Section 4: Manage User Identities With NNLS

Course 3015 – Novell Nterprise Linux Services

Novell

Manage User Identities With NNLS

Objectives:

1. Manage User Objects with iManager
2. View User Information With eGuide
3. Access a Linux Server With Linux User Management (LUM)

Manage User Objects with iManager

Objective 1

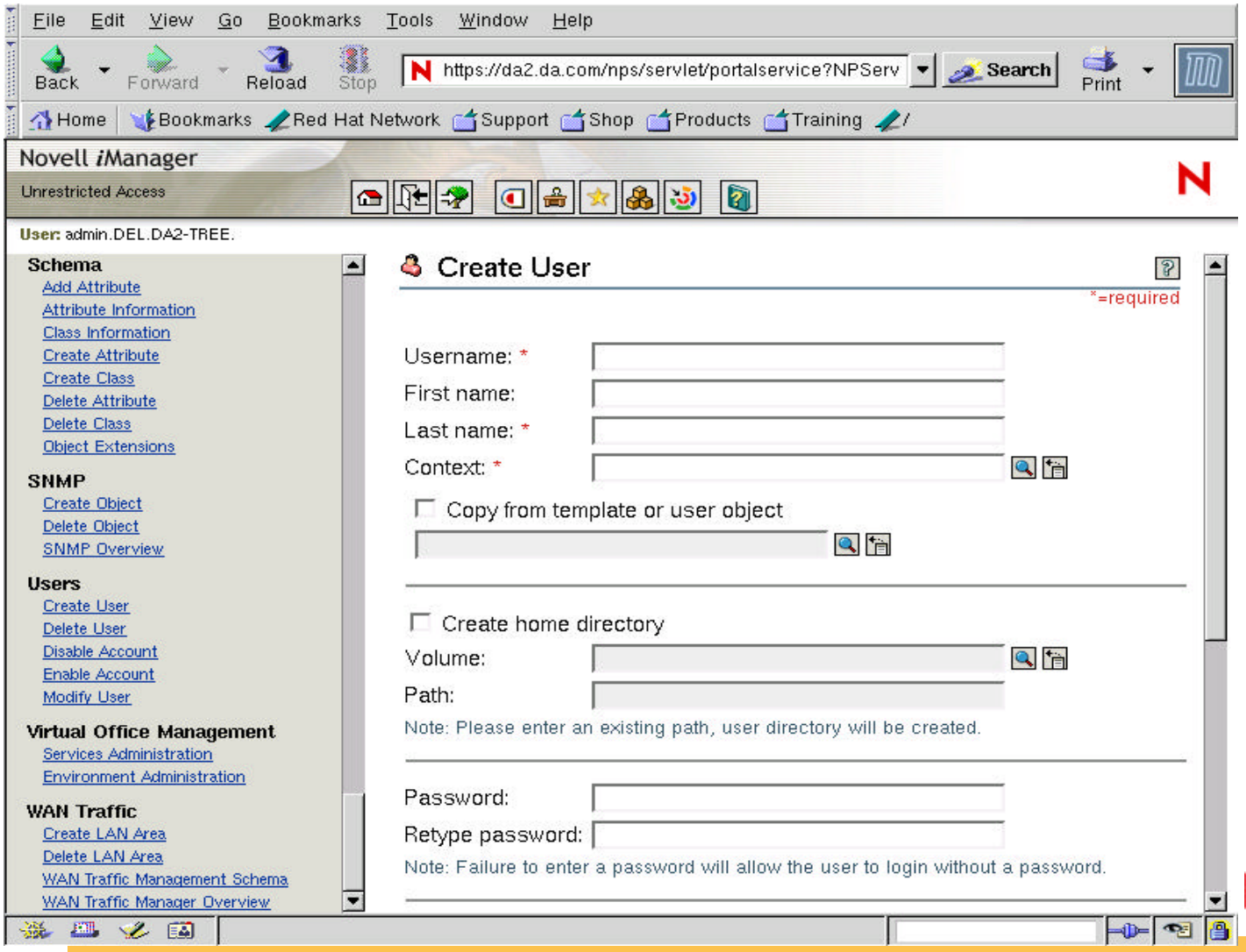
Novell

Manage User Objects with iManager

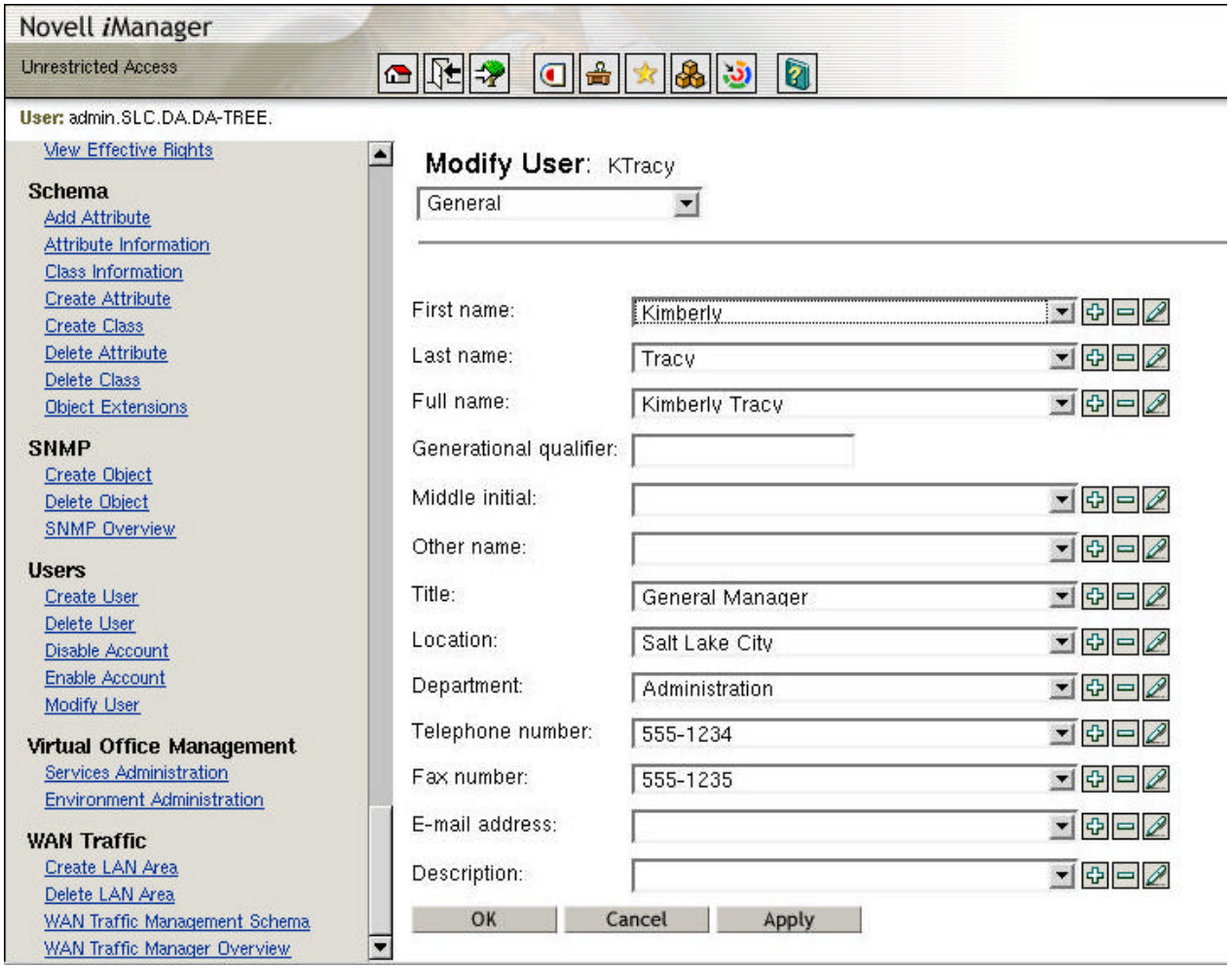
To manage user objects on your Linux server with iManager, you need to know the following:

- How to Create User Objects
- How to Modify User Objects
- How to Move Objects
- How to Delete User Objects
- How to Extend the eDirectory Schema with an Auxiliary Class

How to Create User Objects

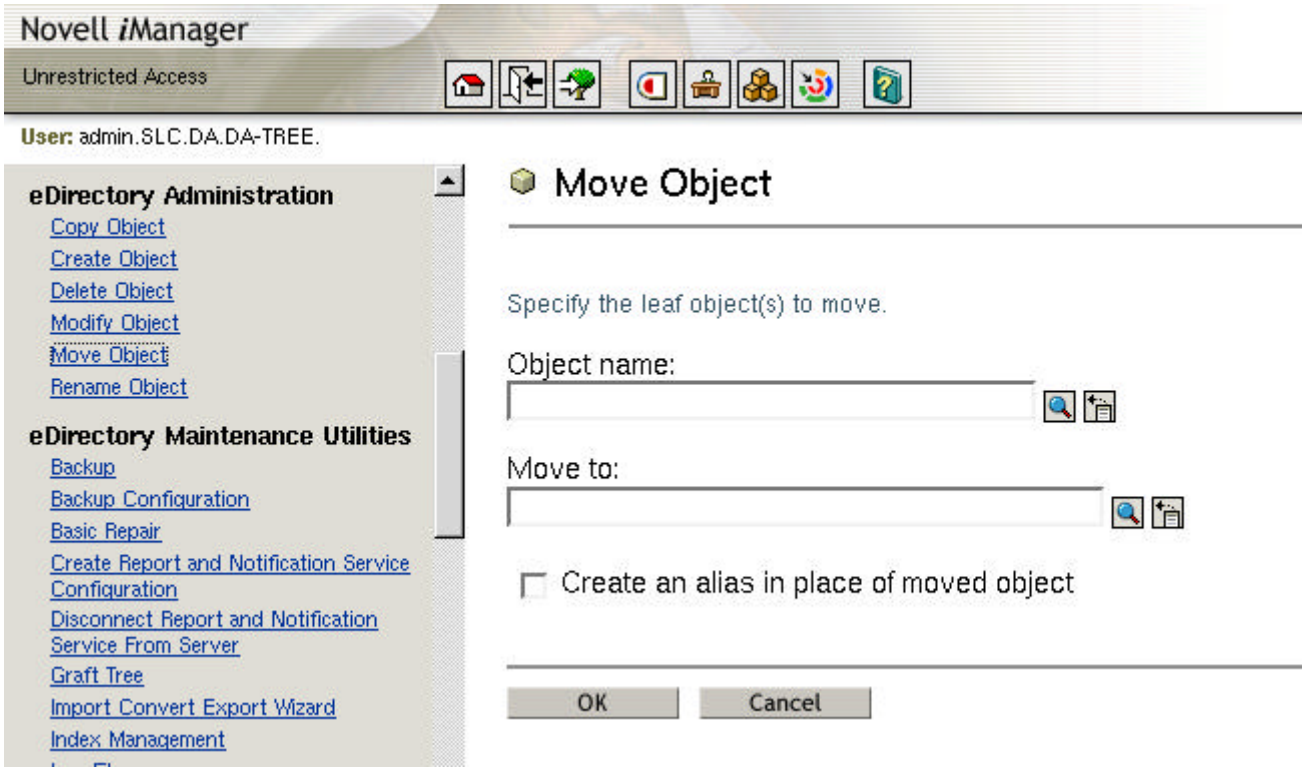


How to Modify User Objects

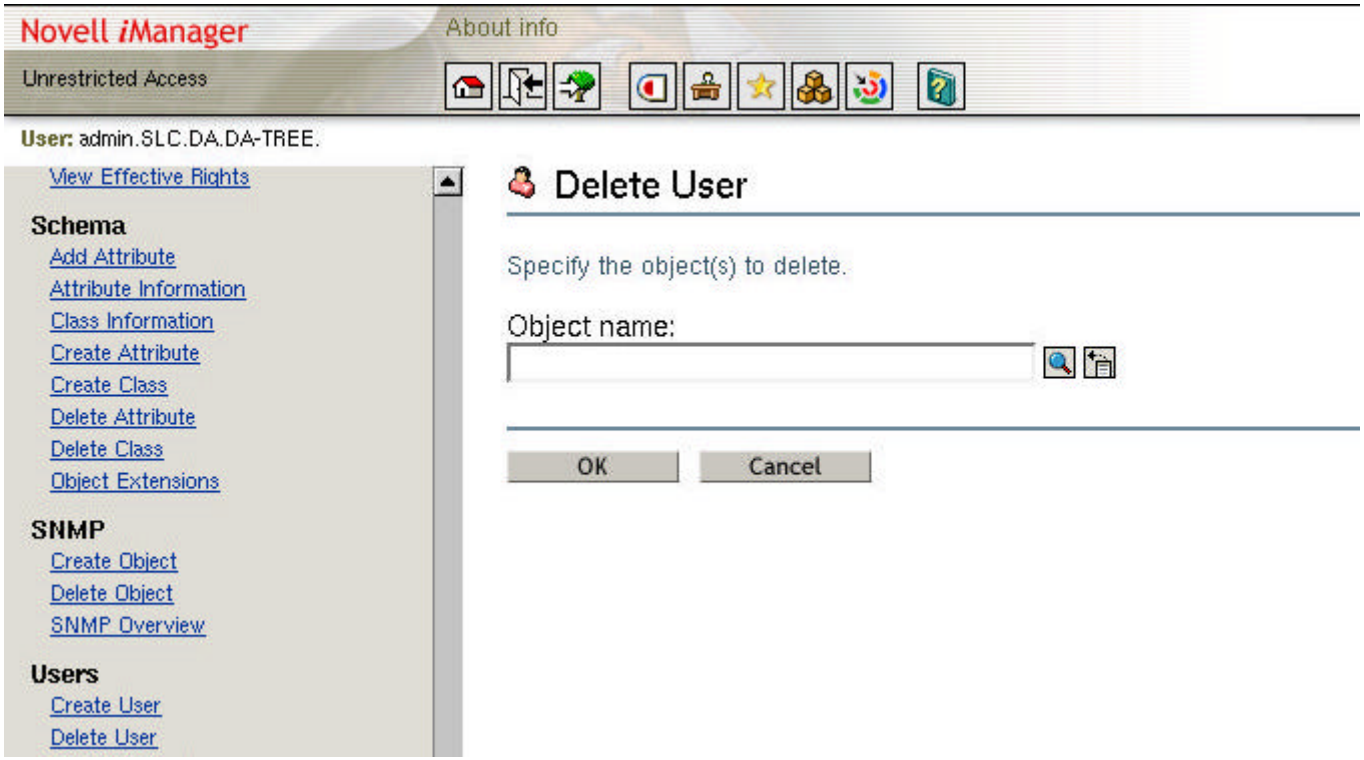


Novell

How to Move User Objects



How to Delete User Objects



Exercise 4-1: Manage User Objects

As a network administrator for your Digital Airlines office, you are responsible for creating and modifying employee user accounts in eDirectory.

The following employees were hired and need user accounts in eDirectory:

- Bret Grow
- Kate Bailey
- Janet Nelson
- Jack Goldman

Exercise 4-1: Manage User Objects (continued)

In this exercise, you do the following:

- Part I: Create a Group Object
- Part II: Create User Objects
- Part III: Modify a User Object
- Part IV: Create a User From Another User Object

How to Extend the eDirectory Schema with an Auxiliary Class

To extend the eDirectory schema with an auxiliary class, you need to know the following:

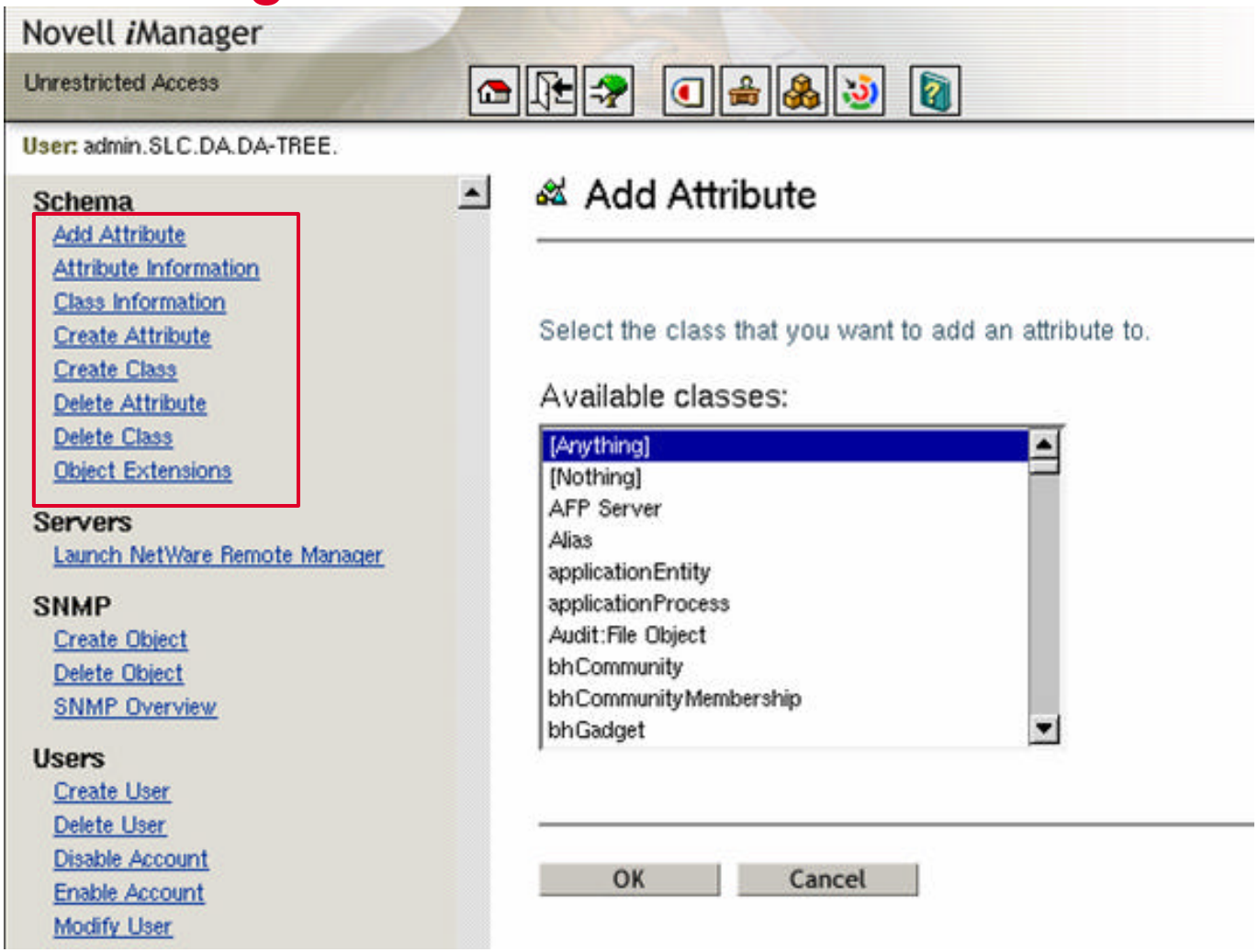
- What the Schema Is
- Schema Management Options in iManager
- How to View the Schema
- How to Create an Auxiliary Class

What the Schema Is

The eDirectory schema defines the classes of objects that the tree can contain, such as users, groups, and printers.

The schema also specifies the attributes (properties) that comprise each object type, including those that are required when creating the object and those that are optional.

Schema Management Options in iManager



How to View the Schema

In iManager, do the following:

1. At the left under Schema Management, select **Attribute Information** or **Class Information**.
2. From the drop-down list, select an attribute or class; then select **View**.

How to Create an Auxiliary Class

An auxiliary class is a set of properties (attributes) that is added to particular eDirectory object instances rather than to an entire class of objects.

To create an Auxiliary class, do the following:

1. Use iManager to access the **Create Class** option.
2. Follow the instructions in the wizard.
3. Assign the aux class to an object and enter data.
4. Verify that the class and the data have been added.

Exercise 4-2: Create an Auxiliary Class

Digital Airlines has started to issue two-way radios to its Flight Operations employees.

You choose to extend the eDirectory schema by creating an auxiliary class (named **Radios**) that lets you keep track of the serial numbers of the 2-way radios issued to the employees.

View User Information with eGuide

Objective 2

Novell

View User Information With eGuide

To view user information with eGuide, you need to know the following:

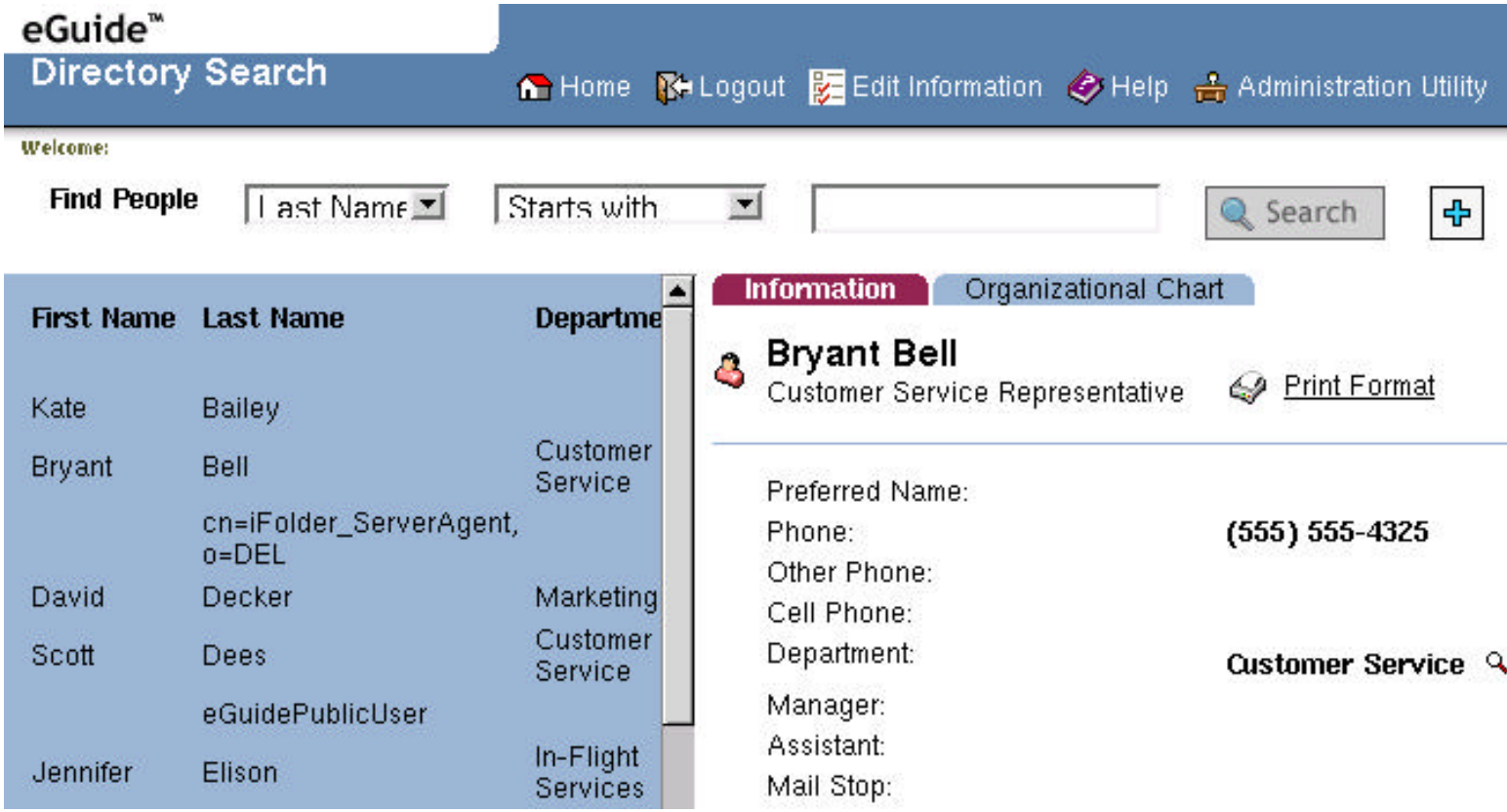
- The Features of eGuide
- How to Access the eGuide Client
- How to Configure eGuide for LDAP

The Features of eGuide

eGuide is a Web application that lets you search for and view information about people, places, and things stored in eDirectory and other LDAP data sources at the same time.

eGuide is independent of platform or a particular application. It can be accessed by any user with rights to your Web server via a standard Web browser.

The Features of eGuide (continued)



The Features of eGuide (continued)

The major features of eGuide are

- Standards-based display and administration with HTML, XML, and XSL make configuration and use simple, convenient, and highly customizable.
- Advanced Search capabilities allow searches on any attribute.
- Data handler controls allow you to display the information the way you want.
- Organizational Charts are automatically generated based on eDirectory attributes.

The Features of eGuide (continued)

- Anonymous and User Authentication modes are supported, including contextless login, cookies, and support for eDirectory password restrictions.
- Authenticated Searching utilizes access control lists in eDirectory to determine if a user can access particular attribute information.
- eGuide works seamlessly with Novell iChain® and Novell Portal Services, and is an excellent add-on to DirXML® synchronization projects.
- eGuide is compatible with eDirectory or any other LDAP-enabled directory service.

How to Access the eGuide Client

You can access eGuide by doing one of the following:

- Select the **Launch Novell eGuide Client** icon from the Administration utility.
- From your Web browser, enter **http://*web_server*/eGuide**.

How to Configure eGuide for LDAP

The process of configuring eGuide involves identifying the LDAP data source and specifying how eGuide will access that data source.

To understand how this connection is configured, you need to know the following:

- Anonymous binds
- eGuide proxy user
- Secure connections (TLS)

Exercise 4-3: Set Up and Access eGuide

In this exercise, you do the following:

- Part I: Access eGuide to View Digital Airlines Employees
- Part II: Configure eGuide for Users

Access a Linux Server With Linux User Management (LUM)

Objective 2

Novell

Access a Linux Server With Linux User Management (LUM)

To use LUM for managing user accounts, you need to know the following:

- What LUM Is
- LUM Components
- eDirectory LUM Objects
- User Accounts
- Group Accounts
- How to Configure LUM
- How to Perform Basic LUM Tasks

What LUM Is

Normally Linux users authenticate against information stored in a **passwd** file on the Linux server. This authentication gives them specific rights to Linux services.

LUM lets users authenticate against an eDirectory user object for access to Linux services without an entry in the passwrd file.

What LUM Is (continued)

With LUM you can modify or create eDirectory users and groups that can then access the NNLS server. This is required if either of the following scenarios apply to your NNLS implementation:

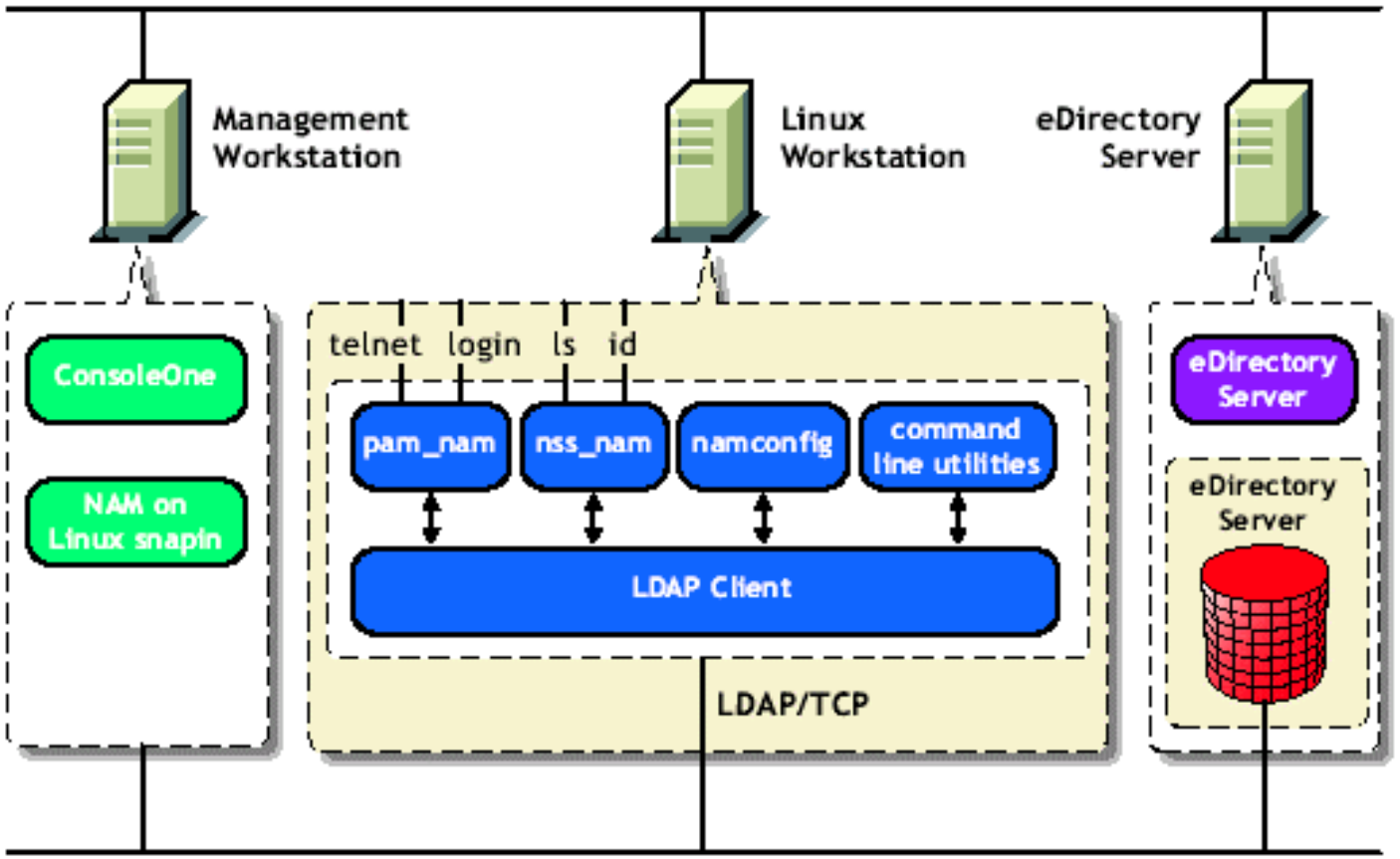
- You want users who are accessing PAM-enabled services, such as login or ftp, on the NNLS server to authenticate through eDirectory.
- You need to provide Samba share-based file services on the NNLS server to Windows users on your network.

LUM Components

The following are the LUM components that enable eDirectory user profile management:

- pam_nam
- nss_nam
- namconfig
- Command line utilities

LUM Components (continued)



eDirectory LUM Objects

LUM deals with 5 types of eDirectory objects:

- **User**

  LUM extends the schema of the user object to store Linux attributes.

- **Group**

  LUM extends the schema of the group object to store Linux attributes.

- **Linux Workstation**

  This object stores information about access control to the server or workstation and other details required for LUM operations.

eDirectory LUM Objects (continued)

- **Linux Config**

  This object stores LUM configuration information for a specific LUM domain.

- **Template**

  This object facilitates the creation of new users who share certain common requirements.

User Accounts

The level of access assigned to an account determines the privileges the account holder has on the system.

Each Linux user account is identified by a unique user name (also called login name or User ID).

Group Accounts

Users are classified into groups to simplify access control to the system.

Every user must belong to at least one default group, the primary group.

Each group is identified by a group name and a Group ID.

How to Configure LUM

As part of the installation process, basic configuration parameters are set that allow LUM to work.

However, you might need to configure LUM after the initial installation for a variety of reasons, such as optimizing performance.

How to Configure LUM (continued)

To understand how to configure LUM, you need to know the following:

- Secure LDAP Connections
- Trustee Assignments and Rights for LUM Objects
- How to Use NAMCONFIG

Secure LDAP Connections

If you configure LUM to use SSL, the NNLS server uses a secure LDAP connection to eDirectory.

This ensures that information exchanged between the NNLS server and eDirectory is securely encrypted.

Trustee Assignments and Rights for LUM Object

When an eDirectory user is being assigned a Linux profile, the following trustees are assigned:

- [Read] rights for all Linux-related attributes to the [Public] trustee
- [Read] rights for the Group Membership attribute to the [Public] trustee
- [Compare] right for the CN attribute to the [Public] trustee

Trustee Assignments and Rights for LUM Object (continued)

When an eDirectory group is assigned a Linux profile, the following trustees are assigned:

- [Read] rights for the Members attribute to the [Public] trustee
- [Read] rights for all Linux-related attributes to the [Public] trustee

How to Use NAMCONFIG

The namconfig utility lets you add or remove LUM from a specified eDirectory context, as well as retrieve or set LUM configuration parameters.

Entering **man namconfig** at a command prompt displays the entire namconfig documentation.

How to Use NAMCONFIG (continued)

The following are basic tasks you can perform with the namconfig utility:

- Configuring a workstation with LUM
- Configuring LUM with LDAP SSL
- Remove LUM
- Setting or getting LUM configuration parameters
- Importing the SSL certificate

How to Perform Basic LUM Tasks

To manage user accounts with LUM, you need to know how to do the following:

- Create a LUM Group
- Create LUM Users
- Assign Passwords to LUM Users
- Create Home Directories for LUM Users
- Edit a Linux Config Object

Create a LUM Group

You can create a LUM group by doing one of the following:

- Create a LUM Group Using namgroupadd
- Convert an eDirectory Group to a LUM Group
- Designate a group as a LUM group during object creation in iManager

(None of these methods creates a Linux group, they just add LUM attributes to eDirectory LUM group objects.)

Create LUM Users

You can create LUM users by doing one of the following:

- Create a LUM User Using namuseradd
- Create Multiple LUM Users with make_nam_user.sh
  - Can be modified to add passwords
- Convert an eDirectory User to a LUM User
- Designate a User as a LUM User During User Object Creation

Assign Passwords to LUM Users

The make_name_user.sh script creates eDirectory users, but it doesn't assign them passwords.

However, passwords are required to log in to the NNLS server.

If you do not modify the **make_name_user.sh** script to add passwords, you can assign eDirectory passwords to LUM users by using **NMAS Login Methods: eDirectory Password** properties for the user object.

Create Home Directories for LUM Users

Initially, LUM users do not have the file system rights (home directories, etc.) normally assigned to Linux users when they are created.

To complete the setup for your LUM users, you need to create a home directory for each user on the NNLS server by logging in as the user in a text-based console (**Ctrl+Alt+F*x***).

Edit a Linux Config Object

You can edit a Linux Config object from iManager by selecting **Linux Config** (under Linux User Management) and selecting the Linux Config object you want to modify.

Exercise 4-4: Implement LUM in Your Container

In this exercise, you do the following:

- Part I: Create a LUM Group for Database User Employees
- Part II: Add Database User Employees to the LUM Group
- Part III: Test LUM Access
- Part IV: Troubleshoot LUM Access

Novell®