

Section 3: Provide Directory Services with eDirectory

Course 3015 - Novell Nterprise Linux Services



Novell.

Introduction

Section 3: Provide Directory Services with eDirectory



Novell.



Introduction

Before you can understand how NNLS works and how to configure many of the NNLS components for a lab or production environment, you need to understand the purpose of eDirectory, how eDirectory works, and how to perform some basic eDirectory administrative tasks.

Objectives

Section 3: Provide Directory Services with eDirectory





Implement Directory Services with eDirectory

Objectives:

1. Describe the Purpose of eDirectory
2. Describe How eDirectory Works
3. Perform eDirectory Administration Tasks

Describe the Purpose of eDirectory

Objective 1



Novell.

N Describe the Purpose of eDirectory

To describe the purpose of eDirectory, you need to know the following:

- What a Full-Service Directory Provides
- The Role of eDirectory



What a Full-Service Directory Provides

A full-service Directory is a database that provides features such as discovery, security, storage, and relationship management.



What a Full-Service Directory Provides (continued)

You typically use a full-service Directory in the following ways:

- To organize data
- To more easily provide access to information
- To provide security
- To provide services to customers



The Role of eDirectory

The role of eDirectory is to provide the basic foundation for Directory services and the following benefits:

- Central management of network information, resources, and services
- A standard method of managing, viewing, and accessing network information, resources, and services
- A logical organization of network resources that is independent of the physical characteristics or layout of the network



The Role of eDirectory (continued)

- Dynamic mapping between an object and the physical resource it refers to

Describe How eDirectory Works

Objective 2



Novell.



Describe How eDirectory Works

To describe how eDirectory works, you need to know the following about eDirectory:

- eDirectory Tree Architecture
- How eDirectory Uses Foundation Services
- eDirectory and LDAP



eDirectory Tree Architecture

The eDirectory tree is a hierarchical structure that stores and organizes objects. It includes the tree object and container objects.

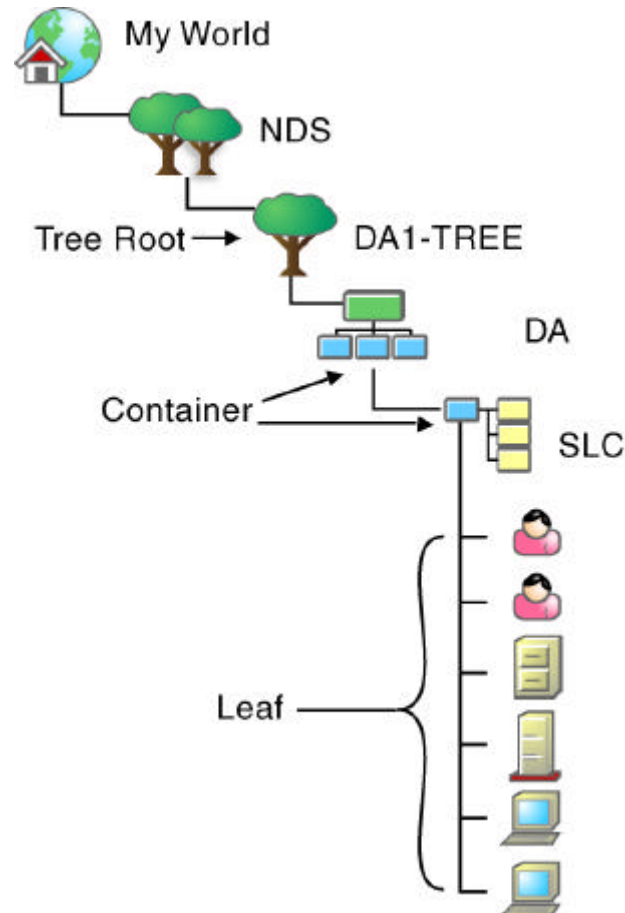
The top of the tree is called the *tree object*. *Container objects*, like folders in a file system, are placed in the tree object or in other containers.

Leaf objects, like files stored in folders, are placed within containers.



eDirectory Tree Architecture (continued)

Digital Airlines Tree Structure

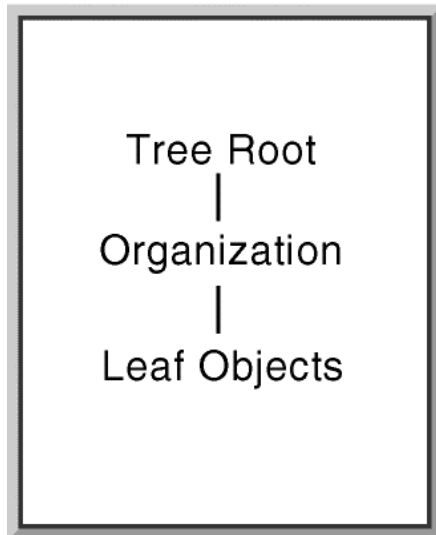




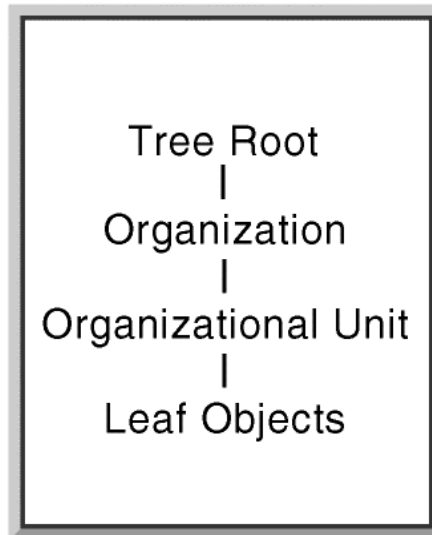
eDirectory Tree Architecture (continued)

eDirectory Tree Design

Structure 1



Structure 2



Structure 3





eDirectory Tree Architecture

(continued)

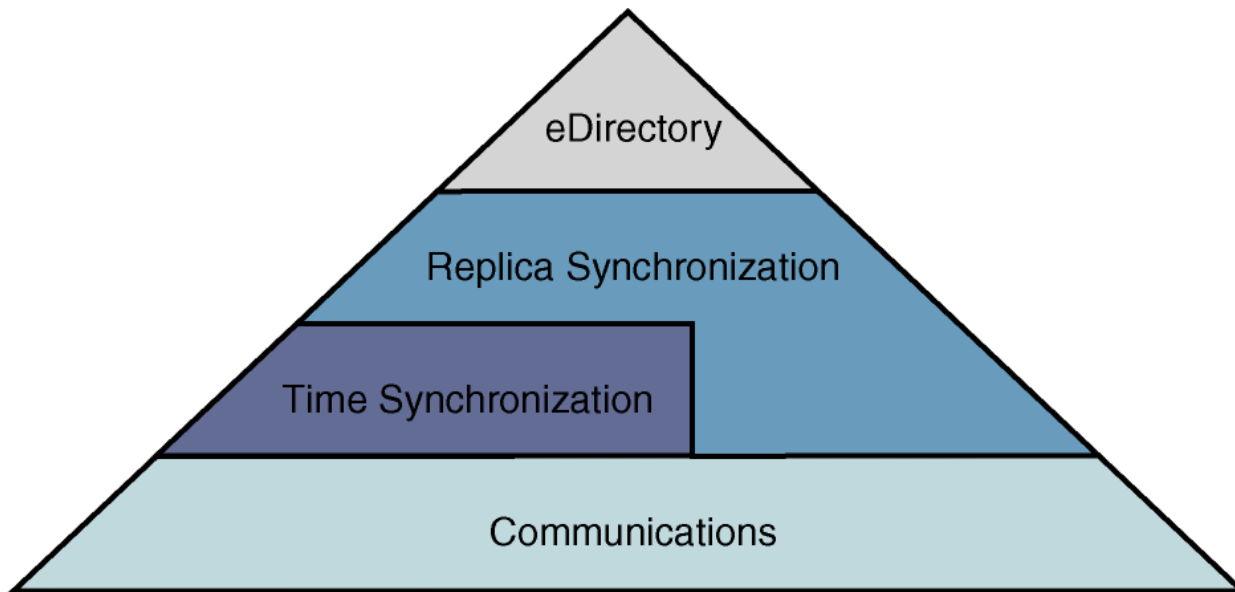
Container restrictions lead to the following hierarchical tree structure requirements:

- The tree object must be at the top.
- Country and organization objects are in the tree object.
- Organization objects are in country objects.
- Organizational unit objects are in organization objects or in other organizational unit objects.



How eDirectory Uses Foundation Services

eDirectory relies on a foundation of error free communications, accurate time synchronization, and efficient replica synchronization.





How eDirectory Uses Foundation Services (continued)

To understand how these foundation services help keeping eDirectory running smoothly, you need to know the following:

- SLP and eDirectory
- Time Synchronization and eDirectory
- Partitions and Replication in eDirectory

You should also understand **Transport Layer Security (TLS)** to effectively utilize eDirectory in a Linux environment.



SLP and eDirectory

On IP networks, the Service Location Protocol (SLP) provides the dynamic discovery of services.

Discovery of network services is essential to eDirectory operation.

In addition, services such as eDirectory can contain a rich set of attributes that clients and applications can use to identify services that meet their needs.



SLP and eDirectory (continued)

Novell provides a basic level of SLP v1 support (SLP v2 on NetWare) with eDirectory for Linux as described by the following:

- **User Agents and Service Agents.** To configure the agents, you edit the `slpuasa.conf` file to specify configuration information and then run the `slpuasa` daemon.



SLP and eDirectory (continued)

- **Starting and Stopping the Daemon Process.** The slpuasa can be started and stopped as follows:

/etc/init.d/slpuasa {start/stop} (SuSE)

/etc/rc.d/init.d/slpuasa {start/stop} (Red Hat)

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

If you don't want to (or cannot) use SLP, you can use a flat file, hosts.nds, to resolve tree names to server referrals.



SLP and eDirectory (continued)

- **eDirectory Interoperability with OpenSLP on Linux.**

Novell SLP v1 is now an optional package. In fact, Novell recommends using a third-party SLP solution, such as OpenSLP (which is SLP v2), if a more robust SLP solution is needed.

If OpenSLP RPMs are already installed on Linux, the eDirectory installation will skip the Novell SLP installation. eDirectory uses the platform specific SLP APIs by default.

N Time Synchronization and eDirectory

To understand time synchronization in eDirectory, you need to know the following:

- The Relationship Between Time Synchronization and eDirectory
- NTP Design Configuration
- Linux and Network Time Protocol



The Relationship Between Time Synchronization and eDirectory

Time synchronization is not a service provided by eDirectory. However, it is a very important part of maintaining the integrity of the eDirectory tree.

Every time a change is made to an object, the change is time stamped to allow the change to be made on all servers holding a copy of that object in the proper sequence.

Without proper time synchronization, it would be possible to have servers in the tree with different times while holding copies of the same eDirectory objects.



NTP Design Configuration

Any computers on your network with Internet access can get time from NTP servers on the Internet.

NTP synchronizes clocks to the Universal Time Coordinated (UTC) standard, the international time standard.

The only way to achieve time synchronization in a mixed environment is by using an open standard protocol for time synchronization such as NTP.



NTP Design Configuration (continued)

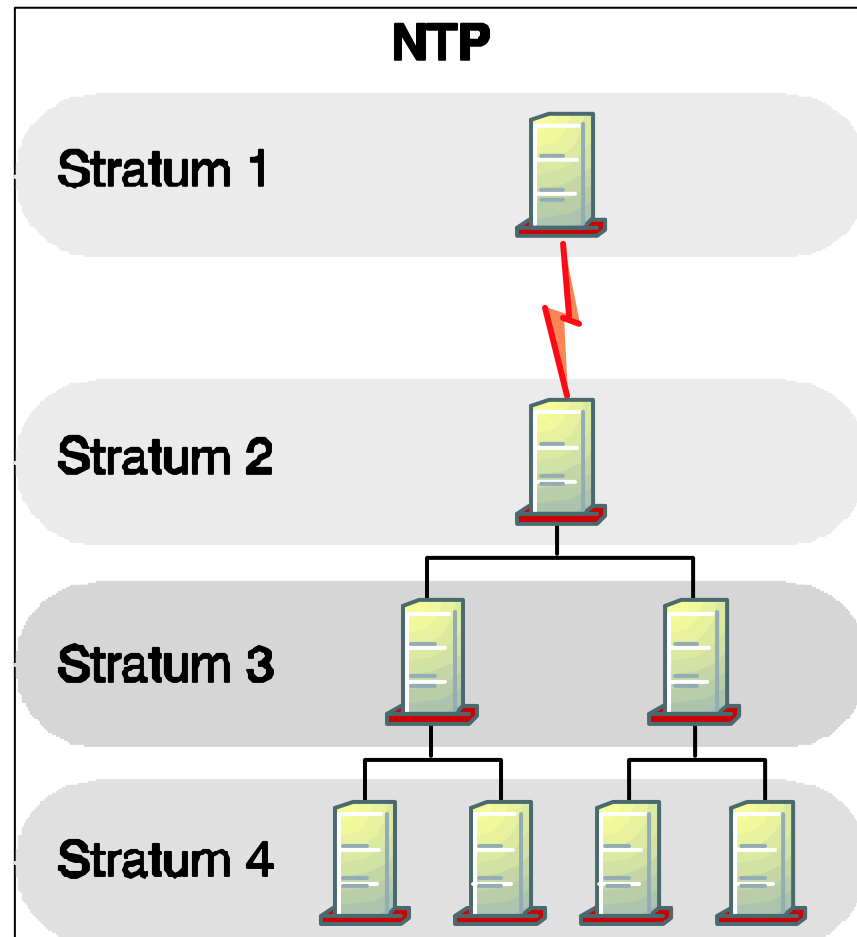
NTP introduces the concept of a stratum. Stratum-x is used as a designation of the location of the servers in NTP tree hierarchy.

Stratum-1 is the first (highest) level in the hierarchy and it denotes servers that adjust their time by means of some external reference time source (such as GPS and radio).

Servers that synchronize their time to Stratum-1 servers are denoted as Stratum-2, and those that use Stratum-2 servers to synchronize their time are denoted as Stratum-3, and so on.



NTP Design Configuration (continued)





Linux and Network Time Protocol

Linux uses a time synchronization service called the NTP Daemon (Red Hat) or the XNTP Daemon (SuSE).

Both daemons work much the same way as W32Time.

You configure the daemon to obtain time from a particular time server using **ntp.conf** and then start the service (**xntpd start** for SuSE or **xntpd start** for Red Hat).



Partitions and Replication in eDirectory

To understand how partitions and replication work in eDirectory, you need to know the following:

- Partitioning
- Partition Size and Number
- Replica Types
- Replica Rings



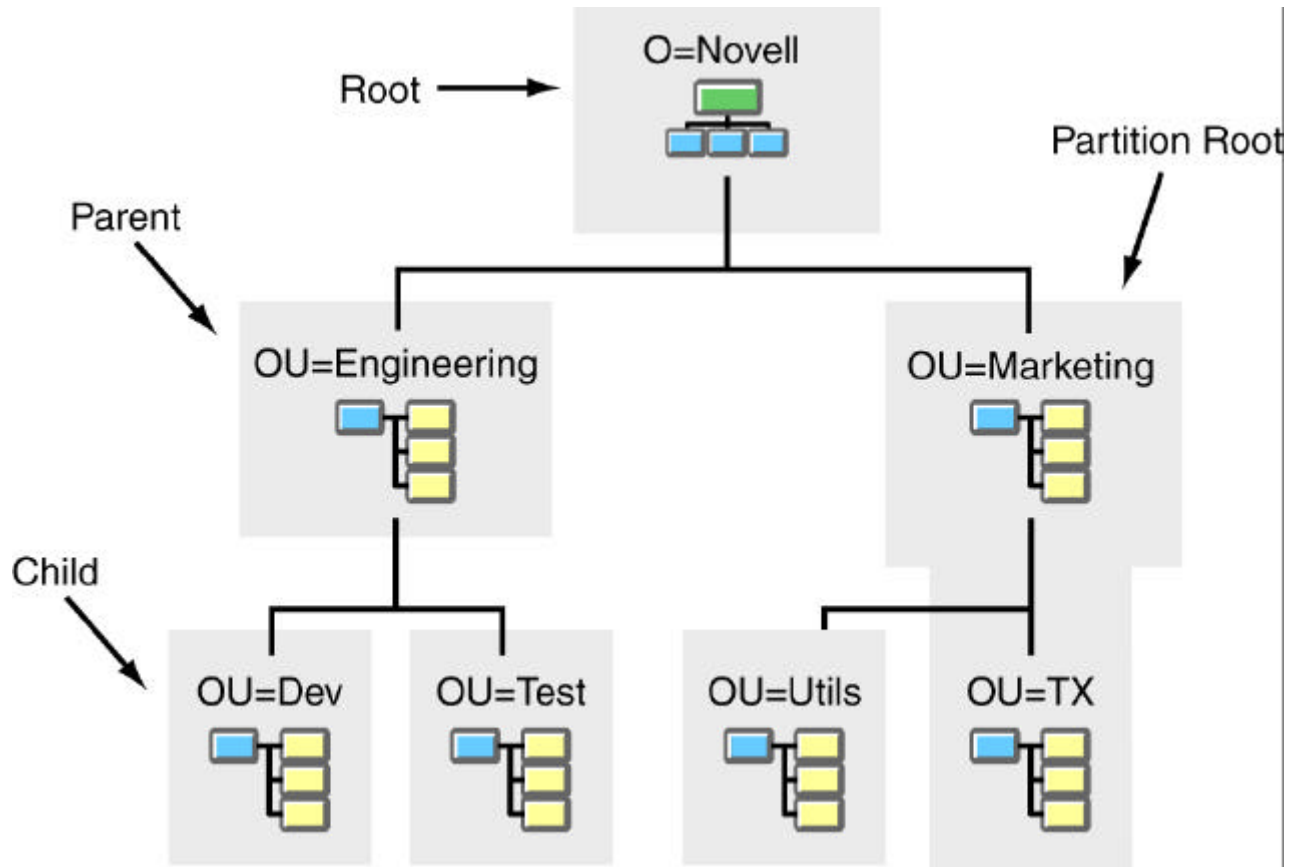
Partitioning

Partitioning is the process of dividing the eDirectory database. You can divide the eDirectory database into logical units (called ***partitions***) that can be distributed among multiple servers.

Partitions only contain eDirectory information. They do not include information on the file system, directories, or files.



Partitioning (continued)





Partitioning (continued)

The 6 partitions in the diagram have the following names: Novell, Engineering, Dev, Test, Marketing, and Utils. The top or root partition of the tree can be called either **Novell** or **Root**.

When a partition is subordinate to another in the eDirectory tree, it is referred to as a ***child*** partition. The partition above it is referred to as the ***parent*** partition.



Partitioning (continued)

Partitioning and replication provide the following benefits:

- **eDirectory fault tolerance.** Redundantly stores eDirectory data on various servers.
- **Efficient access to eDirectory information.** Improves network response time and reduces network traffic by decreasing the size of the database and placing information near the users who need it the most.



Partition Size and Number

With eDirectory 8.7.x, there are no hard and fast rules regarding partition size or the numbers of objects and replicas.

However, there are practical limitations to all of these parameters.



Partition Size and Number (continued)

These limitations depend on various factors such as

- The number of objects
- The rate object information is changing
- The number and type of attributes changing
- The available bandwidth between servers
- The distance between replicas
- The speed of replication
- The number of replicas to synchronize to
- The applications running on the network
- The acceptable latency



Replica Types

A single instance of a partition is called a **replica**. When you create a partition the first replica is called the **master replica**. A partition can have only one master replica.

A server can contain many replicas, but the server can contain only 1 replica of each partition.

Distributing replicas on multiple servers is called **replication**.



Replica Types (continued)

In eDirectory, there are 6 replica types:

- Master
- Read/Write
- Read-Only
- Subordinate Reference
- Filtered Read/Write
- Filtered Read-Only



Replica Types (continued)

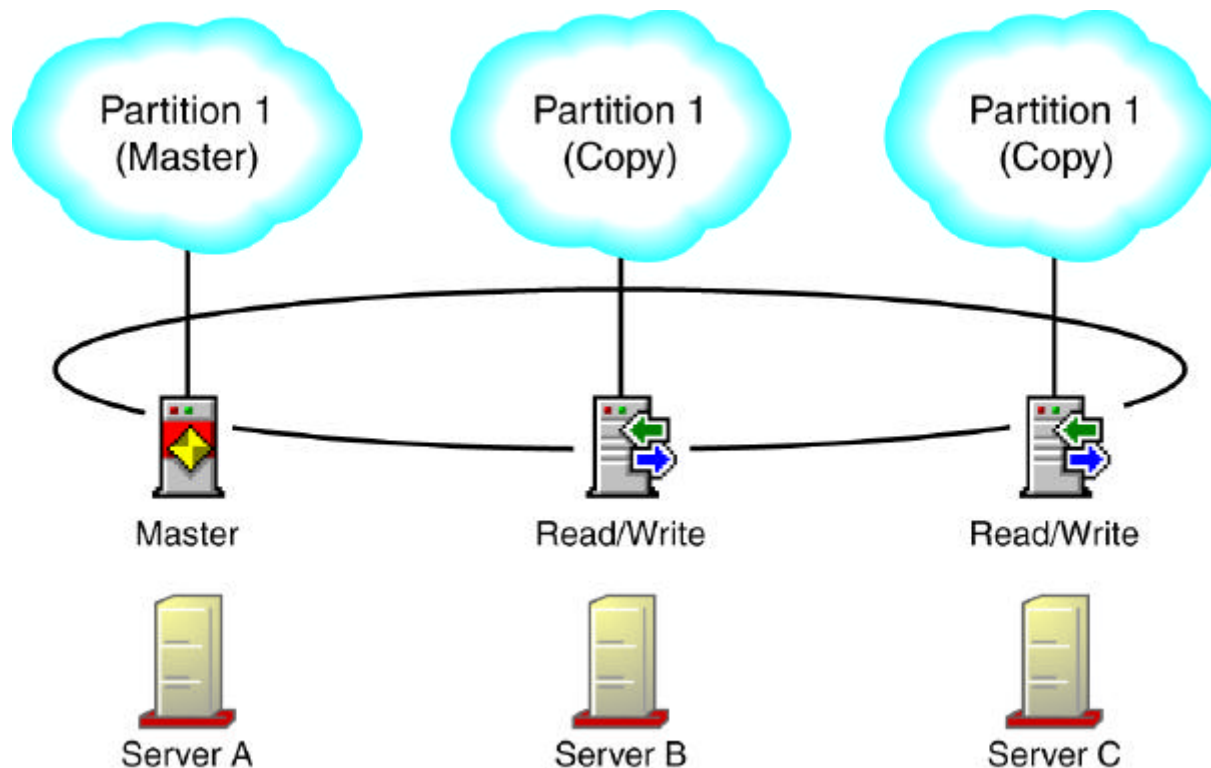
Both the master and read-write replicas can be used to create, modify, and delete objects; however, only the master replica can be used to create and delete subordinate partitions.

Filtered replicas contain a filtered set of objects or object classes along with a filtered set of attributes and values for those objects.



Replica Rings

A **replica ring** (or **replica list**) contains a list of servers that hold a copy or replica of a partition.





Replica Rings (continued)

Changes made to objects within a partition are sent to all other replicas of that partition using the replica ring of the partition root object.

The replica ring includes

- A list of each server containing the replica
- The type of replica
- The replica's current state



Transport Layer Security (TLS)

eDirectory 8.7.x provides support for Transport Layer Security/Secure Sockets Layer (TLS/SSL) services based on the OpenSSL source code.

TLS allows for connections to be encrypted in the session layer. The encrypted port doesn't have to be used to get a TLS connection; there's another way.



Transport Layer Security (TLS) (continued)

Implied TLS Port (636) - LDAP Group Object

Modify Object: LDAP Server - DA1



Connections ▾

Transport Layer Security (TLS / SSL)

Server Certificate:	SSL CertificateDNS 
Client Certificate:	Not Requested ▾
Trusted Root Containers:	<div><div>▾</div><div></div></div>
<input type="checkbox"/> Require TLS for all operations	
<input type="checkbox"/> Enable and require mutual authentication	

Ports

<input checked="" type="checkbox"/> Enable Encrypted Port	Port: <input type="text" value="636"/>
<input checked="" type="checkbox"/> Enable Non-Encrypted Port	Port: <input type="text" value="389"/>

Restrictions

Concurrent Bind Limit: binds ('0' for no limit)



Transport Layer Security (TLS)

(continued)

The LDAP server automatically starts a TLS session when a client connects to the secure port.

A client can also connect to the clear-text port (non-encrypted port) and later use TLS to upgrade the connection to an encrypted connection.



Exercise 3-1: Explore Your eDirectory Tree With iManager

After installing eDirectory with the NNLS install script, you can use iManager to view and explore your eDirectory tree.

In this exercise, you use iManager to explore your eDirectory tree and LDAP object properties.



eDirectory and LDAP

LDAP is an internet communications protocol that lets client applications access directory information.

It is based on the X.500 Directory Access Protocol (DAP) but is less complex than a traditional client, and can be used with any directory service that follows the X.500 standard and provides an LDAP server component.



eDirectory and LDAP (continued)

To understand eDirectory and LDAP, you need to know the following:

- Records and Attributes
- LDAP Naming Contexts and eDirectory Partitions
- Novell LDAP Server Object
- Novell LDAP Group Object
- How LDAP Clients Bind to eDirectory
- LDAP Data Interchange Format (LDIF)



Records and Attributes

In LDAP standards documentation, an *entry* consistently means a *record* in the directory database.

In eDirectory, a *record* is called an *object*.

In most directory documentation (including eDirectory), the term *attribute* refers to the *fields* of a record.

N

LDAP Naming Contexts and NDS Partitions

In LDAP, a ***naming context*** is the same thing as an eDirectory ***partition***.

Just as an eDirectory partition is a branch of the NDS tree with only one parent, an LDAP naming context specifies a branch of a hierarchical tree.



Novell LDAP Server Object

The Novell LDAP Server object stores configuration data for an eDirectory LDAP server, is named **LDAP Server - *server name***, and is created in the same container as the NCP Server object.

The LDAP server module used on each platform is

- **NetWare:** NLDAP.NLM (NLM)
- **Windows:** NLDAP.DLM (NDS Services)
- **Unix/Linux:** /usr/sbin/nldap (daemon)



Novell LDAP Group Object

The Novell LDAP Group object stores configuration data that can be applied to a single LDAP server or a group of LDAP servers such as

- Referral options
- Object class attribute mappings between LDAP clients and eDirectory
- Proxy user authentication
- TLS for simple binds with password setting



Novell LDAP Group Object (continued)

During installation, an LDAP Group object named **LDAP Group - *server name*** is created in the same container as the Server object.

N How LDAP Clients Bind to eDirectory

All LDAP clients bind or connect to eDirectory as one of the following types of users:

- **[Public] User (Anonymous Bind):** a connection that does not contain a username or password.
- **Proxy User (Proxy User Anonymous Bind):** an anonymous connection linked to an eDirectory user object



LDAP Data Interchange Format (LDIF)

An LDIF file consists of a series of records separated by line separators.

An LDIF file specifies a set of directory entries or a set of changes to be applied to directory entries, but not both.

There is a one-to-one correlation between LDAP operations that modify the directory (add, delete, modify, and modrdn), and the types of change records ("add," "delete," "modify," and "modrdn" or "moddn").



LDAP Data Interchange Format (LDIF) (continued)

The following are operations you find in an LDIF file:

- Add
- Delete
- Modrdn
- Modify



Add

The following is an example of an LDIF document with an add operation:

```
version: 1
#add new entry
dn: cn=Fiona Jensen,ou=users,o=acme
changetype: add
objectclass: inetorgperson
sn: Jensen
telephonenumber: +1 216 555 1212
title: Manager
```



Delete

The following is an example of an LDIF document with a delete operation:

```
version: 1
```

```
#delete an entry
```

```
dn: cn=Joy Smith,ou=test,ou=users,o=acme
```

```
changetype: delete
```



Modrdn

The modrdn operation shown in the following LDIF document is an example of renaming an entry:

```
version: 1
```

```
#modify an entry's relative distinguished name
```

```
dn: cn=Fiona Jensen,ou=users,o=acme
```

```
changetype: modrdn
```

```
newrdn: Fiona Jones
```

```
deleteoldrn: 1
```



Modify

The following example modifies an entry to delete the title attribute and adds a postaladdress attribute; if a value already exists, a second value is added and the original value is left alone:

```
dn: cn=Robert Smith,ou=users,o=acme
```

```
changetype: modify
```

```
delete: title
```

```
add: postaladdress
```

```
postaladdress: 123 Anywhere Drive
```



Novell Import/Convert/Export (ICE) Utility

The Novell Import/Convert/Export (ICE) utility lets you do the following:

- Import data from LDIF files to the LDAP directory
- Export data from the LDAP directory to an LDIF file
- Migrate data between LDAP servers
- Import and export comma separated (CSV) files



Novell Import/Convert/Export (ICE) Utility (continued)

ICE Wizard ?

Welcome to the ICE Wizard

The ice wizard will step you through the import, export or migration of data.

Select the task you would like to perform.

☒ Import data from file on disk
☐ Export data to a file on disk
☐ Migrate data between servers

Advanced Settings

☐ Run in verbose mode

Schema rules:

Placement rules:



Novell Import/Convert/Export (ICE) Utility (continued)

You can start ICE from a command prompt by using the following syntax:

ice general_options -S <source handler> <source handler options> -D <destination handler> <destination handler options>

The following is an example of using ICE from the command line:

ice -S LDIF -f \root\ldif\add.ldif -c -v



Exercise 3-2: Import an LDIF File

To finish configuring your eDirectory tree, you need to add employees and groups to populate your container.

In this exercise, you use an LDIF file and the ICE wizard to add employees and groups.

Perform eDirectory Administration Tasks

Objective 3



Novell.



Perform eDirectory Administration Tasks

To perform administration tasks for eDirectory on Linux, you need to know the following:

- Command Line Utilities
- How to Start and Stop eDirectory on Linux
- Where eDirectory Files Are Located
- Novell iManager
- Novell iMonitor
- How to Perform a Health Check in iMonitor



Command Line Utilities

The following command line utilities are available to help you with eDirectory management, monitoring, and troubleshooting tasks:

- `ldapconfig`
- `ndsbackup`
- `ndsconfig`
- `ndsmonitor`
- `ndslogin`
- `ndsmerge`
- `ndsrepair`



Command Line Utilities (continued)

- `ndsstat`
- `ndstrace`
- `nmasinst`

You can use the **man** command (such as **man `ndsconfig`**) to view online manual pages for each command.

You can remove eDirectory from the NNLS server outside of the NNLS install using the **`/usr/sbin/nds-uninstall`** command at a shell prompt.



ndsconfig

The following is the command line syntax for ndsconfig:

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

The following is an ndsconfig example that removes the eDirectory server object and services from a tree:

ndsconfig rm -a cn=admin.o=company



ndsrepair

The following is the command line syntax for
ndsrepair:

ndsrepair *command_option*

The following is an ndsrepair example that performs
an unattended full repair:

ndsrepair -U



ndstrace

The following is the command line syntax for ndstrace:

ndstrace command_option

The following is an ndstrace example that schedules the backlink process to begin:

set ndstrace = *B

N How to Stop and Start eDirectory on Linux

Do the following:

1. From a shell prompt change to the init.d directory by entering **cd /etc/rc.d/init.d** (Red Hat) or **cd /etc/init.d** (SuSE); then enter **./ndsd stop**.
2. Start the daemon by entering **./ndsd start** (or enter **./ndsd restart** to stop and start with one command).

```
[student@DA3 student]$ su -  
Password:  
[root@DA3 root]# cd /etc/rc.d/init.d  
[root@DA3 init.d]# ./ndsd stop  
Stopping Novell eDirectory server...  
done  
[root@DA3 init.d]# ./ndsd start  
Starting Novell eDirectory server...  
done  
[root@DA3 init.d]# █
```



Where eDirectory Files Are Located

During a default installation, the following eDirectory directories are created:

- **/var/novell/nici**
Stores the Novell International Cryptographic Infrastructure (NICI) files
- **/var/nds**
Stores a variety of eDirectory files, including log files, eDirectory reports, DIB files, and certificate server files
- **/etc/nds** (Red Hat) or **/etc** (SuSE)
Stores the nds.conf (eDirectory configuration) file, along with other eDirectory configuration files for iMonitor



Novell iManager

Novell iManager provides a Web-based management tool that uses roles to delegate eDirectory administration, management, and services.

In this (and other sections), you are introduced to performing a variety of management tasks with iManager that are critical to maintaining eDirectory.



Novell iManager

Novell iManager

Unrestricted Access

User: admin.anc.DA2-TREE.

Roles and Tasks

- DirXML Management**
 - [Activation Installation](#)
 - [Activation Request](#)
 - [Create Driver](#)
 - [Create Rule](#)
 - [Create StyleSheet](#)
 - [Dataflow](#)
 - [Dataflow \(Table view\)](#)
 - [Export Driver](#)
 - [Import Drivers](#)
 - [Load Sample Objects](#)
 - [NDS2NDS Driver Certificates](#)
 - [Overview](#)
- DirXML Planning**
 - [Design Dataflow](#)
- Dynamic Groups**
 - [Create Dynamic Group](#)
 - [Create Extended Object](#)
 - [Delete Dynamic Group](#)
 - [Modify Dynamic Group](#)
- eDirectory Administration**
 - [Copy Object](#)
 - [Create Object](#)
 - [Delete Object](#)
 - [Modify Object](#)
 - [Move Object](#)
 - [Rename Object](#)

Novell iManager
Version 2.0.2

www.novell.com

You are currently logged in as user **admin.anc** in the Novell eDirectory **DA2-TREE** tree with Unrestricted access.

Unrestricted Access
This mode displays all of the roles and tasks installed. Although all roles and tasks are visible, the authenticated user will still need the necessary rights to use the tasks.

Assigned Access
This mode displays only the roles and tasks assigned to the authenticated user. This mode takes full advantage of the Role Based Services (RBS) technology.

Collection Owner Access
This mode displays the roles and tasks in any and all collections for which the authenticated user is an owner. It allows user Admin to use all of the roles and tasks in the collections, even if specific rights have not been assigned. Role Based Services (RBS) must be installed in order to use this mode.

Tree Down Access
This troubleshooting mode is used to correct eDirectory availability problems on your network. Tomcat must be stopped and restarted to access this mode. See the iManager 2.0 Administration Guide for additional information (<http://www.novell.com/documentation/ig/imanager20>).



Novell iMonitor











While Novell iManager gives you the tools for performing management and configuration tasks, **Novell iMonitor** gives you monitoring and diagnostic capability on all servers in your eDirectory tree.

iMonitor shows the view of eDirectory from the perspective of each server. You can look at eDirectory in depth on a partition, replica, or server basis.




Novell iMonitor (continued)

NDS™ iMonitorNovember 29, 2003 4:47:01 am

Agent Summary

Novell.


 **.CN=DA1. OU=SLC. O=DigitalAir. T=DIGITALAIR-TREE.**

Identity: .CN=admin. OU=SLC. O=DigitalAir. DIGITALAIR-TREE.

Links:

- [Agent Synchronization](#)
- [Known Servers](#)
- [Schema](#)
- [Agent Configuration](#)
- [Trace Configuration](#)
- [Agent Health](#)
- [Agent Process Status](#)
- [Agent Activity](#)
- [Connections](#)
- [Error Index](#)

Partition Synchronization Status

Partition	Errors	Last Successful Sync.	Maximum Ring Delta	Replica's Perishable Data Delta	
 .DIGITALAIR-TREE.	2	9614:32:42	9614:32:23	9614:32:24	Replica Synchronization, Agent Health, Change Cache, Continuity

Servers Known to Database Totals

Type	Count	Up	Down	Unknown
Known Servers	4	1	3	0
In Replica Ring	3	1	2	0

Agent Process Status Totals



Novell iMonitor (continued)

iMonitor provides a Web-based alternative or replacement for many of Novell's traditional server-based eDirectory tools such as DSBROWSE, DSDIAG, and ndstrace.



Novell iMonitor (continued)

NDS™ iMonitor November 29, 2003 4:54:04 am

Trace

[.CN=DA1. OU=SLC. O=DigitalAir. T=DIGITALAIR-TREE.](#)

Identity: [.CN=admin. OU=SLC. O=DigitalAir. DIGITALAIR-TREE.](#)

Refresh Settings:

Refresh Interval

Previous Buffer

Go to:

Trace:

[Trace Configuration](#)
[Event Configuration](#)
[Trace History](#)

```
04: 54: 03 D4896580 Agent: Calling DSAResolveName conn:5 for client . \[Public\].  
04: 54: 03 D4896580 Agent: Calling DSAReadObjectInfo conn:2 for client .DA1.SLC.DigitalAir.DIGITALAIR-TREE.  
04: 54: 03 D4896580 Agent: Calling DSARead conn:2 for client .DA1.SLC.DigitalAir.DIGITALAIR-TREE.  
04: 54: 03 D4896580 Agent: Calling DSAResolveName conn:2 for client .DA1.SLC.DigitalAir.DIGITALAIR-TREE.  
04: 54: 03 D4896580 Agent: Calling DSAReadObjectInfo conn:2 for client .DA1.SLC.DigitalAir.DIGITALAIR-TREE.  
04: 54: 03 D4896580 Agent: Calling DSAListPartitions conn:2 for client .DA1.SLC.DigitalAir.DIGITALAIR-TREE.  
04: 54: 03 D4896580 Agent: Calling DSACompare conn:2 for client .DA1.SLC.DigitalAir.DIGITALAIR-TREE.  
04: 54: 03 D7CCF240 Agent: Calling DSAGetServerNetAddress conn:26 for client .admin.SLC.DigitalAir.DIGITALAIR-TREE.  
04: 54: 03 D7CCF240 Agent: Calling DSAGetServerNetAddress conn:26 for client .admin.SLC.DigitalAir.DIGITALAIR-TREE.  
04: 54: 03 D7CCF240 Agent: Calling DS Ping conn:26 for client .admin.SLC.DigitalAir.DIGITALAIR-TREE.  
04: 54: 03 D7CCF240 Agent: Calling DS Ping conn:26 for client .admin.SLC.DigitalAir.DIGITALAIR-TREE.  
04: 54: 03 D7CCF240 Agent: Calling DSAGetServerNetAddress conn:28 for client . \[Public\].  
04: 54: 03 D7CCF240 Agent: Calling DSAGetServerNetAddress conn:28 for client . \[Public\].  
04: 54: 03 D7CB71C0 Agent: Calling DSAGetServerNetAddress conn:26 for client .admin.SLC.DigitalAir.DIGITALAIR-TREE.  
04: 54: 03 D7CB71C0 Agent: Calling DSAGetServerNetAddress conn:26 for client .admin.SLC.DigitalAir.DIGITALAIR-TREE.
```



Novell iMonitor (continued)

iMonitor also allows for many of the diagnostic features available in ndsrepair.

NDS™ iMonitor November 29, 2003 7:03:02 am

Repair

.CN=DA1. OU=SLC. O=DigitalAir. T=DIGITALAIR-TREE.

Identity: .CN=admin. OU=SLC. O=DigitalAir. DIGITALAIR-TREE.

Downloads:
[dsrepair.htm](#)
[Archived DIB - 00000000.\\$DU](#)

Delete Old DIB sets:

	Repair	Archive	Date	Size
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Saturday, May 24, 2003	6895KB	

Links:
[Agent Summary](#)
[Agent Synchronization](#)
[Known Servers](#)
[Schema](#)
[Agent Configuration](#)
[Trace Configuration](#)

NDS Repair Advanced Switches

Check the desired boxes and select the "Start Repair" button to start NDS Repair.

<input checked="" type="checkbox"/> Repair Local DIB	<input type="checkbox"/> Create DIB Archive
<input type="checkbox"/> Run in Unattended Mode	<input type="checkbox"/> Disable Reference Checking
<input type="checkbox"/> Report Move Obits	<input type="checkbox"/> Repair Volume Objects
<input type="checkbox"/> Repair Network Addresses	<input type="checkbox"/> Repair Volume Objects & Do Trustee Check

Support Options:

Start Repair

Schedule Repair

This section of the form allows the repair to be configured to run on either a periodic basis, or at a later time.

Scheduling Options

Frequency: ☐ One Time ☐ Daily ☐ Weekly ☒ Monthly

Start Time: 10:00 10:00



Novell iMonitor (continued)

To understand how to use iMonitor for eDirectory maintenance tasks, you need to know the following:

- iMonitor Modes of Operation
- How to Access iMonitor



iMonitor Modes of Operation

iMonitor can be used in 2 different modes of operation:

- **Direct mode**

Your web browser is pointed directly at an address or DNS name on a machine running the iMonitor service and reads information only on that machine's local eDirectory DIB.

- **Proxy mode**

Your web browser is pointed at an iMonitor running on 1 machine but is gathering information from another machine.



How to Access iMonitor

You can securely access iMonitor (for example, as admin) by entering the following URL in a web browser:

https://IP_or_dns:8010/nds

You can also use **http://IP_or_dns:8008/nds** for non-secure access, but you will be limited to the features you can use.



How to Access iMonitor (continued)

The first page you see is the agent summary. The information immediately shows what is happening on your server.

You can use this page to view the health of your eDirectory servers, including synchronization information, agent process status, and the total number of servers known to your database.



How to Access iMonitor (continued)

NDS™ iMonitor November 29, 2003 4:47:01 am

Agent Summary

 [.CN=DA1. OU=SLC. O=DigitalAir. T=DIGITALAIR-TREE.](#)

Identity: [.CN=admin. OU=SLC. O=DigitalAir. DIGITALAIR-TREE.](#)

Links:

- [Agent Synchronization](#)
- [Known Servers](#)
- [Schema](#)
- [Agent Configuration](#)
- [Trace Configuration](#)
- [Agent Health](#)
- [Agent Process Status](#)
- [Agent Activity](#)
- [Connections](#)
- [Error Index](#)

Partition Synchronization Status

Partition	Errors	Last Successful Sync.	Maximum Ring Delta	Replica's Perishable Data Delta	
 .DIGITALAIR-TREE.	2	9614:32:42	9614:32:23	9614:32:24	Replica Synchronization, Agent Health, Change Cache, Continuity

Servers Known to Database Totals

Type	Count	Up	Down	Unknown
Known Servers	4	1	3	0
In Replica Ring	3	1	2	0

Agent Process Status Totals



How to Perform a Health Check in iMonitor

To understand how to perform a health check in iMonitor, you need to know the following:

- Why Health Checks Are Necessary
- When and How Often Health Checks Are Needed
- Health Check Elements
- iMonitor Health Check Procedure
- How to Run an Agent Health Report



Why Health Checks Are Necessary

Performing a regular eDirectory health check helps keep your eDirectory tree stable and efficient.

Because the eDirectory tree is the backbone of your company's network, you risk downtime and serious problems if you postpone performing regular eDirectory health checks.

N

When and How Often Health Checks Are Needed

In general, if your network doesn't change often (servers and partitions are added only every couple of months and only simple changes are made frequently), perform health checks once a month.

If your network is more dynamic (partitions or servers are added weekly or your organization is reorganizing), perform health checks weekly.



Health Check Elements

A basic health check includes the following health check report elements:

- eDirectory version
- Time synchronization
- Partition continuity



Health Check Elements (continued)

In this course we focus on a basic health check.

However, an extended health check includes background processes such as the following:

- Schema synchronization status
- Obituaries
- External references
- Limber status



iMonitor Health Check Procedure

Do the following in iMonitor:

1. At the left under Links, select **Agent Configuration**.
2. At the left under Links, select **Agent Synchronization**; then verify partition synchronization information.
3. Select **Continuity**.
4. At the left under Links, select **Agent Process Status**.



How to Run an Agent Health Report

iMonitor has some default reports that you can run. These reports provide quicker access to problems with eDirectory:

1. From iMonitor at the top of the page, select the **Report** icon.
2. Select **Report Config**.
3. From the list of runnable reports, select the option to run the **Agent Health** report.



How to Run an Agent Health Report (continued)

NDS™ iMonitor November 12, 2002 3:05:47 pm

Agent Health

[? ? ? ? ? ? ? ? ? ?](#)

Novell.

[.CN=DA1. OU=SLC. O=DigitalAir. T=DIGITALAIR-TREE.](#)

Identity: [.CN=admin. OU=SLC. O=DigitalAir. DIGITALAIR-TREE.](#)

Reports:

- [Reports](#)
- [Report Config](#)

Links:

- [Agent Summary](#)
- [Agent Synchronization](#)
- [Known Servers](#)
- [Schema](#)
- [Agent Configuration](#)
- [Trace Configuration](#)
- [Agent Health](#)
- [Agent Process Status](#)
- [Agent Activity](#)
- [Connections](#)

Report

[Health](#)

Health Check

Description	Results
Agent	
Partition/Replication	



How to Run an Agent Health Report (continued)

When problems exist, you can select the **Agent** link to see the reason for the marginal status.

The screenshot shows the NDS iMonitor Agent Health window. The title bar reads "NDS™ iMonitor" and "November 12, 2002 3:09:37 pm". The "Agent Health" tab is selected. The main area displays a green status icon and the text ".CN=DA1. OU=SLC. O=DigitalAir. T=DIGITALAIR-TREE." Below this, the "Identity" is listed as ".CN=admin. OU=SLC. O=DigitalAir. DIGITALAIR-TREE." On the left, a "Links:" section contains several underlined links: Agent Summary, Agent Synchronization, Known Servers, Schema, Agent Configuration, Trace Configuration, Agent Process Status, Agent Activity, Connections, and Error Index. The main panel lists various health checks with their status (green circle with a question mark) and values. The "Agent Process - Reference Check" and "Agent Process - Schema" checks show red error codes -626 and -625 respectively.

Health Check	Status	Value
Time delta tolerance	Green	
Agent Software Version	Green	10410.98
DS Loaded	Green	
DS Open	Green	
Database Lock Held	Green	0
Database Lock Queue	Green	0
Database Lock Queue Time	Green	0
Outstanding Requests	Green	1
Agent Process - Obituary	Green	
Agent Process - Reference Check	Red	-626
Agent Process - Limber	Green	
Agent Process - Schema	Red	-625



How to Run an Agent Health Report (continued)

To investigate problems with replicas, select the **Ring** link.

The screenshot shows the NDS iMonitor Agent Health window. The title bar reads "NDS™ iMonitor" and the date/time is "November 12, 2002 3:15:12 pm". The "Agent Health" tab is selected. The main area displays the identity ".CN=DA1. OU=SLC. O=DigitalAir. T=DIGITALAIR-TREE." and the user identity ".CN=admin. OU=SLC. O=DigitalAir. DIGITALAIR-TREE.".

On the left, under "Links:", there is a list of links: Agent Summary, Agent Synchronization, Known Servers, Schema, Agent Configuration, Trace Configuration, Agent Process Status, Agent Activity, Connections, and Error Index.

The main content area shows the "Health" tab selected, with "Partition/Replication" chosen. A "Health Check" section displays a table with the following data:

Description	Results
? Partition/Replication	---

Below this, a "Health Check: Partition" section displays a table with the following data:

Partition	Description	Results
.T=DIGITALAIR-TREE.	Replica Synchronization ? Ring	---



Exercise 3-3: Verify Your Server and eDirectory Status

Because your tree only includes 1 server, 1 partition, and 1 replica, many of the tasks you perform in this exercise might seem unnecessary.

However, when working with eDirectory in a production environment, these tasks are vital for monitoring and troubleshooting the health of eDirectory and your network.



Exercise 3-3: Verify Your Server and eDirectory Status (continued)

In this exercise, you do the following:

- Part I: Check Your Server Status
- Part II: View Replicas and Partitions
- Part III: Check Schema Synchronization
- Part IV: Complete a Manual Health Check
- Part V: Run the Agent Health Report

Novell®