see "Understanding WAN Traffic Manager" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

4.5 Disk Space Check on Upgrading to eDirectory SP7 or later

When eDirectory server is upgraded from 8.7.x and 8.8 to eDirectory 8.8 SP7 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 6, "Upgrade Requirements of eDirectory 8.8," on page 95.

4.6 Installing Novell eDirectory on Windows

This section contains the following information:

4.6.1 Installing or Updating Novell eDirectory 8.8 on a Windows Server

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 157.
- DHCP Options for Service Location Protocol (http://www.openslp.org/doc/rfc/rfc2610.txt)
- OpenSLP Documentation (http://www.openslp.org/documentation.html)

3 If you have Autorun turned off, run `setup.exe` from the `nt` folder (32-bit eDirectory) and `windows` folder (64-bit eDirectory) in the Novell eDirectory 8.8 SP7 CD or from the downloaded file.

4 Click *Install*.

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

- NICI 2.7

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

  You might have to reboot the server after the NICI installation. If the installer displays a message saying that you need to reboot your server before continuing, click *OK* to reboot. 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.

5 Click *Next*.

6 View the license agreement, then click *I Accept*.

7 Select a language for the installation, then click *Next*.

8 Specify or confirm the installation path, then click *Next*.

9 If the installation folder does not already exist, and you want the installer to create the folder for you, click *Yes*.

10 Specify or confirm the DIB path, then click *Next*.

11 If the DIB folder does not already exist, and you want the installer to create the folder for you, click *Yes*.

12 (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.

13 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 the *Novell eDirectory 8.8. SP7 What's New Guide* (http://www.novell.com/documentation/edir88/edir88new/data/front.html) for more information.

  For information on using dots in container names, see "Installing into a Tree with Dotted Name Containers" on page 80.

14 (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 2.7 Administration Guide* (http://www.novell.com/documentation/imanager27/imanager_admin_275/data/hk42s9ot.html).

15 (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 77.

16 Specify whether to configure the SecretStore module. By default, the *Configure SecretStore* option is selected.

17 Select the NMAS™ login methods you want to install.

  See "Installing NMAS Server Software" on page 80 and "Installing NMAS Client Software" on page 80 for more information.

18 Click *Next*.

19 Click *Finish* to complete the eDirectory installation.

20 When the installer completes the installation, click *Done*.

NOTE: After you install eDirectory, we recommend you exclude the DIB directory on your eDirectory server from any antivirus or backup software processes. Use the eDirectory Backup Tool to back up your DIB directory.

For more information about backing up eDirectory, see "Backing Up and Restoring Novell eDirectory," in the *Novell eDirectory 8.8 SP7 Administration Guide*.

4.6.2 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 153

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 151 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 Appendix B, "eDirectory Health Checks," on page 151.

4.6.3 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 4-1 *Defaults for the LDAP Configuration Screen*
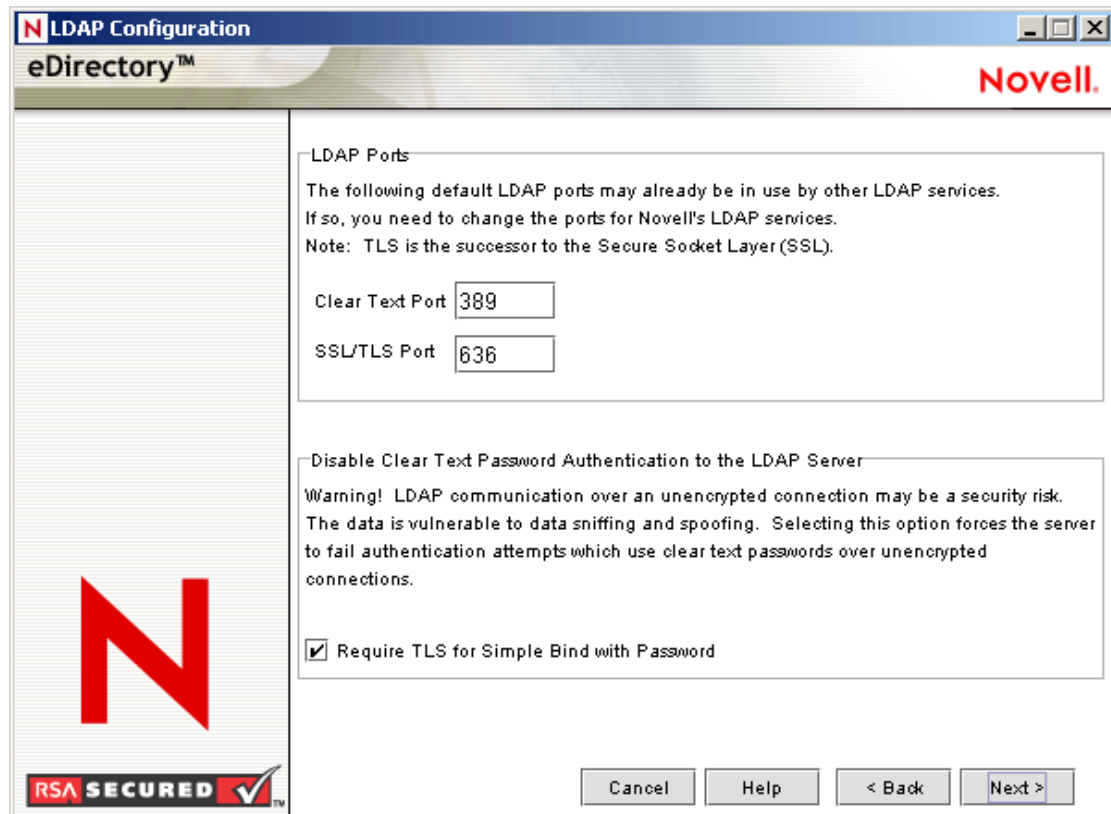
Scenario: Require TLS for Simple Bind with Password Is Enabled: Olga is using a client that asks for a password. After Olga enters a password, the client connects to the server. However, the LDAP server does not allow the connection to bind to the server over the clear-text port. Everyone is able to 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 4-2 *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. For more information, see "Verifying That the LDAP Server Is Running" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

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. For more information, see "Verifying That the LDAP Server Is Running" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

4.6.4 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/nmas33/admin/data/a53vj9a.html) in the *Novell Modular Authentication Services 3.3 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.

4.6.5 Installing NMAS Client Software

The NMAS client software must be installed on each client workstation where you want to use the NMAS login methods.
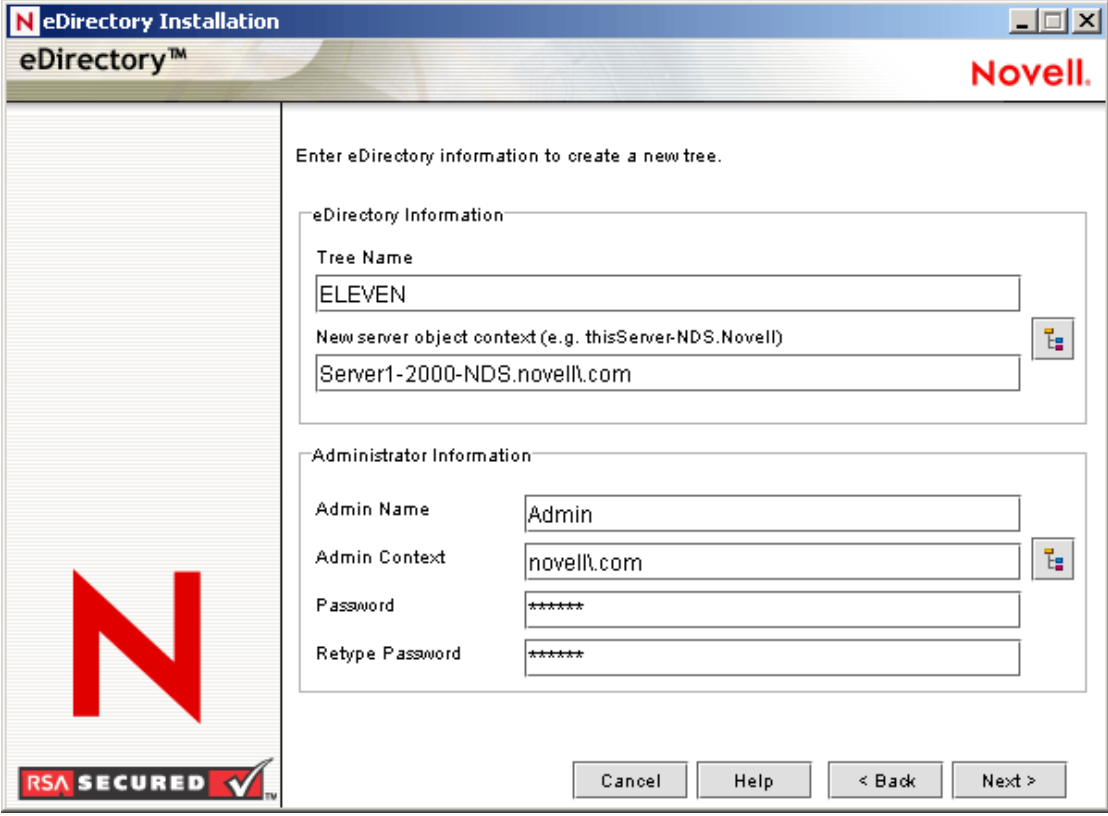
1 At a Windows client workstation, insert the *Novell eDirectory 8.8* CD.

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.

4.6.6 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 4-3 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 4-3 *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 4-4).

Figure 4-4 *iMonitor Login Screen*

4.6.7 Unattended Install and Configure to eDirectory 8.8 SP7 on Windows

eDirectory 8.8 SP7 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 or upgrade. You can perform either of the following setup using the unattended installation of eDirectory:

* Standalone installation or upgrade of eDirectory depending on whether it is a complete installation of eDirectory or not. The standalone upgrade process upgrades only the installed files.
* Configuration of installed eDirectory. If you install eDirectory, a complete configuration of eDirectory is performed. Otherwise, when you upgrade eDirectory, the installer only configures the upgraded files.
* A combination of both installation or upgrade and configuration of eDirectory. It can either be installation and configuration of eDirectory or an upgrade and configuration of only the required files.

For more information on how to mention the setup for unattended installation, refer to the section "Adding Features to the Automated Installation" on page 83.

Prerequisites

* Ensure Microsoft Visual C++ 2005 Runtime Libraries are installed. Install them manually from:

  32-bit: `vcredist_x86.exe`, located at `eDirectory\nt\i386\redist_pkg`

  64-bit: `vcredist_x86.exe` and `vcredist_x64.exe` located at `eDirectory\nt\x64\redist_pkg`

* Ensure NICI is installed:

  32-bit: `eDirectory/Windows/x64/nici/wcniciu0.exe`

  64-bit: `eDirectory/Windows/x64/nici/wcniciu0.exe`

* Set to program mode:

  Run `Windows/SysWOW64/novell/nici/set_server_mode.bat`

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 82
* "Adding Features to the Automated Installation" on page 83
* "Controlling Automated Installation" on page 88
* "Unattended Installation of eDirectory using Response File" on page 91

Response Files

Installing or upgrading to eDirectory 8.8 SP7 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 SP7 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` (for 32-bit) and `eDirectory\windows\x64\NDSonNT\response.ni` (for 64-bit) 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".

- **mode:** The type of setup on eDirectory. The three types of setup are:
  - install: Performs installation of eDirectory or an upgrade of the required files.
  - configure: Configures eDirectory. If you only perform an upgrade of the required files, then the installer only configures the upgraded files.
  - full: Performs both installation and configuration of eDirectory. This type of installation can either be installation and configuration of eDirectory or an upgrade and configuration of only the required files.

    By default, the mode key is set to full.

NOTE: If you opt for the full setup mode, then while uninstalling eDirectory you cannot opt for individual deconfiguration and uninstallation option.

- **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 `Files` 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\Files
```

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 4-5   *Installing eDirectory*
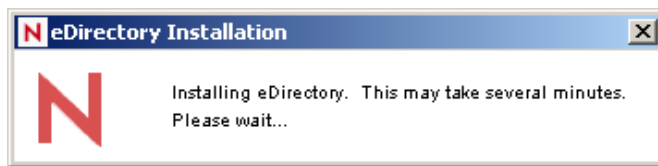
Adding NMAS Methods

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 4-1   *NMAS Methods*

Method Name	Method Type
CertMutual	Certificate mutual login method
Challenge Response	The Novell challenge response NMAS method
DIGEST-MD5	Digest MD5 login method
GSSAPI	SASL GSSAPI mechanism for eDirectory. Authentication to eDirectory through LDAP using a Kerberos ticker
NDS	NDS login method (default)
Simple Password	Simple password NMAS login method

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 4-6   *NMAS Login Method Creation*
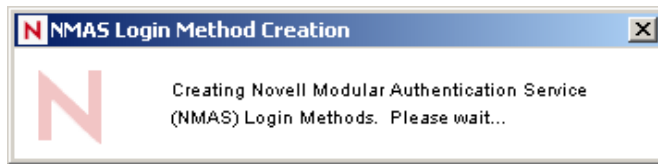
The following is sample text in the response file for choosing the NMAS methods:

```
[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 4-7 *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 DisplayLanguage 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

Configuration Mode Settings

If the setup mentioned in the mode key is configure, then ensure that you do not change the RestrictNodeRemove value of the ConfigurationMode key in the [Initialization] section.

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 4-8 *SNMP Service Shutdown*
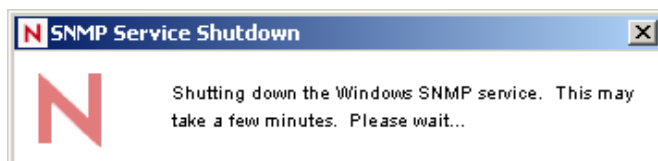
The following is sample text in the response file for stopping SNMP services:

[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 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.

Depending on the setup mode you have mentioned, use either of the following commands:

NOTE: The `nopleasewait` option used in the commands ensures that the status window for installation, upgrade, or configuration is not displayed.

Install

32-bit: *<Unzipped Location>*`\nt\I386\NDSonNT>install.exe /silent /nopleasewait /template=`*<Response file>*

For example, `D:\builds\88SP7_i386\nt\I386\NDSonNT>install.exe /silent /nopleasewait /template=D:\builds\88SP7_i386\nt\I386\NDSonNT\response.ni`

64-bit: *<Unzipped Location>*`\windows\x64\NDSonNT>install.exe /silent /nopleasewait /template=`*<Response file>*

For example, `D:\builds\88SP7_i386\windows\x64\NDSonNT>install.exe /silent /nopleasewait /template=D:\builds\88SP7_i386\nt\I386\NDSonNT\response.ni`

Configure

32-bit and 64-bit: *<Windows Drive>*`\Program Files\Common Files\novell>install.exe /silent /restrictnoderemove /nopleasewait /template=`*<Response file>*

For example, `c:\Program Files\Common Files\novell>install.exe /silent /restrictnoderemove /nopleasewait /template=D:\builds\88SP7_i386\nt\I386\NDSonNT\response.ni`

A combination of installation or upgrade and configuration of eDirectory

32-bit: *<Unzipped Location>*`\nt\I386\NDSonNT>install.exe /silent /nopleasewait /template=`*<Response file>*

For example, `D:\builds\88SP7_i386\nt\I386\NDSonNT>install.exe /silent /nopleasewait /template=D:\builds\88SP7_i386\nt\I386\NDSonNT\response.ni`

64-bit: `<Unzipped Location>\windows\x64\NDSonNT>install.exe /silent /nopleasewait /template=<Response file>`

For example, `D:\builds\88SP7_i386\windows\x64\NDSonNT>install.exe /silent /nopleasewait /template=D:\builds\88SP7_i386\nt\I386\NDSonNT\response.ni`

5 Relocating the DIB

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

5.1 Linux and UNIX

Complete the following procedure to relocate your DIB:

1 Check the server status by entering the following command at the command line:

```
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.dir
```

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

4 Copy the DIB to the new location as follows:

```
cp -rp current__location new__location
```

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

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

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

```
n4u.nds.dir=new__location
```

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

```
n4u.nds.dir=/home/nds/
```

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
```

5.2 Windows

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

6 Upgrade Requirements of eDirectory 8.8

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 6-1 *iMonitor Output showing References to an Object*

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

6.1 Reference Changes in 8.8 SP1 or later versions

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 Flexible Adaptable Information Manager (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 SP1 or later versions. 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. Therefore, 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.

6.2 Upgrade Process in 8.8 SP7

The `ndsconfig upgrade` command is used to upgrade the necessary configuration of the individual components such as HTTP, LDAP, SNMP, SAS, and NMAS. eDirectory database is upgraded to a new format if eDirectory versions prior to eDirectory 8.8 SP1 are upgraded to eDirectory 8.8 SP7.

The appropriate upgrade utility is called after the packages are upgraded to eDirectory 8.8 SP7.

A new offline database upgrade utility is available with eDirectory 8.8 SP1 onwards.

NOTE: In case 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	Windows
ndsupg	ndsupg.exe

```
SuSE:/opt/novell/eDirectory/bin #
SuSE:/opt/novell/eDirectory/bin # ./ndsdibupg --help
./ndsdibupg - DIB Upgrade Utility for Novell eDirectory 8.8 SP1 v20114.24
Usage: ./ndsdibupg [-qdv] [-l logfile] <dibdirectory>
Options:
    -q          Quite.  Do not bring up the text UI
    -d          Dry run.  Will not commit the upgraded dib
    -v[0-3]     Verbosity in log message.  This will be valid only if -l option
is given
        0       Only query messages will be logged.
        1       Only transaction messages will be logged
        2       Only general messages will be logged
        3       All messages will be logged ( default )
    -l<logfile> Log file name where messages will be logged.
SuSE:/opt/novell/eDirectory/bin #
```

The following table discusses the ndsupg options.

Table 6-1   *ndsupg 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. **IMPORTANT:** ds.nlm should be unloaded before loading dsup.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. ndsupg 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 DIB directory: /var/opt/novell/eDirectory/data/dib ####
     options

Log File: /var/opt/novell/eDirectory/log/ndsdibupg.log
Starting the DIB upgrade: Nov 25 19:52:32

Opening the DIB to start upgrade process...
Total DIB size: 158 MB
QUERY CRITERIA:
    FLD:30 == 4278190110
  AND
    FLD:33.34 == "Reference"
  {OptInfo: UsingIX=143, KeyMatch=YES, RecMatch=NO, FromKeyLen=16,
   FromKey=(1F FF 00:2 1E 02 99 87 88 87 99 87 93 83 87 05),
   UntilKeyLen=16, UntilExcl=Yes,
   UntilKey=(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=570, RecsFetched=570, RecsRejected=0, RecsNotFound=0}

#                                                    2
.
.
.
#################################################  100
Indexing progress: Index 220 is offline.  Last record processed = 84088.

DIB upgrade process completed (Nov 25 19:53:05 ).
Status: success(0)
```

6.3 Performing a Dry Run before Upgrading eDirectory

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

Here, the -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.

6.3.1 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 8.2, "Migrating to eDirectory 8.8 SP7 Without Upgrading the Operating System," on page 110 for further details.

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

Answer: The upgrade scans 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 to use the `ndsconfig upgrade` command 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.

7 Configuring Novell eDirectory on Linux, Solaris, or AIX Systems

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

7.1 Configuration Utilities

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

7.1.1 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 1.6.4, "Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 26.

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 7.2, "Configuration Parameters," on page 103 for a description of ndsconfig parameters.

IMPORTANT: After installation, ensure that you run the ndsconfig utility from the installed location on the server, which is /opt/novell/eDirectory/bin by default. Do not run ndsconfig from the installation package.

7.1.2 Using LDAP Tools to Configure the LDAP Server and LDAP Group Objects

You can use the LDAP tools included with eDirectory on Linux, Solaris, and AIX systems to modify, view, and refresh the attributes of LDAP Server and Group objects.

For more information, see "Using LDAP Tools on Linux, Solaris, or AIX" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

7.1.3 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 37.

7.1.4 Using ndsd init Script

The ndsd init script starts the daemon when the system boots up, with the configuration parameters from the default configuration file, `/etc/opt/novell/eDirectory/conf/nds.conf`.

Before invoking ndsd, ensure that any SLP (Service Location Protocol) agent is running on the host. You can install OpenSLP, any native SLP available with your operating system, or Novell SLP.

To start ndsd, enter the following:

For Linux and Solaris: `/etc/init.d/ndsd start`

For HP-UX: `/sbin/init.d/ndsd start`

To stop ndsd, enter the following:

For Linux and Solaris: `/etc/init.d/ndsd stop`

For HP-UX: `/sbin/init.d/ndsd stop`

The following shell scripts are created in `/opt/novell/eDirectory/sbin`:

- `pre_ndsd_start`
- `post_ndsd_start`
- `pre_ndsd_stop`
- `post_ndsd_stop`

As the name indicates, the `pre_ndsd_start` script is executed before the ndsd binary is started by the `/etc/init.d/ndsd` script. The `post_ndsd_start` script is executed after the ndsd binary is started by the `/etc/init.d/ndsd` script. Similarly, the `pre_ndsd_stop` and `post_ndsd_stop` scripts are executed before and after killing the ndsd process, respectively.

Users can add commands of their choice to these scripts to get them executed. By default, the `post_ndsd_start` script has commands to ensure that `/etc/init.d/ndsd` comes out after ensuring that the LDAP services are up and running.

7.2 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. You should 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.
	This option is supported only by Novell SLP and not OpenSLP.
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.

Parameter	Description
`n4u.server.signature-level`	Determines the level of enhanced security support. Increasing this value increases security, but decreases performance.
	Default = 1
	Range = 0 to 3
`n4u.nds.dir`	The eDirectory directory information database.
	Default:
	`/var/opt/novell/eDirectory/data/`
	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 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
`n4u.nds.janitor-interval`	The interval (in minutes) after which the eDirectory Janitor process is executed.
	Default = 2
	Range = 1 to 10080

Parameter	Description
n4u.nds.backlink-interval	The interval (in minutes) after which 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
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.

Parameter	Description
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 *Novell eDirectory 8.8 SP7 Tuning Guide for UNIX* Platforms* 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 the `/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 to the `nds.conf` man page.

7.3 Security Considerations

The following security considerations are recommended:

- 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 the `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 the LDAP Server object to `Use Higher Cipher (greater than 128 bit)`.

8 Migrating to eDirectory 8.8 SP7

This document guides you to migrate your Novell eDirectory 8.7.3.*x* server to eDirectory 8.8 SP7 when you have to upgrade your operating system also.

With the change in the operating systems supported in eDirectory 8.8 SP7, there are certain versions that eDirectory 8.8 SP7 does not support that were earlier supported with eDirectory 8.7.3.*x*.

There are two scenarios while migrating to eDirectory 8.8 SP7:

◆ **Migrating to eDirectory 8.8 SP7 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 SP7.

◆ **Migrating to eDirectory 8.8 SP7 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.

8.1 Migrating to eDirectory 8.8 SP7 While Upgrading the Operating System

In this scenario, you can migrate to eDirectory 8.8 SP7 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 8-1 *Migration Path*

Operating System	Starting State	Intermediate State	Desired State
Windows	Windows 2000 SP4 + eDirectory 8.7.3.x	Windows 2003 SP2 + eDirectory 8.7.3.x	Windows 2003 SP2 + eDirectory 8.8 SP7
	Windows 2003 SP2 + eDirectory 8.7.3.x	Windows 2003 SP2 + eDirectory 8.8 SP7	Windows 2008 SP2 + eDirectory 8.8 SP7
	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 file.		
Linux	SLES 9 + eDirectory 8.7.3.x	SLES 10 + eDirectory 8.7.3.x	SLES 10 + eDirectory 8.8 SP7
	RedHat AS 4.0 + eDirectory 8.8 SP2	RedHat AS 5.3 + eDirectory 8.8 SP2	RedHat AS 5.3 + eDirectory 8.8 SP7

Operating System	Starting State	Intermediate State	Desired State
Solaris	Solaris 9 + eDirectory 8.8 SP2	Solaris 10 + eDirectory 8.8 SP2	Solaris 10 + eDirectory 8.8 SP7
AIX	AIX 5.3 + eDirectory 8.8 SP6	AIX 6.1 + eDirectory 8.8 SP6	AIX 6.1 + eDirectory 8.8 SP7

Recommendations

1 Backup your eDirectory 8.7.3.*x* files before upgrading the operating system. Stop eDirectory and back up 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.

8.2 Migrating to eDirectory 8.8 SP7 Without Upgrading the Operating System

This method is used in scenarios where there is no operating system upgrade path to supported eDirectory 8.8 SP7 version.

For example, eDirectory 8.7.3.*x* is installed on SLES 9. A customer using SLES 9 wants to upgrade to eDirectory 8.8 SP7. eDirectory 8.8 SP7 is supported on SLES 11 and there is no upgrade path from SLES 9 to SLES 11.

Complete the following steps to migrate to eDirectory 8.8 SP7:

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` directory from `/var/novell` and restore the `nici` directory to `/var/opt/novell`

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

6 Install eDirectory 8.8 SP7 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 the `nds.conf` file and add the following.

```
n4u.nds.dir=_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:

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

12 Run `ndsconfig upgrade` after setting the path.

9 Migrating eDirectory from NetWare to OES 2 Linux

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 tasks, and post-migration tasks for you.

The following sections give you more details on the migration procedure for eDirectory. For more information, see the Novell Open Enterprise Server Migration Web site (http://www.novell.com/products/openenterpriseserver/migrate.html) and the *OES 2 SP3: Upgrading to OES - Best Practices Guide* (http://www.novell.com/documentation/oes2/upgrade_to_oes_lx/data/front.html).

9.1 Planning Your Migration

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

9.1.1 System Requirements

❏ The target server must run OES 2 and should have the eDirectory 8.8 SP7 RPMs already installed.

❏ If the target OES 2 server has a default eDirectory 8.8 SP7 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.

9.1.2 Prerequisites

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

9.1.3 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 9-1 *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

9.1.4 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.

9.2 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.

9.3 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.

Option	Description
`-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

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.

For more information on how to remove the eDirectory instance from a server, see Section 1.6.4, "Using the ndsconfig Utility to Add or Remove the eDirectory Replica Server," on page 26.

2 Restore and unlock the database in the source server.

For more information on how to unlock and restore the database, see "Using the eMBox Client for Backup and Restore" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

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

9.4 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 information on repairing eDirectory instance, refer to "DSRepair Options" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

10 Deploying eDirectory on High Availability Clusters

The primary method through which Novell eDirectory supports high availability is by configuring multiple servers through synchronization. However, clustering may be a more viable alternative for achieving high availability in some environments.

This section provides guidelines for configuring eDirectory on high availability clusters by using shared storage. The information in this section is generalized for shared storage high availability clusters on supported Windows and Linux platforms, and the information is not specific to a particular cluster manager.

State data for eDirectory must be located on the shared storage so that it is available to the cluster node that is currently running the services. This means that the eDirectory DIB must be located on the cluster shared storage. The root eDirectory instance on each of the cluster nodes must be configured to use the DIB on the shared storage.

In addition to the DIB, it is also necessary to share NICI (Novell International Cryptographic Infrastructure) data so that server-specific keys are replicated among the cluster nodes. NICI data used by all cluster nodes must be located on the cluster shared storage.

Other eDirectory configuration and log data should also reside on shared storage.

eDirectory 8.8 SP7 includes a utility for both Linux and Windows servers that automatically configures eDirectory in your clustered environment, including copying data to a specified shared storage location, updating the appropriate configuration parameters, and setting up eDirectory services on cluster nodes other than the primary node.

The procedures in the following sections are based on the following assumptions:

- You are familiar with eDirectory installation procedures.
- You are using a two-node cluster.

  NOTE: A two-node cluster is the minimum configuration used for high availability. However, the concepts in this section can easily be extended to a cluster with additional nodes. Note that eDirectory does not support load balancing by using multiple cluster nodes.

This section covers the following topics:

10.1 Clustering eDirectory Services on Linux

This section describes how to configure eDirectory 8.8 by using high availability clustering on Linux.

10.1.1 Prerequisites

- Two or more Linux servers with clustering software
- External shared storage supported by the cluster software, with sufficient disk space to store all eDirectory and NICI data
- Virtual IP address
- Novell eDirectory 8.8 SP7 or later

NOTE: The nds-cluster-config utility only supports configuring the root eDirectory instance. eDirectory does not support configuring multiple instances and non-root installations of eDirectory in a cluster environment.

10.1.2 Installing and Configuring eDirectory

1 Install and configure eDirectory on the server you want to use as the primary cluster node. For more information on installation and configuration procedures, refer to the Section 1.6.2, "Using the nds-install Utility to Install eDirectory Components," on page 20.

NOTE

- When configuring eDirectory, the default NCP server name is the host server name of the computer on which you installed eDirectory. Because eDirectory is hosted on multiple hosts in a clustered environment, however, you should specify an NCP server name that is unique to the cluster instead of using the default name. For example, you can specify the name `clusterserver` for the NCP server when you configure eDirectory on the primary cluster node.

- During the configuration process, ensure you set the virtual IP address for your eDirectory installation. In a clustered environment, eDirectory only listens on the virtual IP address, not on the system IP address.

2 After you install and configure eDirectory, navigate to the `nds.conf` file, which is located in the `/etc/opt/novell/eDirectory/conf`.

3 Edit the `nds.conf` file to set the value of the `n4u.nds.preferred-server` setting to the virtual IP address of the clustered installation, then save and close the file.

4 Verify the eDirectory installation by using the `ndsstat` command.

eDirectory must be up and running on the primary cluster node.

5 Mount the shared file system by using the cluster manager.

6 Back up all data in the following directories before running the configuration utility:

- `/var/opt/novell/nici`
- `/var/opt/novell/eDirectory/data` (n4u.server.vardir)
- `/var/opt/novell/eDirectory/data/` (n4u.nds.dir)

- `/etc/opt/novell/eDirectory/conf` (n4u.server.configdir)
- `/var/opt/novell/eDirectory/log`

NOTE: If you install eDirectory in a non-default location, you can use the `ndsconfig get` command to find the `vardir`, `dir` paths used in your installation. `nds.conf` should be in the default location, which is `/etc/opt/novell/eDirectory/conf/nds.conf`.

7 On the primary cluster node server, open a terminal and run the following command to stop the eDirectory service:

`ndsmanage stopall`

8 In the terminal, navigate to the location of the configuration utility, `nds-cluster-config`. The utility is located in the `/opt/novell/eDirectory/bin` directory.

9 Run the following command:

`nds-cluster-config -s /<sharedfilesystem>`

Where `<sharedfilesystem>` is the location you want to use for the eDirectory shared cluster data.

NOTE: You can also run the utility in unattended mode by using the `-u` option. If you use this option, the utility does not ask for confirmation when configuring eDirectory on a cluster.

If you use the unattended option, you must also use the `-s` option and specify the shared cluster file system.

10 After the utility verifies the cluster shared storage is valid, click *y* to continue with configuration on the cluster.

The configuration utility moves the data in the directories above to the following locations on the shared file system:

- `<sharedfilesystem>/nici`
- `<sharedfilesystem>/data`
- `<sharedfilesystem>/data/`
- `<sharedfilesystem>/conf`
- `<sharedfilesystem>/log`

11 Start eDirectory services by running the following command:

`ndsmanage startall`

12 Check the status of eDirectory by using ndsstat. eDirectory services should be up and running.

13 Stop eDirectory services by running the following command:

`ndsmanage stopall`

14 Log in to the server you want to use as the secondary node of the cluster.

15 Use the cluster manager to move the shared storage to the secondary node.

16 Install the same version of eDirectory on the secondary cluster node that you installed on the primary cluster node, but do not configure eDirectory.

17 In the terminal, navigate to the location of the configuration utility on the secondary node. The utility is located in the `/opt/novell/eDirectory/bin` directory.

18 Open a terminal and run the following command:

`nds-cluster-config -s /<sharedfilesystem>`

Where *<sharedfilesystem>* is the cluster shared storage. The path of the *<sharedfilesystem>* should be same as the path location specified when the primary node was configured.

The nds-cluster-config utility links the secondary cluster node to the shared eDirectory data located on the shared cluster file system.

19 Start eDirectory services by running the following command:

```
ndsmanage startall
```

Verify the status of eDirectory by using the `ndsstat` command.

20 Stop eDirectory services on the secondary node by running the `ndsmanage stopall` command.

21 After successfully configuring eDirectory on both nodes of the cluster, you must also change the startup mode of the ndsd service on each node by using the following command:

```
chkconfig -d ndsd
```

22 After the configuration utility finishes configuring the secondary node, you can use the cluster manager to add the eDirectory services in the cluster.

IMPORTANT: Ideally, the cluster manager checks that the same DIB is not accessed by two or more nodes simultaneously. However, you must ensure that ndsd does not run from two or more cluster nodes simultaneously. This is because accessing the same DIB through two or more nodes leads to DIB corruption.

10.1.3 Configuring SNMP Server in Clustered Linux Environments

1 On all the nodes, modify the `snmpd.conf` file. For more information, see "Installing and Configuring SNMP Services for eDirectory" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

2 Start ndssnmpsa.

3 Select Yes as the `Remember password` option.

4 To start the snmp service, perform either of the following:

   ◆ Add `/etc/init.d/ndssnmpsa start` to the `post_ndsd_start` script and `/etc/init.d/ndssnmpsa stop` to the `pre_ndsd_stop` script.

   ◆ Add `ndssnmpsa` as a cluster resource with a dependency on eDirectory resource.

NOTE: Because eDirectory is listening on a virtual IP address, traps have the IP address of the host, which is the Agent IP address.

10.2 Clustering eDirectory Services on Windows

This section describes how to configure eDirectory 8.8 by using high availability clustering on Windows.

   ◆ Section 10.2.1, "Prerequisites," on page 120
   ◆ Section 10.2.2, "Installing and Configuring eDirectory," on page 121
   ◆ Section 10.2.3, "Configuring SNMP Server in Clustered Windows Environments," on page 122

10.2.1 Prerequisites

   ◆ Two or more Windows servers with clustering software

- External shared storage supported by the cluster software
- Virtual IP address
- Novell eDirectory 8.8 SP7 or later

10.2.2 Installing and Configuring eDirectory

1 Install and configure eDirectory on the server you want to use as the primary cluster node. For more information on installation and configuration procedures, refer to the Section 4.6.1, "Installing or Updating Novell eDirectory 8.8 on a Windows Server," on page 75.

2 Mount the shared volume by using the cluster manager.

3 Back up all DIB files and NICI data before running the configuration utility.

4 On the primary cluster node, open a terminal and navigate to the `NDSCons.exe` utility. The utility is located in the *`<eDirectory installation folder>`* folder by default.

5 In the terminal, run the following command:

```
NDSCons.exe
```

6 In the NDSCons utility, click *Shutdown* to stop all eDirectory services.

7 Click *Yes* to confirm.

8 In the terminal, navigate to the location of the configuration utility, `dsclusterconfig.exe`. The utility is located in the <eDirectory installation folder> folder by default.

9 Run the following command:

```
dsclusterconfig.exe -s /<sharedfilesystem>
```

Where *`<sharedfilesystem>`* is the location you want to use for the eDirectory shared cluster data.

NOTE

- You can also run the utility in unattended mode by using -s with `-u` option.
- You must specify a folder within a shared drive mounted on the primary cluster node. You cannot specify only a drive name. For example, instead of specifying `E:`, you must specify `E:\Novell`.

---

10 After the utility verifies the cluster shared storage is valid, click *y* to continue with configuration on the cluster.

The configuration utility moves the data in the directories above to the following locations on the shared file system:

- *`<sharedfilesystem>`*`/nici`
- *`<sharedfilesystem>`*`/Files`

In addition to moving eDirectory data to the shared file system, the utility copies the eDirectory service registry key to the shared volume, saving the key as the file `ndsConfigKey`.

The utility also changes the Startup Type of the `NDS Server` service on the primary node computer from `Automatic` to `Manual`.

11 In the NDSCons utility, click *Startup* to start all eDirectory services.

12 Verify that all eDirectory services are running, then use the NDSCons utility to stop services again.

13 Close the NDSCons utility.

14 Log in to the server you want to use as the secondary node of the cluster.

15 Use the cluster manager to move the shared storage to the secondary node.

16 Use the eDirectory installer to perform an unattended installation of eDirectory on the secondary node. Ensure that the mode of installation is `install`.

17 In the terminal, navigate to the location of the configuration utility on the secondary node. The utility is located in the eDirectory installation folder by default.

18 Run the following command:

```
dsclusterconfig.exe -s /<sharedfilesystem>
```

Where `<sharedfilesystem>` is the cluster shared storage. The path of the `<sharedfilesystem>` should be same as the path location specified when the primary node was configured.

19 The dsclusterconfig utility updates registry on the secondary cluster node to the shared eDirectory data located on the shared cluster file system.

20 After the configuration utility finishes configuring the secondary node, open the NDSCons utility.

21 In the NDSCons utility, click *Startup*.

22 Click *Yes* to confirm.

23 When NDSCons starts all eDirectory services, verify eDirectory, then click *Shutdown*.

24 Click *Yes* to confirm.

25 To configure eDirectory in the Cluster Resource group, create a new resource in the Resource Group to be used for eDirectory.

You must provide the following details:

- Resource type - Generic Service
- Dependent on - IP address and shared disk in the Resource Group
- Service name - `NDS Server0`
- No start parameters
- Registry keys - `SYSTEM\CurrentControlSet\Services\NDS Server0`

NOTE: Ideally, the cluster manager checks that the same DIB is not accessed by two or more nodes simultaneously. However, you must ensure that ndsd does not run from two or more cluster nodes simultaneously. This is because accessing the same DIB through two or more nodes leads to DIB corruption.

10.2.3 Configuring SNMP Server in Clustered Windows Environments

1 On the primary cluster node, configure the master agent and set the startup type to automatic. For more information, see "Installing and Configuring SNMP Services for eDirectory" in the *Novell eDirectory 8.8 SP7 Administration Guide*.

2 Save the eDirectory password when it prompts for the password.

3 Start the sub-agent.

4 Perform Step 1 to Step 3 on the other nodes.

10.3 Troubleshooting Clustered Environments

10.3.1 Repairing or Upgrading eDirectory on Clustered Nodes

While you perform a repair or upgrade on any of the cluster nodes, the other cluster nodes must be paused or on standby to ensure that automatic failover does not occur.

10.3.2 Creating Windows Registry Keys

As part of the configuration process in clustered Windows environments, the configuration utility automatically creates a registry key,
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NDS Server0\ImagePath`, on the cluster shared file system. eDirectory needs the registry key in order to start the `x86 NDS Server` service on the cluster nodes.

If the utility cannot create the registry key and returns an error message during configuration, you must use the Registry Editor to manually create the registry key on all cluster nodes, even if the configuration utility appears to have successfully completed the configuration.

Create the following registry key on all nodes:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NDS Server0\ImagePath`

Assign the following value to the `ImagePath` key:

`"<primarynodeinstallfolder>\NDS\ndsserv.exe" /DataDir="<sharedstorage>\Files" ds`

Where `<primarynodeinstallfolder>` is the folder where you installed eDirectory on the primary node and `<sharedstorage>` is the path to the shared file system location.

10.4 Configuration Utility Options

The options available for use in the configuration utility are as follows:

`<configuration utility> [-h] [-u] [-s /<sharedfilesystem>]`

Where `<configuration utility>` is either `nds-cluster-config` or `dsclusterconfig.exe`, depending on the platform, and `<sharedfilesystem>` is the location you want to use for the eDirectory shared cluster data.

Parameter	Description
-h	Displays the configuration utility help.
-s	Specifies the shared directory path for the cluster.
-u	Enables the utility to configure eDirectory on the cluster in unattended mode.
	If you run the utility by using the -u option, you must also use the -s option and specify the shared directory path. For example:
	`nds-cluster-config -u -s <sharedfilesystem>`

11 Uninstalling Novell eDirectory

This chapter contains the following information:

11.1 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 SP7 Administration Guide*.

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

11.1.1 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.

11.1.2 Unattended Uninstallation of eDirectory

On Windows, the unattended uninstallation of eDirectory uses predefined text files that facilitate the unattended uninstallation.You can perform the following actions by using the unattended uninstallation mode of eDirectory:

- Deconfiguration of the installed eDirectory.
- Standalone uninstallation of eDirectory.
- Both uninstallation and deconfiguration of eDirectory.

The following sections discuss various features of unattended eDirectory uninstallation:

- "Response Files" on page 126
- "remove.rsp File Sections and Keys" on page 126
- "Add Features to the Automated Uninstallation" on page 127
- "Remove Configuration File Changes" on page 128
- "Unattended Uninstallation of eDirectory using Response File" on page 128

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 by 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` (for 32-bit) and `eDirectory\windows\x64\NDSonNT\remove.rsp` (for 64.bit) 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.

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 `Files` subfolder inside the NDS location, but administrators can change this parameter and provide a different location

mode: The type of setup on eDirectory. The three types of setup are:

- deconfigure: Performs the deconfiguration of eDirectory.
- uninstall: Performs uninstallation of eDirectory.
- full: Performs both deconfiguration and uninstallation of eDirectory.

NOTE: If you opt for the full setup mode during unattended install, then while uninstalling eDirectory you cannot opt for individual deconfiguration and uninstallation option.

ConfigurationMode: If the setup mentioned in the mode key is deconfigure, then ensure that you do not change the `RestrictNodeRemove` value of the `ConfigurationMode` key

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 the `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. Depending on the required setup, you must use either of the following commands:

Deconfigure

```
<Windows Installed Drive>\Program Files\Common Files\novell\ni\bin>install.exe -
remove /restrictnoderemove /nopleasewait ..\data\ip.db ..\data\remove.rsp
Novell:NDSForNT:1.0.0 0 NDSonNT
```

Uninstall

1 Rename the `ip.db` file present in the *<Windows Drive>*\Program Files\Common Files\novell\ni\data directory to another name.

2 Copy the `ip_conf.db` file in the *<Windows Drive>*\Program Files\Common Files\novell\ni\data folder to `ip.db`.

3 Run the following command:

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

Deconfiguration and Uninstallation of eDirectory

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

After performing an uninstallation of eDirectory or combination setup, delete the following folders:

- `C:\Novell\NDS` (default location, or else from the eDirectory installed directory)
- `C:\Novell\NDS\Files` (default location, or else from the eDirectory DIB location)
- `<Windows Installed Drive>:\Program Files\Common Files\Novell\ni`
- `<Windows Installed Drive>:\Windows\system32\NDScpa.cpl`

11.1.3 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:\Windows\system32\novell\nici` (32-bit) and `C:\Windows\SysWOW64\novell\nici` (64-bit) 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.

11.1.4 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 by using the following procedure:

1. Navigate to *Add/Remove Programs* or *Programs and Features* on the Windows server where eDirectory is installed.
2. Remove the following redistribution package:

   32-bit: `Microsoft Visual C++ 2005 Redistributable`

   64-bit: `Microsoft Visual C++ 2005 Redistributable` and `Microsoft Visual C++ 2005 Redistributable (x64)`

11.2 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. This utility is available at `/opt/novell/eDirectory/sbin/nds-uninstall`. However, `ndsconfig rm` is not supported on OES2 SP2 or later versions.

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 SP7 Administration Guide*.

1 Execute the `nds-uninstall` command.

2 Use the following syntax:

```
nds-uninstall [-s][-h]
```

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

Paramet er	Description
-h	Displays the help strings.
-s	Removes the eDirectory packages and binaries even when instances are configured. However, this option does not remove the DIB directory and the NDS configuration file.
	IMPORTANT: Ensure that using this option is not affecting other services for a long period.

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

11.3 Unattended Uninstallation of eDirectory on UNIX

1 Remove the instances of eDirectory:

```
ndsconfig rm -a <user name> -w passwd -c
```

2 Use either of the following in the automated script for the de-configuration of eDirectory:

Passing the password through environment variable: `ndsconfig rm -a <user name> -w env:<environment variable> -c`

Passing the password through file: `ndsconfig rm -a <user name> -w file:<filename with absolute/relative path> -c`

3 (Optional) In case of multiple instances, run the following command for individual instances:

```
ndsconfig rm -a <user name> -w passwd  --config-file <absolute path for
configuration file>
```

For example:

```
ndsconfig rm -a admin.novell -w n -c
```

```
ndsconfig rm -a admin.novell -w env:ADM_PASWD -c
```

```
ndsconfig rm -a admin.novell -w file:/Builds/88SP7/adm_paswd -c
```

4 To uninstall the eDirectory packages, run the nds-uninstall script to remove the eDirectory packages:

```
nds-uninstall -u
```

11.4   Caveats for Uninstalling eDirectory

When you uninstall eDirectory and install it again, the eDirectory server cannot be accessible to the other servers in the network. All the distributed operations such as synchronization and obituary processing do not take place on the partitions whose replicas are present in the eDirectory server. If this state persists for a while, it might impact all the servers and the processes running on them.

Avoid uninstalling a newer version of eDirectory and install an earlier version, because:

- ◆ Does not revert the schema related upgrades.
- ◆ eDirectory might not be functional if DIB is upgraded to the newer version.
- ◆ Removes all the existing configuration files, except for the nds.conf.

However, consider the following when you uninstall a newer version of eDirectory and install an earlier version:

- ◆ Upgrade the DIB to the newer version. Else, eDirectory might not be functional.
- ◆ Back up the existing configuration files, except for the nds.conf, and restore when eDirectory is installed again.
- ◆ Does not revert the schema related upgrades.

12 Auditing eDirectory Events

You can audit eDirectory events in one of the following ways:

12.1 Auditing with Novell Audit

Using the Novell Audit package, you can send events generated by eDirectory to an outside auditing client for monitoring purposes.

Earlier eDirectory instrumentation was a part of Novell Audit. However, from eDirectory 8.8 SP3 version onwards, eDirectory instrumentation is bundled with eDirectory. You need to install this package for auditing eDirectory events with Novell Audit.

Use the following information to install, configure, or uninstall Novell Audit on Linux, Solaris, and Windows servers:

12.1.1 Supported Platforms

NOTE: eDirectory does not support auditing events on servers running AIX.

32-Bit eDirectory

Linux

32-bit

- SUSE Linux Enterprise Server (SLES) 11
- SLES 10 SP1, SP2 and SP3
- SLES 10 SP1, SP2 and SP3 XEN
- Red Hat Enterprise Linux (RHEL) 5**
- RHEL 5** AP
- RHEL 5** AP Virtualization
- RHEL 6.0

64-bit

- SLES 11 64-bit
- SLES 10 SP1, SP2, SP3 64-bit
- SLES 10 SP1, SP2 and SP3 XEN 64-bit
- RHEL 5** 64-bit
- RHEL 5** AP 64-bit
- RHEL 5** AP Virtualization 64-bit
- RHEL 6.0

Solaris

- Solaris* 10 on Sun SPARC

Windows

- 32-bit Windows* 2003 Enterprise Server SP2
- 32-bit Windows* 2008 Server (Standard/Enterprise/Data Center Edition)

** Latest service pack

64-bit eDirectory

Linux

- SLES 11 64-bit
- SLES 10 SP1, SP2 and SP3 64-bit
- SLES 10 SP1, SP2 and SP3 XEN 64-bit
- RHEL 5** 64-bit
- RHEL 5** AP 64-bit

- RHEL 5** AP Virtualization 64-bit
- RHEL 6.0

Solaris

- Solaris* 10 on Sun SPARC

Windows

- 64-bit Windows* 2008 Server (Standard/Enterprise/Data Center Edition)
- Windows 2008 R2 Server (Standard/Enterprise/Data Center Edition)

**- Latest service pack

12.1.2 Prerequisites

❑ eDirectory 8.8 SP7 auditing supports only the Audit Platform Agent.

❑ Installing and using the Novell Audit iManager Plug-in requires iManager 2.7.3 or later. For more information, refer to the Novell iManager Documentation Page (http://www.novell.com/documentation/imanager27/index.html).

12.1.3 Installing Novell Audit Packages

- "Linux" on page 135
- "Solaris" on page 136
- "Windows" on page 137

Linux

If the Audit Platform Agent configuration file (`logevent.conf`) already exists in the `/etc`, back up the file before installing the Audit packages, because the new package overwrites the existing configuration.

If the Audit module is already loaded, unload the `auditds` module by using the `ndstrace -c "unload auditds"` command.

For OES 2 SP3 32-bit, you must download the eDirectory standalone build for Linux 32-bit from the Novell Downloads (http://download.novell.com/) Web site. Extract the build and use the `novell-AUDTedirinst-8.8.7-xx.i586.rpm` file.

For OES 2 SP3 64-bit, you must download the eDirectory standalone build for Linux 64-bit from the Novell Downloads (http://download.novell.com/) Web site. Extract the build and use the `novell-AUDTedirinst-8.8.7-xx.x86_64.rpm` file.

For the 32-bit Audit package:

1 Install `novell-AUDTplatformagent-2.0.2-62.i586.rpm` from the setup directory of the extracted eDirectory build for the Linux platform.

```
#rpm -Uvh /root/eDirectory/setup/novell-AUDTplatformagent-2.0.2-62.i586.rpm
```

2 Install `novell-AUDTedirinst-8.8.7-xx.i586.rpm` from the setup directory of the extracted eDirectory build for the Linux platform.

`#rpm -Uvh /root/eDirectory/setup/novell-AUDTedirinst-8.8.7-xx.i586.rpm`

For the 64-bit Audit package:

1 Install `novell-AUDTplatformagent-2.0.2-62.x86_64.rpm` from the setup directory of the extracted eDirectory build for the Linux platform.

`#rpm -Uvh /root/eDirectory/setup/novell-AUDTplatformagent-2.0.2-62.x86_64.rpm`

2 Install the `novell-AUDTedirinst-8.8.6-xx.x86_64.rpm` from the setup directory of the extracted eDirectory build for the Linux platform.

`#rpm -Uvh <eDirectory build extracted folder>/eDirectory/setup/novell-AUDTedirinst-8.8.6-xx.x86_64.rpm`

Run `ndstrace -c "load auditds"` to load the `auditds` module. This step is common for loading the Audit module on both 32 and 64-bit eDirectory.

Solaris

If the Audit Platform Agent configuration file (`logevent.conf`) already exists in the `/etc`, then back up the file before installing the Audit packages, as the new package overwrites the existing configuration.

If the Audit Platform Agent is already loaded, unload `auditds` module by using `ndstrace -c "unload auditds"` command.

For 32-bit Audit package

Install `NOVLaudpa.pkg` from the setup directory of the extracted eDirectory build for the Solaris platform.

For example,

`#pkgadd -a <eDirectory build extracted folder>/eDirectory/setup/admin.audit -d <path to the downloaded Audit Platform Agent location>/NOVLaudpa.pkg all`

`#pkgadd -a <eDirectory build extracted folder>/eDirectory/setup/admin.audit -d <eDirectory build extracted folder>/eDirectory/setup/NOVLaudin.pkg`

For 64-bit Audit package

Install `NOVLaudpax.pkg` from the setup directory of the extracted eDirectory build for the Solaris platform.

For example:

`#pkgadd -a <eDirectory build extracted folder>/eDirectory/setup/admin.audit -d <path to the downloaded Audit Platform Agent location>/NOVLaudpax.pkg all`

`#pkgadd -a <eDirectory build extracted folder>/eDirectory/setup/admin.audit -d <eDirectory build extracted folder>/eDirectory/setup/NOVLaudinx.pkg`

Windows

If the Audit Platform Agent configuration file (`logevent.cfg`) already exists in the `C:\WINDOWS`, back up the file before installing instrumentation, because the new package overwrites the existing configuration.

For 32-bit installation of Audit packages and Audit Platform Agent:

1 Run the `pa_win32.exe` file for 32-bit Audit Platform Agent from the installer folder.

2 Unzip the `eDirectoryInstrumentation-win-8.8.7.zip` file for 32-bit Instrumentation from the `<installerFolder>`/nt/auditds/. Unzipping this file creates a `Novell` directory.

3 Copy the `Novell\NDS\nauditds.dlm` to the `C:\Novell\NDS` directory or to any other directory where eDirectory is installed.

4 Copy the `Novell\NDS\ediraudit.sch` file to the `C:\Novell\NDS` directory or to any other directory where eDirectory is installed on the Windows server.

For 64-bit installation of Audit packages and Audit Platform Agent:

1 Run the `pa_win64.exe` file for 64-bit Audit Platform Agent.

2 Unzip the `eDirectoryInstrumentation-win-8.8.7.zip` file for 64-bit Audit package from the `<installerFolder>`/nt/auditds/. Unzipping this file creates a `Novell` directory.

3 Copy the `Novell\NDS\nauditds.dlm` to the `C:\Novell\NDS` directory or to any other directory where eDirectory is installed.

4 Copy the `Novell\NDS\ediraudit.sch` file to the `C:\Novell\NDS` directory or to any other directory where eDirectory is installed on the Windows server.

12.1.4 Installing the Novell Audit iManager Plug-in

To configure auditing of eDirectory events using the Novell Audit Platform Agent, you must first install the Novell Audit plug-in for iManager.

Installing and using the Novell Audit iManager plug-in requires iManager 2.7.4 or later. See the *iManager Installation Guide* (https://www.netiq.com/documentation/imanager27/imanager_install_275/data/hk42s9ot.html) for iManager installation requirements and download instructions.

The Novell Audit iManager plug-in is bundled with eDirectory 8.8 SP6 plug-ins. eDirectory 8.8 SP6 plug-ins can be downloaded from the Novell download site (http://download.novell.com/SummaryFree.jsp?buildid=EKamexBB_F4~).

The installation instructions are available on the eDirectory 8.8 Plug-ins for iManager 2.7 download page (http://www.novell.com/documentation/edir88/esd/ii_edir886_iman_27_plugins.html).

12.1.5 Understanding eDirectory Event Reporting

eDirectory uses two different event reporting systems to log events, *journal* and *inline*. By default, eDirectory logs events using journal event reporting, but you can enable inline event reporting in iManager. For more information about enabling inline event reporting, see Section 12.1.9, "Configuring Novell Audit for eDirectory," on page 140.

Journal: This reporting system provides synchronous post-event reporting. With journal event reporting enabled, when an event is generated, eDirectory adds the event to the journal event processing queue. eDirectory then uses a separate thread to process events in the queue and sends those events to the auditing client.

Inline: This reporting system provides synchronous pre-event reporting. With inline event reporting enabled, when an event is generated, eDirectory uses the same thread to send the event directly to the client. Note that enabling inline event reporting can affect eDirectory performance.

12.1.6   Understanding eDirectory Event Types

You can configure eDirectory to log events in the following categories:

- Meta
- Objects
- Attributes
- Schema
- Connections
- Agent
- Miscellaneous
- Bindery
- Replica
- Partition
- LDAP

We recommend auditing the following default set of event types:

Category	Event Type
Meta	All event types
Objects	- Add Property - Allow Login - Change Password - Change Security Equals - Create - Delete - Delete Property - Login - Logout - Modify RDN - Move (Destination) - Move (Source) - Remove - Rename - Restore - Search - Verify Password
Attributes	All event types

Category	Event Type
Agent	◆ DS Reloaded
	◆ Local Agent Closed
	◆ Local Agent Opened
	◆ NLM Loaded
Miscellaneous	◆ Generated CA Keys
	◆ Recertified Public Key
LDAP	◆ LDAP Bind
	◆ LDAP Modify
	◆ LDAP Password Modify
	◆ LDAP Add Response
	◆ LDAP Unbind
	◆ LDAP Delete
	◆ LDAP Modify DN
	◆ LDAP Modify Response
	◆ LDAP Search
	◆ LDAP Bind Response
	◆ LDAP Delete Response
	◆ LDAP Add
	◆ LDAP Search Response
	◆ LDAP Modify DN Response

12.1.7 Understanding eDirectory Auditing Event Filtering

You can also filter events for one or more specific object classes or attributes, depending on the event type. eDirectory evaluates all generated events against the configured filters on the eDirectory server and sends *only* events matching those filters through to the auditing client.

Multiple filters filter eDirectory events separately. For example, if you configure filtering on both a specific object class and one or more attributes, eDirectory sends events matching *any* of those filters to the client. You cannot configure filtering so that eDirectory sends only events of a certain object class *and* certain attributes to the client. You can select multiple object classes or attributes for which you want to filter eDirectory events.

NOTE: You can only filter a combined maximum of 256 object classes and attributes.

Click one of the following hyperlinked event types to select one or more object classes or attributes to filter for that event type:

Category	Event Type	Filtering Type
Objects	◆ Create	Object Class
	◆ Delete	

Category	Event Type	Filtering Type
Attributes	◆ Add Value ◆ Delete Value	Object Class or Attribute
LDAP	◆ LDAP Modify ◆ LDAP Delete ◆ LDAP Modify DN ◆ LDAP Add	Object Class

For example, if you want to be notified when someone creates a user account in eDirectory, you can create a filter using iManager to look for only Create Object events that create a User object.

In iManager, navigate to *Roles and Tasks > eDirectory Auditing > Audit Configuration*, select the NCP Server you want to monitor, and then click the *Novell Audit* tab. In the Objects list, click the *Create* hyperlink. In the *Available Object Classes* list, select *User*, then click the right arrow to move *User* to the *Selected Object Classes* list, and then click *OK*.

With the filter configured, eDirectory checks all generated events for user-creation events and sends those events to the client. If you do not select other event types or configure filtering for other object classes or attributes, eDirectory *only* audits user-creation events.

Note that Object and LDAP category filters only allow you to filter on object classes, while Attribute category filters allow you to filter on both object classes and attributes.

If you select one of the event types above but do not specify an object class or attribute on which to filter, eDirectory sends all events of that event type to the client.

12.1.8 Configuring the Novell Audit Platform Agent

If the Audit Platform Agent is not already configured, edit the Platform Agent configuration file to set the Audit Server's host address in the LogHost. The configuration file is located by default at the following directory:

- ◆ Linux: /etc/logevent.conf
- ◆ Windows: *Windows_directory*\logevent.cfg

For example, modify the LogHost attribute as follows:

```
LogHost=192.168.1.8
```

For more information, refer to the "Configuring the Audit Platform Agent" (http://www.novell.com/documentation/novellaudit20/novellaudit20/data/al36zjk.html) section in the *Novell Audit 2.0 Administration Guide.*

12.1.9 Configuring Novell Audit for eDirectory

Follow the procedure below to use iManager to configure auditing of eDirectory events with the Novell Audit Platform Agent.

NOTE: For information about configuring XDASv2 auditing, see the *Novell XDASv2 Administration Guide* .

Using iManager, select the eDirectory event types that you want to audit:

1 Log in to the iManager console using the following URL:

`https://`*`ip_address_or_DNS`*`/nps/`

where *`ip_address_or_DNS`* is the IP address or DNS name of your iManager server. For example:

`https://192.168.0.5/nps/`

2 Under *Roles and Tasks*, select *eDirectory Auditing > Audit Configuration*.

3 Browse to and select the NCP Server object that corresponds to the eDirectory Server from which you want to collect events. Click *OK*.

4 Click the *Novell Audit* tab to display the eDirectory Instrumentation Settings page.

5 *If you do not want eDirectory to send replicated events to another replica in the replica ring,* select *Do Not Send Replicated Events*. You can use this option to filter out unnecessary event noise and reduce log size.

6 *If you want to enable inline pre-event reporting,* select *Register For Events Inline*. Note that selecting this option can slow eDirectory performance.

7 Select the event types that you want to audit.

8 *If you want to filter events for one or more specific object classes,* complete the following steps:

    8a Click one of the following hyperlinked objects:

- *Objects > Create*
- *Objects > Delete*
- *Attributes > Add Value*
- *Attributes > Delete Value*
- *LDAP > LDAP Add*
- *LDAP > LDAP Modify*
- *LDAP > LDAP Delete*
- *LDAP > LDAP Modify DN*

    8b In the *Available Object Classes* list, select the object classes for you want to audit events and click the right arrow.

    8c Click *OK*, then click *OK* again.

9 *If you want to filter events for one or more specific attributes,* complete the following steps:

    9a Click one of the following hyperlinked objects:

- *Attributes > Add Value*
- *Attributes > Delete Value*

    9b In the *Available Attributes* list, select the attributes for you want to audit events and click the right arrow.

    9c Click *OK*, then click *OK* again.

> **NOTE:** eDirectory evaluates events individually against all filters, so if an event matches one filter but not another, eDirectory still sends the event to the client. For more information about filtering events, see Section 12.1.7, "Understanding eDirectory Auditing Event Filtering," on page 139.

10 Click *Apply*, then click *OK*.

Changes to your auditing configuration take effect within three minutes. If you want to immediately apply changes, you can also unload and then reload the Audit module. For more information about loading the audit module, see Section 12.1.10, "Loading the Audit Module," on page 142.

12.1.10 Loading the Audit Module

Use the following procedures to load or unload the Audit module.

- "Linux" on page 142
- "Windows" on page 142

Linux

1 Run the following command to load the Audit module if it is not already loaded:

   ndstrace -c "load auditds"

2 Run the following command to unload the Audit module:

   ndstrace -c "unload auditds"

   NOTE: Step 1 and Step 2 are common for 32 and 64-bit eDirectory.

3 To automatically load Audit modules when eDirectory is started, edit the /etc/opt/novell/eDirectory/conf/ndsmodules.conf file and add the following line:

   auditds   auto   #eDirectory instrumentation

Windows

1 To load the Audit module, click *Start > Control Panel > Novell eDirectory Services*. Select *nauditds* from the Services tab, then click *Start*.

2 To unload the Audit module, click *Start > Control Panel > Novell eDirectory Services*. Select *nauditds* from the Services tab, then click *Stop*.

   NOTE: Step 1 and Step 2 are common for 32 and 64-bit eDirectory.

3 To automatically load the Audit module when eDirectory is started, complete the following steps:

   3a Click *Start > Control Panel > Novell eDirectory Services*.

   3b Select *nauditds* from the *Services* tab, then click *Startup.*

   3c Select *Automatic*, then click *OK*.

4 To disable automatic loading of Audit module when eDirectory is started, complete the following steps:

   4a Click *Start > Control Panel > Novell eDirectory Services*.

   4b Select *nauditds* from the *Services* tab, click *Startup.*

   4c Deselect the *Automatic* check box, then click *OK*.

12.1.11 Monitoring eDirectory Events with Sentinel

Novell Sentinel provides a Collector for collecting and auditing eDirectory events. In order to monitor some types of eDirectory events in Sentinel, you must ensure that certain eDirectory auditing settings are configured properly.

For detailed information on configuring auditing settings, see Section 12.1.9, "Configuring Novell Audit for eDirectory," on page 140.

For information on configuring Sentinel to collect eDirectory events, see the *Sentinel Collector Guide for Novell eDirectory*, located on the Sentinel Plug-ins site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Auditing Create Object Events

When creating an object that will be used as an account, eDirectory first creates a generic object, then modifies the object class to a user type with an Add Value event. If you want Sentinel to properly collect the event, you must enable auditing of Add Value events in iManager. If you do not enable Add Value event auditing, the Sentinel Collector cannot parse Create Object events and will generate a "Configuration Error" event in Sentinel.

To enable auditing of Create Object events, launch iManager and navigate to the *eDirectory Auditing > Audit Configuration > Novell Audit* window. Select both *Objects > Create* and *Attributes > Add Value*.

Auditing LDAP Events

eDirectory considers each LDAP request to be a transaction, and generates events when a request is initiated and when a response is received and the transaction is completed.

In Sentinel, however, each request-response pair is treated as one event. In order to audit a type of LDAP event in eDirectory using Sentinel, you must enable auditing for both the request event and the response event. For example, to audit an LDAP bind request, you must configure auditing for both LDAP Bind and LDAP Bind Response events in iManager.

Auditing Failed Login Events

If you want to monitor failed login events in eDirectory, you must use iManager to enable auditing on Add Value events on the eDirectory server. You must also enable Intruder Detection on the eDirectory container or containers where you want to audit failed login events.

IMPORTANT: You must enable Intruder Detection and Add Value event auditing on each server with a replica of the container you want to monitor.

Use the following procedure to enable Intruder Detection on a container:

1 Log in to the iManager console using the following URL:

```
https://ip_address_or_DNS/nps/
```

where `ip_address_or_DNS` is the IP address or DNS name of your iManager server. For example:

```
https://192.168.0.5/nps/
```

2 Under *Roles and Tasks*, select *Directory Administration > Modify Object*.

3 Browse to and select the eDirectory container you want to audit. Click *OK*.

4 On the General tab, click *Intruder Detection*.

5 Select *Detect intruders*.

6 Click *OK*.

NOTE: You do not need to configure any other Intruder Detection-related settings or enable the *Lock account after detection* setting.

12.1.12 Uninstalling the Novell Audit Packages

The following sections explain how to uninstall the Novell Audit packages:

- ◆ "Uninstalling Audit Packages on Linux" on page 144
- ◆ "Uninstalling Audit Packages on Solaris" on page 144
- ◆ "Uninstalling Audit Packages on Windows" on page 145

Uninstalling Audit Packages on Linux

To uninstall Audit packages on Linux:

1 Unload the Audit module by using the command `ndstrace -c unload auditds`.

2 Uninstall the `novell-AUDTedirinst-8.8.6-`*xx* RPM.

NOTE: The rpm name is same for both 32 and 64-bit Audit packages.

`#rpm -e --nodeps novell-AUDTedirinst-8.8.6-`*xx*

3 Disable automatic loading of Audit modules when eDirectory is started by editing the `/etc/opt/novell/eDirectory/conf/ndsmodules.conf` file and removing the line corresponding to auditds (if it exists). The line corresponding to auditds is as follows:

`auditds      auto     #eDirectory Instrumentation`

NOTE: If no other auditing is installed, then uninstall the `novell-AUDTplatformagent-2.0.2-62` Audit Platform Agent by using `#rpm -e novell-AUDTplatformagent-2.0.2-62` command. The RPM name is same for both 32 and 64-bit auditing packages.

Uninstalling Audit Packages on Solaris

To uninstall Audit packages on Solaris:

1 Unload the Audit module by using the `ndstrace -c "unload auditds"` command.

2 Uninstall the `NOVLaudin` package for 32-bit Audit and `NOVLaudinx` package for 64-bit Audit.

For example the package can be uninstalled using the following commands:

`#pkgrm NOVLaudin`

`#pkgrm NOVLaudinx`

3 Disable automatic loading of Novell Audit when eDirectory is started by editing the `/etc/opt/novell/eDirectory/conf/ndsmodules.conf` file and removing the line corresponding to auditds (if it exists). The line corresponding to auditds is as follows:

`auditds      auto     #eDirectory Instrumentation`

NOTE: If no other instrumentation is installed then uninstall the `NOVLaudpa` Audit Platform Agent package for 32-bit Audit package and `NOVLaudpax` Audit Platform Agent package for 64-bit Audit package. For example, the package can be removed using the `#pkgrm NOVLaudpa` command and the `#pkgrm NOVLaudpa` command.

Uninstalling Audit Packages on Windows

On Windows, the procedure to uninstall 32-bit Audit packages and 64-bit Audit packages is same.

To uninstall Audit packages on Windows:

1 Unload the Audit module as follows:

   1a Navigate to *Start > Control Panel > Novell eDirectory Services.*

   1b Select *Services*.

   1c Click `nauditds.dlm`, then click *Stop*.

2 Delete `nauditds.dlm` from the `C:\Novell\NDS` directory.

3 Delete the `ediraudit.sch` file from the `C:\Novell\NDS` directory.

4 Complete the following steps to disable automatic loading of Audit packages when eDirectory is started:

   4a Navigate to *Start > Control Panel > Novell eDirectory Services*.

   4b Select *Services*.

   4c Click `nauditds.dlm`, then click *Startup*.

   4d Disable the `Automatic` option by clearing the check-box.

   4e Click *OK*.

NOTE: If no other instrumentation is installed, uninstall the Audit Platform Agent by deleting the `logevent.dll` file from `C:\Novell\NDS`.

12.2 Auditing with XDASv2

The XDASv2 specification provides a standardized classification for audit events. It defines a set of generic events at a global distributed system level. XDASv2 provides a common portable audit record format to facilitate the merging and analysis of audit information from multiple components at the distributed system level. The XDASv2 events are encapsulated within a hierarchical notational system that helps to extend the standard or existing event identifier set.

By default, the XDASv2 packages are installed when eDirectory is installed. For more information on auditing with XDASv2, refer to the *Novell XDASv2 Administration Guide* .

NOTE: eDirectory does not support auditing events on servers running AIX.

A Linux, Solaris, and AIX Packages for Novell eDirectory

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

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

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
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.
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
NOVLldif2	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.

B eDirectory Health Checks

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, 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.

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>]`
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 155.

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 153.

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 153)
- Warning (page 153)
- Critical (page 154)

The status of the health checks is logged into a log file. For more information, refer to Section B.5, "Log Files," on page 155.

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 154.

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 non-master 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 .

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 154 and Figure B-2 on page 155.

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://forums.novell.com/netiq/netiq-product-discussion-forums/edirectory/)

- Troubleshooting Documentation (http://www.novell.com/documentation/edir88/edir88tshoot/data/front.html)
- Error Codes (http://www.novell.com/documentation/nwec/)
- Patches (http://support.novell.com/patches.html)
- Cool Solutions (http://www.novell.com/communities/coolsolutions/edirectory)

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.
Windows	nsdcheck.log	The log file will be saved at *install_directory*\novell nds\. **NOTE:** *install_directory* is user specified.

C Configuring OpenSLP for eDirectory

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

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, it is worth reading these documents and internalizing 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, you can 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 Windows, `slpd.exe` runs as a service on the local machine. User agents query the local service agent by sending messages to the loop-back address on a well-known port.

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

1. Checking all statically configured DA addresses (and adding new ones to the SA's known DA cache).

2. Requesting a list of DA's and scopes from DHCP (and adding new ones to the SA's known DA cache).

3. Multicasting a DA discovery request on a well-known port (and adding new ones to the SA's known DA cache).

4. Receiving DA advertising packets that are periodically broadcast by DAs (and adding new ones to the SA's known DA cache).

Since a user agent always queries the local service agent first, this is important, as the local service agent's response will determine whether or not the user agent continues to the next stage of discovery (in this case DHCP-- see steps 3 and 4 in "User Agents" on page 158.).

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.