

Linux User Management Technology Guide

Novell® Open Enterprise Server

2.0 SP2

November, 2009

www.novell.com



Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2009 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	7
1 Overview	9
1.1 Benefits	9
1.1.1 Administrator Benefits	9
1.1.2 User Benefits	9
1.2 Understanding Linux User Accounts	9
1.2.1 Username and User ID	10
1.2.2 Password	10
1.2.3 Primary Group Name and Group ID	10
1.2.4 Secondary Group Names and Group IDs	11
1.2.5 Home Directory	11
1.2.6 Preferred Shell	11
1.3 Understanding eDirectory Objects and Linux	11
1.3.1 User Accounts in eDirectory	13
1.3.2 Group Objects in eDirectory	13
1.3.3 Source Workstations	13
1.3.4 Linux/UNIX Workstation Objects in eDirectory	14
1.3.5 The Linux/UNIX Config Object in eDirectory	14
1.4 Putting It All Together	14
1.5 What's Next	15
2 Setting Up Linux User Management	17
2.1 Setting Up Linux Computers to Use eDirectory Authentication	17
2.2 Using iManager to Enable Users for Linux Access	19
2.2.1 Running iManager	20
2.2.2 Determining if a Computer Is Running Linux User Management	21
2.2.3 Enabling eDirectory Users to Log In to Linux Computers	22
2.3 Turning Off Linux User Management and eDirectory Authentication	22
3 Setting Up Linux User Management for Domain Services for Windows	23
4 Linux User Management Technology	25
4.1 Tips and Technologies	25
4.2 Understanding Linux User Management Methods for Enabling User Access	26
4.3 Files Modified by Linux User Management	27
4.3.1 The namcd Linux User Management Caching Daemon	27
4.3.2 Starting and Stopping namcd	27
4.4 Linux User Management and the Pluggable Authentication Module	28
5 Using the Command Line to Configure Linux User Management	29
5.1 Using namconfig	29
5.1.1 namconfig Command Line Parameters	29
5.1.2 Configuring Failover Mechanism	30
5.1.3 Configuring a Workstation with Linux User Management	30
5.1.4 Configuring Linux User Management with LDAP SSL	31

5.1.5	Removing Linux User Management Configuration	31
5.1.6	Setting or Getting Linux User Management Configuration Parameters	32
5.1.7	Using namconfig to Import an SSL Certificate	32
5.2	Editing the nam.conf File	32
6	Managing User and Group Objects in eDirectory	35
6.1	Using Novell iManager to Manage Linux User Management	35
6.1.1	Running iManager	35
6.1.2	Creating a New Group Object for Linux User Management Users	35
6.1.3	Enabling an Existing Group Object for Linux User Management	36
6.1.4	Creating a User Object for Linux User Management	39
6.1.5	Enabling an Existing User Object for Linux User Management	40
6.1.6	Modifying a UNIX Config Object	43
6.1.7	Modifying a UNIX Workstation Object	44
6.1.8	Enabling an Existing User Object for Samba	45
6.2	Using Command Line Utilities to Manage Users and Groups	46
6.2.1	Security Considerations	46
6.2.2	nambulkadd	47
6.2.3	namuseradd	49
6.2.4	namgroupadd	51
6.2.5	namusermod	52
6.2.6	namgroupmod	53
6.2.7	namuserdel	54
6.2.8	namgroupdel	55
6.2.9	namuserlist	56
6.2.10	namgroupdel	56
7	Troubleshooting	59
7.1	Troubleshooting Linux User Management	59
7.1.1	Linux User Management Returns Invalid UID and GID for Users and Groups	59
7.1.2	namconfig Fails	60
7.1.3	namcd Indicates That a Certificate Is Not Found	60
7.1.4	Duplication of UIDs and GIDs	60
7.1.5	A User Cannot Log In	60
7.1.6	Password Expiration Information for the User Is Not Available	60
7.1.7	ID Command Not Giving the Desired Results	61
7.1.8	namcd Not Coming Up after a System Reboot	61
7.1.9	Log Files for Linux User Management	61
7.1.10	Missing Mandatory Attribute Error When Adding a User to a Linux User Management Group	61
7.1.11	SUSE Linux Enterprise Desktops Configured as UNIX Workstation Objects	62
7.2	Making Home Directories Private	62
7.3	Troubleshooting Account Redirection Problems	62
7.4	Changing the Name of the Original Container Passed to namconfig	62
8	Other Issues and Considerations	65
8.1	Linux User Management Configuration for Domain Services for Windows	65
8.2	Allocating User IDs and Group IDs	65
8.3	RFC 2307 Schema Extension	65
8.4	Running Linux User Management in a Virtualization Environment	66
8.5	Configuring Linux User Management for Novell Cluster Services	66
8.6	Security Considerations for Linux User Management	66
8.7	Usernames for Linux User Management Users	66

About This Guide

This guide explains and describes how to use Novell® Linux User Management (LUM), a directory-enabled application that simplifies and unifies the management of user profiles on Linux*-based platforms. It leverages all the scalability, utility, and extensibility of Novell eDirectory™ and adds crucial integration capability. With Linux User Management, you can eliminate many of the complexities of administering a mixed-platform network while smoothing over compatibility issues.

This guide is divided into the following sections:

- ♦ Chapter 1, “Overview,” on page 9
- ♦ Chapter 2, “Setting Up Linux User Management,” on page 17
- ♦ Chapter 3, “Setting Up Linux User Management for Domain Services for Windows,” on page 23
- ♦ Chapter 4, “Linux User Management Technology,” on page 25
- ♦ Chapter 5, “Using the Command Line to Configure Linux User Management,” on page 29
- ♦ Chapter 6, “Managing User and Group Objects in eDirectory,” on page 35
- ♦ Chapter 7, “Troubleshooting,” on page 59
- ♦ Chapter 8, “Other Issues and Considerations,” on page 65

Audience

This guide is intended for network administrators and network installers responsible for integrating and managing users in a Linux and eDirectory environment.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with Open Enterprise Server. To contact us, use the User Comments feature at the bottom of any page in the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

The most recent version of *Linux User Management Technology Guide* is available on the [Novell documentation Web site](http://www.novell.com/documentation) (<http://www.novell.com/documentation>).

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as UNIX* or Linux, should use forward slashes as required by your software.

Linux User Management lets you configure Linux workstations and servers on the network so users can log in to them by using user login information stored in Novell® eDirectory™ instead of user login information stored on each computer.

- ♦ [Section 1.1, “Benefits,” on page 9](#)
- ♦ [Section 1.2, “Understanding Linux User Accounts,” on page 9](#)
- ♦ [Section 1.3, “Understanding eDirectory Objects and Linux,” on page 11](#)
- ♦ [Section 1.4, “Putting It All Together,” on page 14](#)
- ♦ [Section 1.5, “What's Next,” on page 15](#)

1.1 Benefits

Linux User Management and eDirectory work together to simplify administration and provide users with access to network resources.

- ♦ [Section 1.1.1, “Administrator Benefits,” on page 9](#)
- ♦ [Section 1.1.2, “User Benefits,” on page 9](#)

1.1.1 Administrator Benefits

Using Linux User Management and eDirectory to manage user login information eliminates the need to create local users in the `/etc/passwd` and `/etc/shadow` files on each Linux computer. It simplifies user account management by consolidating user accounts into a central point of administration.

You can use eDirectory tools and technologies to manage access to Linux resources on the network. After authenticating, users have the rights and privileges as specified in eDirectory. These are the same rights and privileges that would typically need to be stored in a local account or redirected to other authentication methods, such as NIS. The user account information stored in eDirectory lets users access file and printer resources on the network.

1.1.2 User Benefits

Users can log in to Linux computers by using access methods such as login, FTP, SSH, su, rsh, rlogin, xdm (KDE), and gdm (GNOME*). They simply enter their familiar eDirectory credentials. There is no need to remember a full context. Linux User Management finds the correct user in eDirectory.

Users can log in once, using a single username and password, and have seamless access to all their network resources regardless of platform.

1.2 Understanding Linux User Accounts

Setting up and using eDirectory to manage Linux access requires you to understand how the Linux operating system manages user logins.

Users who want to log in to a Linux computer must have an existing user account, which consists of properties that allow a user to access files and folders stored on the computer. This account information can be created and stored on the computer itself or on another computer on the network. Accounts stored on the computer are called *local user accounts*. Accounts stored in eDirectory are called *eDirectory user accounts*, regardless of whether they are stored on the same computer or another computer. A typical account used to log in to a Linux computer consists of the following information:

- ♦ Username and user ID (UID)
- ♦ Password
- ♦ Primary group name and group ID (GID)
- ♦ Secondary group names and group IDs
- ♦ Location of home the directory
- ♦ Preferred shell

When a local user account is created, Linux records the user-login information and stores the values in the `/etc/passwd` file on the computer itself. The `passwd` file can be viewed and edited with any text editor. Each user account has an entry recorded in the following format:

```
username:password:UID:GID:name:home directory:shell
```

1.2.1 Username and User ID

The username and user ID (UID) identify the user on the system. When a user account is created, it is given a name and assigned a UID from a predetermined range of numbers. The UID must be a positive number and is usually above 500 for user accounts. System accounts usually have numbers below 100.

1.2.2 Password

Each user account has its own password, which is encrypted and stored on the computer itself or on another computer on the network. Local passwords are stored in the `/etc/passwd` file or `/etc/shadow` file. When the user logs in by entering a username and password, Linux takes the entered password, encrypts it, and then compares the encrypted value to the value of the password stored in the user account. If the entered value is the same as the value stored in the password field on the computer, the user is granted access.

Administrators often use the `/etc/passwd` file to hold user account information but store the encrypted password in the `/etc/shadow` file; when this method is used, the `passwd` file entry has an `x` in the password field.

1.2.3 Primary Group Name and Group ID

Groups are used to administer and organize user accounts. When rights and permissions are assigned to a group, all user accounts that are part of the group receive the same rights and permissions. The group has a unique name and identification number (GID). The primary GID and group name are stored as entries in the `/etc/passwd` file on the computer itself or in eDirectory.

Each user has a designated primary (or default) group and can also belong to additional groups called *secondary groups*. When users create files or launch programs, those files and programs are associated with one group as the owner. A user can access files and programs if he or she is a member of the group with permissions to allow access. The group can be the user's primary group or any of his or her secondary groups.

1.2.4 Secondary Group Names and Group IDs

Although not strictly part of the user account, secondary groups are also a part of the user login experience. Groups and GIDs are used to manage rights and permissions to other files and folders. Secondary groups for each user are listed as entries in `/etc/group` on the computer itself.

NOTE: When you use the `id` command to show user IDs and groups, if case-sensitivity is set to `no`, you must enter the exact case to display secondary groups. If you enter a different case, you see only the primary groups.

1.2.5 Home Directory

The home directory is a folder used to store a user's personal documents. In addition, it offers a place to store configuration files unique to the user. Therefore, a user can log in and find his or her environment with the same settings that were used before, even if another user has used the computer. Typically, most computers have all home directories at `/home`, and then individual directories listed by login name (for example, `/home/jsmith`). The `root` user's home directory is an exception. It is traditionally located at `/` or `/root`. Placing home directories under `/home` is not required, but it makes organizational sense. Some administrators divide the `/home` directory by function or department and then subdivide the `/home` directory with users in that department (for example, `/home/engineering/jsmith`).

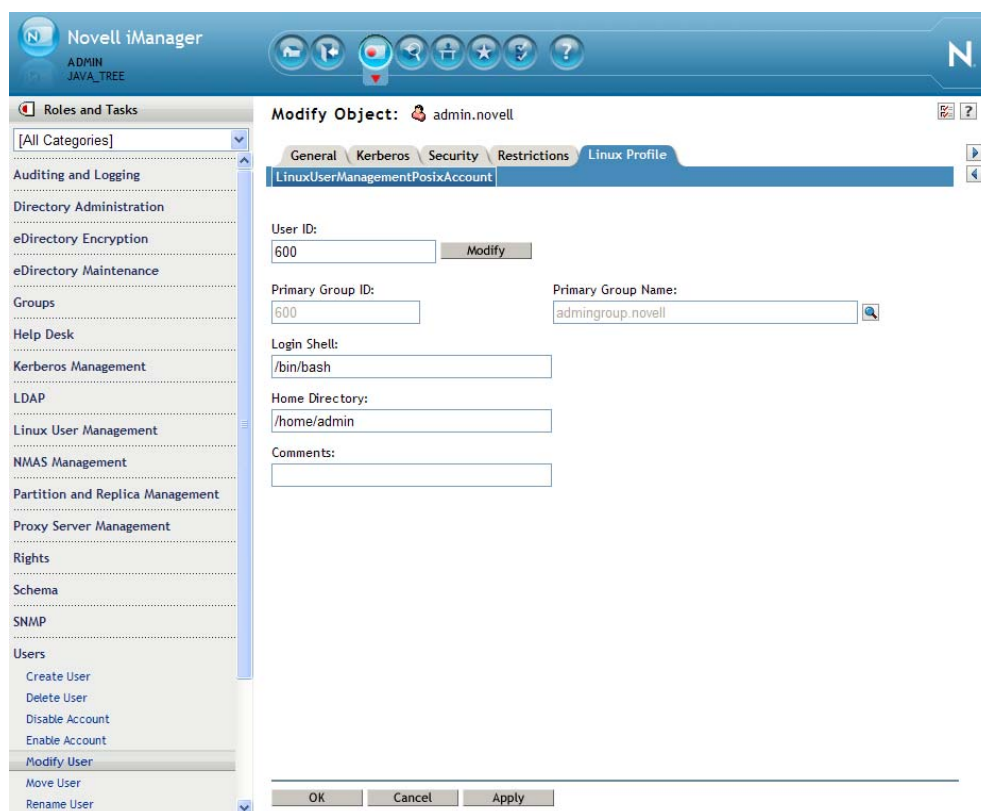
1.2.6 Preferred Shell

A shell is a program designed to accept and execute commands typed at a prompt. It is similar to the DOS `command.com` command interpreter. Several standard shells are available with Linux. The default is usually `/bin/bash`.

1.3 Understanding eDirectory Objects and Linux

eDirectory and Linux User Management technologies work together to provide a solution for managing user access to network resources. eDirectory user login information is stored as a property of the User object. It is viewed and modified by using Novell iManager.

Figure 1-1 The Novell iManager Window



When a user logs in to a Linux computer running Linux User Management, the request is redirected to eDirectory and checked against information in eDirectory. For this to work, the computers and eDirectory must be configured as follows:

- ♦ The target workstation must be running Linux User Management software and must point to the Linux/UNIX Config object on the network.
- ♦ The target workstation must have a representative Linux/UNIX Workstation object in eDirectory, created when Linux User Management components are installed.
- ♦ The user must be enabled for Linux, which means that the user must be a member of a group enabled for Linux and stored in the properties of Linux/UNIX Workstation object. The Linux/UNIX Config object must specify the context of the Linux Workstation object.
- ♦ [Section 1.3.1, “User Accounts in eDirectory,” on page 13](#)
- ♦ [Section 1.3.2, “Group Objects in eDirectory,” on page 13](#)
- ♦ [Section 1.3.3, “Source Workstations,” on page 13](#)
- ♦ [Section 1.3.4, “Linux/UNIX Workstation Objects in eDirectory,” on page 14](#)
- ♦ [Section 1.3.5, “The Linux/UNIX Config Object in eDirectory,” on page 14](#)

1.3.1 User Accounts in eDirectory

User accounts residing on the Linux computer are said to be *local user accounts* and are stored as entries in the `/etc/passwd` file. User accounts in eDirectory are represented by User objects stored in the eDirectory tree.

An eDirectory User object has a rich set of properties and fields to hold user-login properties. When an eDirectory User object is extended to hold Linux user-login properties, it is said to be *LUM-enabled* or *enabled for Linux*. When enabled for Linux, a user can simply access the Linux computer (by using Telnet, SSH, or other supported method) and enter his or her username and password. The access request is redirected to find the appropriate username and login information stored in eDirectory.

When it is extended for Linux, the eDirectory User object holds Linux-related properties, such as user ID, primary group ID, primary group name, location of home directory, and preferred shell.

1.3.2 Group Objects in eDirectory

When a group is enabled for Linux, the group ID is stored as a property of a Linux/UNIX Workstation object. When the user attempts to log in to a Linux computer, he or she only needs to enter a username and password—no context is required. The Linux computer checks its corresponding Linux/UNIX Workstation object in eDirectory for the list of groups approved to log in. Each approved group is searched for the username of the user requesting access. When the first matching username is found, the login is allowed by using the UID, GID, password, and other login information stored in eDirectory. If the username is not found in any of the groups, the login is not allowed.

NOTE: When you Linux-enable a Group object, you can choose to enable all members of the group or you can enable specific users. Users being enabled for the first time receive the group ID as their primary ID. Users previously enabled for Linux receive the GID as a secondary GID. User objects not enabled for Linux cannot log in to a Linux computer, even if they belong to a Linux-enabled group.

In addition to the typical Linux-related properties (for example, Group ID), the eDirectory Group object extended for Linux holds some additional properties:

- ♦ **UamPosixWorkstationList:** Lists the UNIX Workstation objects that the group has permissions to access.
- ♦ **Description:** Displays an alternative description.

1.3.3 Source Workstations

The source workstation is the computer that the user accesses the target workstation from. It is not represented as an object in eDirectory. It can be running any type of operating system, desktop, or server that supports login access protocols such as FTP, SSH, rlogin, and rsh. To log in to a target workstation, the user launches a program that provides one of the supported login access protocols and then enters the address of the target workstation.

1.3.4 Linux/UNIX Workstation Objects in eDirectory

In eDirectory, the Linux/UNIX Workstation object represents the actual computer the user logs in to. The computer, also known as the *target computer*, must have the following characteristics:

- ♦ It is running Linux as either a server or workstation.
- ♦ It is running Pluggable Authentication Module (PAM) along with Novell Linux User Management technology to redirect login requests to eDirectory (see the `/etc/pam.d` directory).
- ♦ It stores the location of the UNIX Config object on the network (see the `nam.conf` file).

A Linux/UNIX Workstation object is created when Linux User Management components are installed on the target computer. The object can be placed in any Organization (O) or Organizational Unit (OU) container in the eDirectory tree.

When logging in to a target workstation, the user needs to enter only his or her username and password. The target workstation receives the login request and uses Linux User Management and PAM to redirect authentication to eDirectory and the Linux/UNIX Config object on the network. The Linux/UNIX Config object directs the request to the target computer's representative Linux/UNIX Workstation object, where the groups, usernames, and full contexts are determined.

The Linux/UNIX Workstation object holds the following set of properties:

- ♦ Target workstation name. The name is Linux/UNIX Workstation appended with the host name of the target workstation (for example, Linux/UNIX Workstation - Server1).
- ♦ List of eDirectory groups (names and contexts) that have access to the target workstation.

1.3.5 The Linux/UNIX Config Object in eDirectory

The Linux/UNIX Config object is an object in eDirectory that stores a list of the locations (contexts) indicating where Linux/UNIX Workstation objects reside on the network (in eDirectory). It also controls the range of numbers to be assigned as UIDs and GIDs when User and Group objects are created. Geographically dispersed networks might require multiple Linux/UNIX Config objects in a single tree, but basic networks need only one Linux/UNIX Config object in the eDirectory tree. The object is created during the Linux OS installation (by selecting Linux User Management) and should be placed in the upper containers of the eDirectory tree.

1.4 Putting It All Together

When properly configured, eDirectory objects and Linux User Management technology let you manage access to Linux resources on the network. Here's how it works:

1. At a source workstation, the user launches a program (such as SSH or FTP) that provides login access to another computer.
2. When prompted by the login program, the user enters his or her username and identifies the name or address of a target workstation. For example, the user might launch SSH, enter `tom` as the username, and the address of a target workstation with the following command:

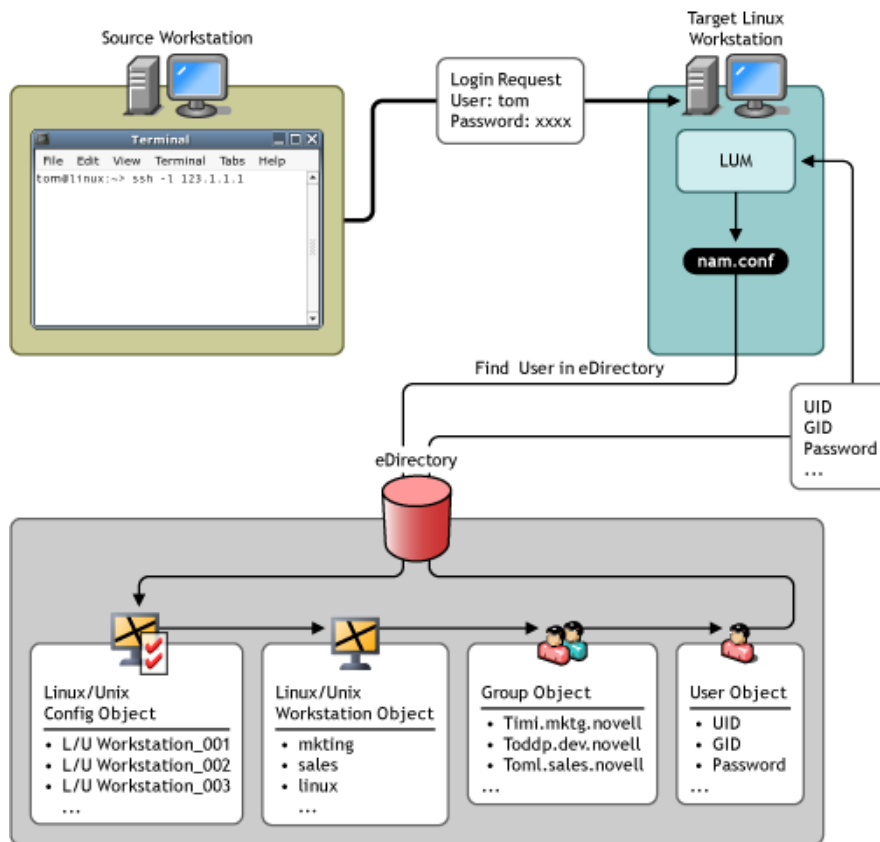
```
ssh -l tom 10.10.1.1
```

3. The target workstation receives the login request, but before granting access, it must find the requester's full context username and verify that the password is correct. This login information is stored in eDirectory instead of on the target workstation.

4. To find the requester's login information, the target workstation (configured with Linux User Management) performs the following actions:
 - a. Finds the location of the Linux/UNIX Config object listed in the local `nam.conf` file.
 - b. Searches the Linux/UNIX Config object properties to find the location of the Linux/UNIX Workstation object.
 - c. Searches the groups approved for access listed in the Linux/UNIX Workstation object to find the requester's username.
- For example, if the login request is from a user named Tom, the list of groups is searched until a User object with the username Tom is found.
- d. Submits the requester's password for verification against the user information stored in eDirectory.
 - e. Grants the login request by using eDirectory login information, such as UID, GID, home directory, and preferred shell.

The following illustration shows how Linux User Management, eDirectory, and PAM all work together to let users log in to target workstations on the network.

Figure 1-2 Logging In to Target Workstations



1.5 What's Next

To install and set up Linux User Management in your network environment, see [Chapter 2, "Setting Up Linux User Management,"](#) on page 17.

Setting Up Linux User Management

2

The following information can help you install and set up Linux User Management technology on your network to gain the advantages of eDirectory™ for user authentication. iManager can be used for basic setup, but you might need to use a command line interface to accomplish some specific tasks. In either case, you need to set up the computer to use eDirectory authentication and create and correctly configure the eDirectory objects.

- [Section 2.1, “Setting Up Linux Computers to Use eDirectory Authentication,” on page 17](#)
- [Section 2.2, “Using iManager to Enable Users for Linux Access,” on page 19](#)
- [Section 2.3, “Turning Off Linux User Management and eDirectory Authentication,” on page 22](#)

This section guides you through the steps required to set up a Linux computer to use eDirectory for authentication, followed by the steps to set up eDirectory by using iManager. Tasks requiring a command line interface are described in [Chapter 5, “Using the Command Line to Configure Linux User Management,” on page 29](#).

2.1 Setting Up Linux Computers to Use eDirectory Authentication

Before users can use eDirectory user-login information to log in, the target workstation or server must be configured with Linux User Management components. You are prompted to set up Linux User Management while installing the operating system. You can also set it up afterwards by using YaST.

IMPORTANT: Setting up Linux User Management requires administrator rights to the container where the Linux User Management objects are created.

To use YaST to install and configure Linux User Management on a workstation or server that is already running:

- 1 Follow the instructions for your platform for adding services to an existing server or workstation. For more information, see the [OES2 SP1: Linux Installation Guide](#).
- 2 From the desktop environment, launch YaST.
- 3 Click *Security and Users > Linux User Management*.
- 4 Specify whether eDirectory is running on the computer itself (Local System) or on another computer on the network (Remote System).

Linux User Management Configuration

Directory Server Address
192.168.1.255

Unix config context (e.g. o=novell)
ou=novell,ou=frd74,o=novell

UNIX workstation context (e.g. o=novell)
ou=novell,ou=level1,ou=frd74,o=novell

Proxy user name with context (e.g. cn=proxy,o=novell)
(optional)

Proxy user password

☒ Restrict access to the home directories of other users

Back Abort Next

- 5 (Conditional) If eDirectory is running on a remote system, specify the remote system's IP address.
- 6 Specify the admin name and context and the admin password, then click *Next*.
- 7 Specify the Linux User Management configuration, then click *Next*.

Linux User Management Configuration

Select services to LUM-enable for authentication via eDirectory

Select All Deselect All

☐ login
☐ ftp
☐ sshd
☐ su
☒ opgnwibem
☐ gdm
☐ gnomesu-pam

Back Abort Next

Specify the locations of the Linux/UNIX Config and the Linux Workstation objects.

NOTE: The Linux Workstation object is also called the *LUM Workstation*.

- ♦ If a Linux/UNIX Config object already exists in the eDirectory tree, specify its name and context. If no Linux/UNIX Config object exists in eDirectory, specify the name and context for a new Linux/UNIX Config object to be created.
 - ♦ Specify the context where the UNIX Workstation object is to be created.
- 8 Select which login access methods should use eDirectory for authentication.
- If you have selected *ftp*, by default OES chooses *vsftpd*.



Installing and configuring Linux User Management technology sets up the target computer to validate login requests against user account information stored in eDirectory. Before users can log in, they must have eDirectory user accounts created with iManager and extended for Linux User Management.

2.2 Using iManager to Enable Users for Linux Access

When Linux User Management components are properly installed, administrators can use Novell eDirectory and iManager to specify which users can access Linux computers on the network. iManager is the browser-based utility for managing eDirectory objects. It runs in a network browser such as Mozilla* Firefox*, Netscape* Navigator*, or Internet Explorer*.

When you create user or group accounts in iManager, you are prompted to enable the User object or Group object for Linux User Management. You can also use iManager to enable existing User or Group objects for Linux.

- ♦ [Section 2.2.1, “Running iManager,” on page 20](#)
- ♦ [Section 2.2.2, “Determining if a Computer Is Running Linux User Management,” on page 21](#)
- ♦ [Section 2.2.3, “Enabling eDirectory Users to Log In to Linux Computers,” on page 22](#)

2.2.1 Running iManager

You can launch iManager by entering the following command in the Address field of a network browser:

`http://target_server/nps`

where *target_server* is the IP address or domain name of the target server. You are prompted to provide the full context of the admin user (for example, admin.mycompany) and password.


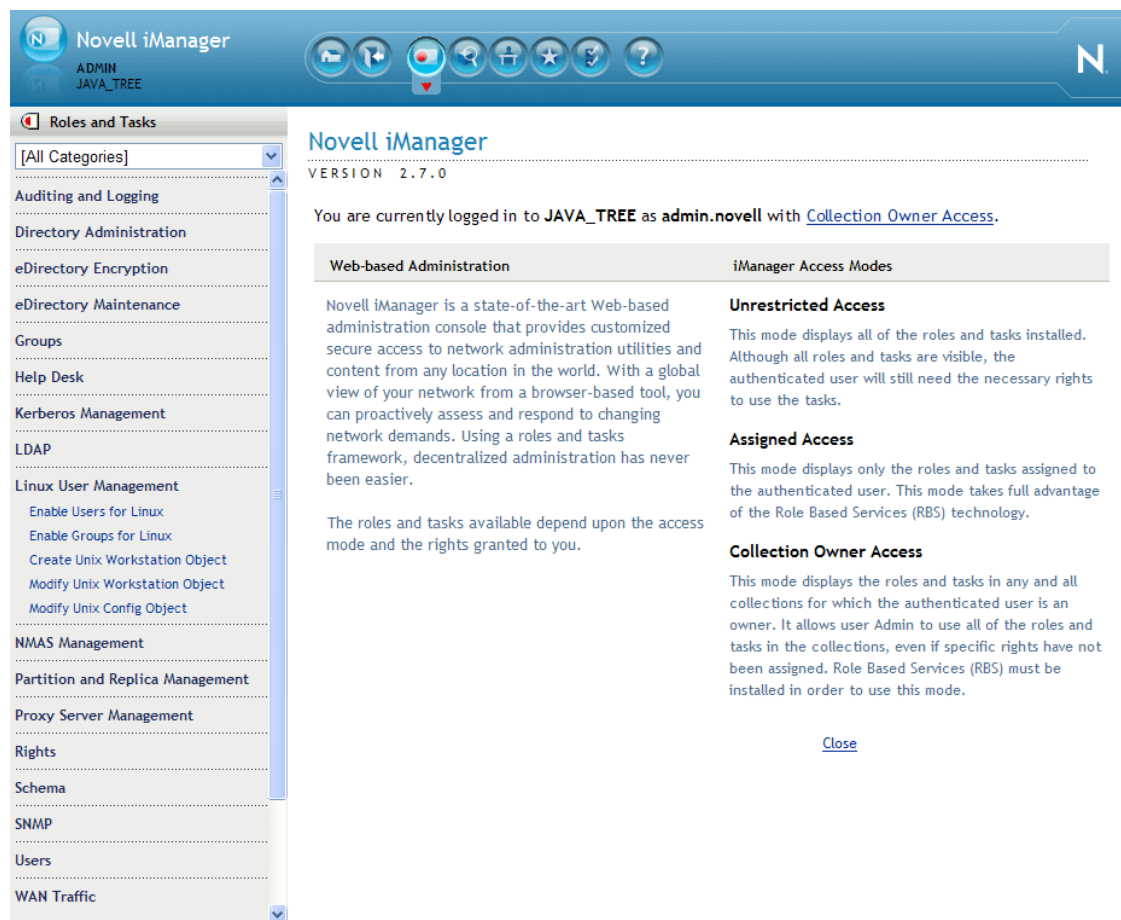
After logging in to iManager, make sure you are in the *Roles and Tasks* view (by clicking  on the top button bar), then select Linux User Management in the navigation panel on the left.

Figure 2-1 Roles and Tasks View



The Linux User Management category in iManager contains links to help you complete the following tasks:

- ♦ Enable users for Linux
- ♦ Enable groups for Linux
- ♦ Modify Linux/UNIX Configuration objects
- ♦ Modify Linux Workstation objects

2.2.2 Determining if a Computer Is Running Linux User Management

For users to log in by using eDirectory login credentials, the computer must be running Linux User Management components. These components can be installed as part of the operating system installation or can be added afterwards through an RPM.


During the Linux User Management installation, you are prompted to create a Linux Workstation object and place it in the network directory (eDirectory). You are also prompted to specify an existing object or create a new Linux/UNIX Config object in eDirectory.

NOTE: Typical networks require only one Linux/UNIX Config object in eDirectory.

To determine if a computer is running Linux User Management components:

- 1 Log in to the target computer.
- 2 Open a shell session.
- 3 Enter `rpm -q novell-lum`
This shows whether the Linux User Management software is *installed*.
- 4 Verify that the `/etc/nam.conf` file exists.
This shows whether Linux User Management is *configured*.
- 5 (Optional) View `nam.conf` in a text editor to see what login access technologies are currently being redirected to eDirectory.

To view Linux workstations available through eDirectory:

- 1 Launch iManager.
- 2 Click *Linux User Management > Modify Linux Workstation Object*.
- 3 Click the Object Selector icon and browse the eDirectory tree.
Each Linux Workstation object  represents a Linux computer on the network.

There might be existing eDirectory Group objects that already provide access to Linux computers on the network.

To view the Groups that can use eDirectory to log in to a Linux computer:

- 1 Launch iManager.
- 2 Click *Linux User Management > Modify Linux Workstation Object*.
- 3 Select a Linux Workstation object, then click *OK*.
Groups listed in the *Group Membership* field provide access to the selected Linux workstation.

To view the Linux computers that members of an eDirectory Group can log in to:

- 1 Launch iManager.
- 2 Click *Groups > View My Groups*.
- 3 Select a group, then click *Edit*.
- 4 From the drop-down list, select *Linux Profile*.

2.2.3 Enabling eDirectory Users to Log In to Linux Computers

You can enable existing eDirectory users to log in to Linux computers by completing the *Enable Users for Linux* task.

1 Select the user (User object) to enable for Linux.

2 Assign the user to a group.

The group and its corresponding GID are assigned as the user's primary GID. If the selected user account already has a primary GID, this group's GID is assigned to the user as secondary.

You can choose one of three ways to assign the user to a group:

- ♦ *Select an Existing eDirectory Group*: If the Group object has not yet been enabled for Linux, using this option extends the its properties to include Linux login attributes. You can click the Object Selector icon to browse the tree for an existing group.
- ♦ *Select an Existing Linux-Enabled Group*: This option lets you select an existing eDirectory Group object, but if you use the Object Selector to browse, you can view and select only those Group objects already extended with Linux login attributes.
- ♦ *Create a New Linux-Enabled Group*: This option lets you create a new eDirectory Group object. When it is created, the Group object is extended to include Linux login attributes.

3 Select the workstations that the group is to have access to.

4 Click *Finish* to apply the changes.

Users should now be able to use eDirectory user login credentials to log in to Linux computers running Linux User Management technology.

2.3 Turning Off Linux User Management and eDirectory Authentication

There might be times when you want to turn off the target workstation's or server's ability to accept logins from eDirectory. You can permanently turn off this ability by removing the Linux User Management software from the target computer. You can temporarily disable eDirectory authentication and Linux User Management by stopping the `namcd` daemon.

To stop `namcd`, open a shell window and enter `rcnamcd stop`.

To turn on eDirectory authentication and Linux User Management, open a shell window and enter `rcnamcd start`.

Setting Up Linux User Management for Domain Services for Windows

3

Novell® Domain Services for Windows* (DSfW) creates seamless cross-authentication capabilities between Windows or Active Directory* and Novell OES 2 Linux or eDirectory servers.

With DSfW, eDirectory users can use familiar Windows desktop operations to access file services regardless of the platform or the operating system where the service resides.

- ♦ When configuring Linux User Management on a DSfW tree, YaST does not prompt for user credentials. It takes the configuration parameters from the DSfW configuration.
- ♦ The UNIX config object and the UNIX workstation objects in an FRD are created under `ou=novell, $domain`.
- ♦ For child domains, the UNIX config object and the UNIX workstation objects are created under `ou=novell, $child_domain`.
- ♦ For name-mapped configurations YaST modifies the existing UNIX config object in the tree if the eDirectory tree is already enabled for Linux User Management. For more information, see [Chapter 7, “Troubleshooting,” on page 59](#)

Linux User Management Technology

4

This section explains the details of the modules and components used by Linux User Management technology.

- ♦ [Section 4.1, “Tips and Technologies,” on page 25](#)
- ♦ [Section 4.2, “Understanding Linux User Management Methods for Enabling User Access,” on page 26](#)
- ♦ [Section 4.3, “Files Modified by Linux User Management,” on page 27](#)
- ♦ [Section 4.4, “Linux User Management and the Pluggable Authentication Module,” on page 28](#)

4.1 Tips and Technologies

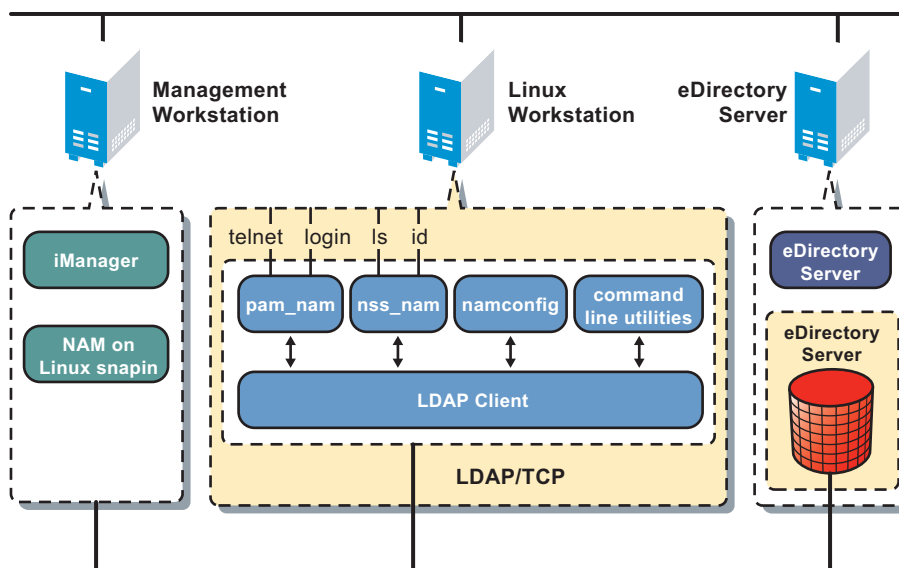
Linux User Management uses the Pluggable Authentication Module (PAM) framework to manage account authentication and other access requests. PAM provides an extensible interface that applications can use to resolve access requests.

After Linux User Management components are installed and configured on a Linux workstation or server, eDirectory™ is used for requests relating to authentication, account management, password management, and session management. Linux User Management technology leverages the following components to provide login access through eDirectory.

- ♦ **pam_nam:** Provides authentication, account, session, and password services for all PAM-enabled applications on the server.
- ♦ **nss_nam:** A Name Service Switch redirector that enables user access to system resources by checking user profiles against access rights.
- ♦ **namconfig:** A Linux command line utility that lets you set Linux User Management configuration parameters. You can also use namconfig to import the SSL certificate into the local machine.
- ♦ **Other command line utilities:** Linux User Management provides Linux command line utilities for creating, managing, and deleting user and group accounts.
- ♦ **iManager plug-in:** Administrators running iManager on a Linux server can use iManager to create, manage, and delete user and group accounts.

The following figure provides a graphical overview of Linux User Management components.

Figure 4-1 Linux User Management Components



4.2 Understanding Linux User Management Methods for Enabling User Access

When a user accesses system resources, the user's profile must be checked for access rights. This requires a one-to-one mapping between the user or group name and system-identifiable numbers such as the User ID or Group ID to enable user provisioning. This is done by name service providers that make name service calls to obtain user or group profiles from user or group databases.

Typically, the Name Service Switch (NSS) redirector is used to isolate name service providers from applications. Linux User Management provides a name switch service provider, `nss_nam`, that retrieves user or group profiles from eDirectory. The switch allows different database providers to be registered for each database, and when an application invokes the NSS, it chains through the providers listed for that database. The `nss_nam` module uses LDAP to retrieve this information from eDirectory.

The `nss_nam` module is plugged in through the `/etc/nsswitch.conf` configuration file. Sample entries from the file are given below:

```
passwd: files nam
group: files nam
```

The first field on each line is the name of the Linux database. The second and subsequent entries, if any, specify the name of the service provider.

eDirectory provides a hierarchical organization of various entities such as users, groups, Linux workstations, and so on. Each User object in eDirectory is a leaf node in a specific branch of the organization-wide tree. The user is identified by a corresponding context, for example, `chuck.javagroup.us.novell`.

By providing a transparent mechanism for contextless login, `nss_nam` does away with the need for Linux users to remember the eDirectory context. `nss_nam` resolves the contextless name provided by the Linux user during login. The contextless name is resolved to the Linux Workstation object for

the current host in eDirectory. The Linux Workstation object specifies the groups with access to the Linux system. Only those users who are members of these groups are allowed to log into the workstation. If a matching user is found, the corresponding Linux profile is returned.

4.3 Files Modified by Linux User Management

When Linux User Management is installed, the install process adds the eDirectory source (by using the string `nam`) to the `passwd` and `group` database entries in the `/etc/nsswitch.conf` file to activate the Linux User Management accounts. For example, the entries might be modified to include `nam` as follows:

```
passwd: files  nam  nisplus
shadow: files  nam  nisplus
group:  files  nam  nisplus
```

The installation also modifies PAM-enabled service files in the `/etc/pam.d./` directory to use eDirectory authentication.

- ♦ [Section 4.3.1, “The `namcd` Linux User Management Caching Daemon,” on page 27](#)
- ♦ [Section 4.3.2, “Starting and Stopping `namcd`,” on page 27](#)

4.3.1 The `namcd` Linux User Management Caching Daemon

When `nss_nam` receives name service requests, it contacts the eDirectory caching daemon, `namcd`, which is responsible for retrieving and caching entries from eDirectory.

The `namcd` daemon caches the fully distinguished name (FDN) of User objects. Whenever the `pam_nam` and the `nss_nam` modules access the eDirectory database to retrieve a User object, the `namcd` daemon caches the FDN of that User object. eDirectory searches the cache before accessing the eDirectory database, making the access quicker. The behavior of `namcd` is determined by the configuration parameters set in the configuration file `/etc/nam.conf`.

The `namcd` daemon also provides a persistent cache on workstations, which improves access time if the data does not change frequently. If you enable persistent caching, all user profiles, group profiles, and the FDNs of User objects are cached. If persistent caching is disabled, only the User FDNs are cached. You can enable or disable persistent caching by setting the `enable-persistent-cache` parameter in the `/etc/nam.conf` file. By default, persistent caching is enabled.

4.3.2 Starting and Stopping `namcd`

To run the `namcd` daemon:

```
/etc/init.d/namcd  start
```

To stop the `namcd` daemon:

```
/etc/init.d/namcd  stop
```

The `namcd` daemon can be configured by using the `namconfig` utility. Its configuration parameters are set in the `/etc/nam.conf` file. For more information, refer to [Section 5.2, “Editing the `nam.conf` File,” on page 32](#).

4.4 Linux User Management and the Pluggable Authentication Module

The `pam_nam` module can be dynamically loaded to provide the necessary functionality upon demand. The PAM sample files are located in `/etc/pam.d/pam_nam_sample`.

The following is an example of an entry in the configuration file for login:

```
auth    required    /lib/security/pam_nam.so
```

Specify the application requiring the authentication service in the first field. Specify the name of the service provided in the second field. In the third field, specify the control flag. In the fourth field, specify the name of the module providing the service.

The control flag can be of the following types:

- ♦ **Required:** This flag is set when authentication by the module is required. If the authentication is not successful, an error message is returned to the caller, after executing all the modules in the stack.
- ♦ **Optional:** This flag is set when authentication by the module is optional. If the module fails, the PAM framework ignores the module failure and continues with processing the next module in the sequence. If this flag is used, the user is allowed to log in, even if that particular module failed.
- ♦ **Sufficient:** This flag is set when authentication is required only by one module. If the module succeeds, the application does not try another module. When authentication fails, the modules with flags set to Sufficient are treated as optional.

The following options can be passed to the PAM module:

- ♦ **use_first_pass:** This option compares the password in the password database with the user's initial password (entered when the user authenticated to the first authentication module in the stack). If the passwords do not match, or if no password has been entered, the module quits and does not prompt the user for a password. This option should only be used if the authentication service is designated as optional in the files in the `/etc/pam.d/nam` or `/etc` directory.
- ♦ **try_first_pass:** This option compares the password in the password database with the user's initial password (entered when the user authenticated to the first authentication module in the stack). If the passwords do not match, or if no password has been entered, the user is prompted for a password. When prompting for the current password, the PAM authentication module uses the following prompt:

```
password
```

However, a different prompt is used if one of the following scenarios occur:

- ♦ The *try_first_pass* option is specified and the password entered for the first module in the stack fails for the PAM module.
- ♦ The *try_first_pass* option is not specified, and the earlier authentication modules listed in the files in the `/etc/pam.d/nam` directory have prompted the user for the password.

In these two cases, the Linux User Management authentication module uses the following prompt:

```
eDirectory password.
```

Using the Command Line to Configure Linux User Management

During the server installation process, Linux User Management components are installed and basic parameters are set. To optimize performance, you can also configure some Linux User Management server components after installation by using the commands in this section.

- ♦ [Section 5.1, “Using namconfig,” on page 29](#)
- ♦ [Section 5.2, “Editing the nam.conf File,” on page 32](#)

5.1 Using namconfig

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

- ♦ [Section 5.1.1, “namconfig Command Line Parameters,” on page 29](#)
- ♦ [Section 5.1.2, “Configuring Failover Mechanism,” on page 30](#)
- ♦ [Section 5.1.3, “Configuring a Workstation with Linux User Management,” on page 30](#)
- ♦ [Section 5.1.4, “Configuring Linux User Management with LDAP SSL,” on page 31](#)
- ♦ [Section 5.1.5, “Removing Linux User Management Configuration,” on page 31](#)
- ♦ [Section 5.1.6, “Setting or Getting Linux User Management Configuration Parameters,” on page 32](#)
- ♦ [Section 5.1.7, “Using namconfig to Import an SSL Certificate,” on page 32](#)

5.1.1 namconfig Command Line Parameters

Table 5-1 *Command Line Parameters for namconfig*

Parameter	Description
add	Configures Linux User Management against the specified Workstation object context in eDirectory.
rm	Removes configuration from Linux User Management.
upgrade	Upgrades from an earlier version of Linux User Management.
set valuelist	Sets the value for the specified Linux User Management configuration parameters. For a complete list of configurable parameters, refer to Table 5-2 on page 32 .
get paramlist	Retrieves the value for the specified Linux User Management configuration parameters. For a complete list of configurable parameters, refer to Table 5-2 on page 32 .
-k	Specifies that the SSL certificate file is to be imported into the local machine.

Parameter	Description
help paramlist	Lets you view the help strings for the Linux User Management configurable parameters. For a complete list of configurable parameters, refer to Table 5-2 on page 32 .
-w <i>workstation_context</i>	Specifies, in LDAP format, the context where the Workstation object will be created.
-a <i>adminFDN</i>	Specifies, in LDAP format, the administrator's name.
-S <i>servername</i>	Specifies the preferred eDirectory server. The server can be specified in terms of its IP address or host name. This is a mandatory parameter.
-r <i>base_context</i>	Specifies, in LDAP format, the base context of the UNIX/Linux Config object that contains the list of workstations contexts.
-o	Specifies the existing LUM configuration to be overwritten. Be aware that this removes the associated Workstation object and creates it again.
<i>port</i>	Specifies the non-SSL port.
-l <i>sslport</i>	Specifies the SSL port.
cache_refresh	Specifies how frequently user and group entries stored in the persistent cache are to be refreshed from eDirectory. A larger value results in less network traffic and less load on the server, but the cache might reflect stale information if the eDirectory database is modified. The value can range from 1 to 2147483647 seconds.
-R <i>alternative LDAP server</i>	Specifies a comma-separated list of alternative LDAP replica servers. The server can be specified by IP address or host name.

5.1.2 Configuring Failover Mechanism

LUM fails if the LDAP server against which LUM is configured is unavailable. To avoid failure, populate the *alternative-ldap-servers* in */etc/nam.conf* with a list of LDAP Servers where LUM can fall back when the primary LDAP server is down.

Ensure that the LDAP servers are replica servers. Else, the persistent-search feature does not work.

5.1.3 Configuring a Workstation with Linux User Management

To configure a specified workstation with Linux User Management, use the following syntax:

```
namconfig add -a adminFDN -r base_context -w workstation_context [-o] -S servername [:port] [-l sslport] [-R server [:port],server [:port],...]
```

Example:

```
namconfig add -a cn=admin,o=novell -r ou=nam,o=novell -w ou=ws,ou=nam,o=novell -S MYSERVER:389
```

Example (secure LDAP):

```
namconfig add -a cn=admin,o=novell -r ou=lum,o=novell -w ou=ws,ou=nam,o=novell -S MYSERVER:389 -l 636
```

NOTE: At a minimum, you must supply: `adminFDN`, `workstation_context`, `base_context`, and `servername` parameters.

For a description of the command line parameters, refer to [Table 5-1 on page 29](#).

After the configuration, you need to change the `/etc/nsswitch.conf` and PAM configuration files to start the product.

5.1.4 Configuring Linux User Management with LDAP SSL

To configure Linux User Management with SSL, use the following command:

```
namconfig add -a cn=admin,o=novell -r ou=lum,o=novell -w ou=ws,ou=nam,o=novell  
-S MYSERVER:389 -l 636
```

where the emphasized fields match your eDirectory containers, etc.

Configuring Linux User Management to use secure LDAP ensures that the information exchanged between the OES server and eDirectory is securely encrypted.

If you configure Linux User Management for secure LDAP, the configuration utility adds parameters to the `/etc/nam.conf` file: `type-of-authentication=2` and `ldap-ssl-port` parameters.

During the configuration, the server certificate is created in the `/var/lib/novell-lum` directory as a hidden file with a `.der` extension.

All PAM authentication requests are then handled by using secure LDAP.

To get user profile information from eDirectory, `nss_nam` uses a regular LDAP connection.

If the server's SSL certificate expires, it can be re-created by using the `namconfig` utility with the `-k` option. The same certificate file can be used by other applications that want to use secure LDAP for communicating with eDirectory.

5.1.5 Removing Linux User Management Configuration

To remove the Linux User Management configuration, use the following syntax:

```
namconfig rm -a adminFDN
```

Example:

```
namconfig rm -a cn=admin, o=novell
```

For a description of the command line parameters, refer to [Table 5-1 on page 29](#).

NOTE: If you delete or change the name of the container originally passed to `namconfig`, you need to delete `nam.conf` and rerun `namconfig`.

5.1.6 Setting or Getting Linux User Management Configuration Parameters

The `namconfig` utility lets you set values for specific Linux User Management configuration parameters or retrieve these values on the command line. To do so, use the following syntax:

```
namconfig {set valuelist | get paramlist | help paramlist}
```

Example:

```
namconfig set servername=namserver
```

This specifies that the server named `namserver` is to be used as the preferred eDirectory server.

```
namconfig get base-name
```

This displays the current eDirectory context in which Linux User Management is installed.

For a description of the command line parameters, refer to [Table 5-1 on page 29](#).

The following parameters cannot be set:

- ♦ `base-name`
- ♦ `schema`
- ♦ `certificate-file-type`

After Linux User Management is configured under a base name, it should not be moved or renamed. If moving or renaming is required, you must manually edit the `/etc/nam.conf` file.

The type of the eDirectory schema is determined during configuration.

5.1.7 Using `namconfig` to Import an SSL Certificate

To import an SSL certificate in to the local machine, use the following syntax:

```
namconfig -k
```

For a description of the command line parameters, refer to [Table 5-1 on page 29](#).

5.2 Editing the `nam.conf` File

The parameters used for configuring Linux User Management are listed in the `/etc/nam.conf` file. The configuration file is stored in the UTF-8 format.

[Table 5-2](#) contains the list of parameters in `/etc/nam.conf`.

Table 5-2 *Linux User Management Configuration Parameters*

Parameter	Description	Default Value
preferred-server	Specifies the eDirectory LDAP server to be contacted. The value can be host name, alias, DNS name, or IP address. The value is set when you configure Linux User Management.	The default is a null string.

Parameter	Description	Default Value
base-name	Specifies the context in eDirectory where Linux User Management is installed. The value is set when you configure Linux User Management.	The default value is a null string.
num-threads	Specifies the number of worker threads in the cache daemon. The value can range from 1 to 25.	The default is 5.
schema	Indicates whether eDirectory 8.1 or earlier or the RFC 2307 schema is supported.	The default schema is rfc2307.
enable-persistent-cache	Specifies whether a persistent cache is to be maintained on the local workstation to store user and group profiles. Values can be yes or no.	The default value is yes.
user-hash-size	Specifies the hash size for the persistent cache to store user entries. The value should be a prime number greater than or equal to 1/4th of the number of user entries. The value can range from 1 to 9973.	The default is 211.
group-hash-size	Specifies the hash size for persistent cache to store group entries. The value should be a prime number greater than or equal to 1/4th of the number of group entries. The value can range from 1 to 9973.	The default is 211.
persistent-cache-refresh-period	Specifies how frequently user and group entries stored in the persistent cache are to be refreshed from eDirectory. A larger value results in less network traffic and less load on the server, but the cache might reflect stale information if the eDirectory database is modified. The value can range from 1 to 2147483647 seconds.	The default period is 28800 seconds (8 hours).
persistent-cache-refresh-flag	Specifies whether all user and group entries or only those used in the current boot session are to be refreshed. This can take the values all or accessed.	The default is all.
create-home	Creates user home directories. Values can be yes or no.	The default value is yes.
user-context	Specifies the user context to which Linux User objects are to be migrated. This is not used in Linux User Management 2.2.	The default value is ou = Linux-users,<base_name>.
group-context	Specifies the group context to which Linux Group objects are to be migrated. This is not used in Linux User Management 2.2.	The default value is ou = Linux-groups,<base_name>.
type-of-authentication	Specifies the type of authentication, either simple (non-SSL) or SSL-based. Values can be 1 (simple authentication) or 2 (SSL-based authentication).	The default value is 1.
certificate-file-type	Specifies the certificate file format. Two values are possible: der and base64.	The default value is der.
ldap-ssl-port	Specifies the LDAP SSL port.	The default is 636.
ldap-port	Specifies the LDAP connection port.	The default is 389.
admin-fdn	Specifies the LDAP server administrator's name.	The default value is a null string.

Parameter	Description	Default Value
alternative-ldap-server-list	Specifies a comma-separated list of names of replica servers.	The default value is a null string.
support-alias-name	Specifies whether to support alias objects (users/groups) in eDirectory. Values can be yes or no.	The default value is no.
support-outside-base-name	Specifies whether to support objects (users/groups) outside the domain to which NAM is configured. Values can be yes or no. If objects (users/groups) with the same name are present in the local domain, then preference is given to the local domain objects.	The default value is yes.
proxy-user-fdn	Specifies the full distinguished name of the proxy user that performs searches.	This value is optional.
proxy-user-pwd	Specifies the password of the proxy user (proxy-user-fdn).	This value is optional.
case-sensitive	Specifies whether to enforce case sensitive user names.	The default value is no.
cache-only	<p>Specifies whether <code>namcd</code> uses only the cache for information about users and groups.</p> <p>If the information about users and groups is not found in the cache, <code>namcd</code> does not request this information from LDAP.</p> <p>The values can be yes or no.</p>	The default value is no.
persistent-search	<p>Specifies whether <code>namcd</code> uses the LDAP persistent search feature. This feature allows <code>namcd</code> to listen to change events in LDAP related to Posix groups and trigger the cache refresh if the change event is relevant.</p> <p>The values can be yes or no.</p>	The default value is yes.
convert-lowercase	Specifies whether to treat all usernames and groupnames as lowercase names.	The default value is no.

Managing User and Group Objects in eDirectory

6

You can use Novell® iManager in a browser or enter commands at the Linux computer console to manage the standard eDirectory™ objects, such as User objects, Group objects, and Linux User Management objects, including UNIX Config and UNIX Workstation objects. You can also use these methods to create users of Samba technology.

- Section 6.1, “Using Novell iManager to Manage Linux User Management,” on page 35
- Section 6.2, “Using Command Line Utilities to Manage Users and Groups,” on page 46

6.1 Using Novell iManager to Manage Linux User Management

Novell iManager is a management utility that runs in an Internet browser. Linux User Management is installed as part of the Open Enterprise Server installation.

- Section 6.1.1, “Running iManager,” on page 35
- Section 6.1.2, “Creating a New Group Object for Linux User Management Users,” on page 35
- Section 6.1.3, “Enabling an Existing Group Object for Linux User Management,” on page 36
- Section 6.1.4, “Creating a User Object for Linux User Management,” on page 39
- Section 6.1.5, “Enabling an Existing User Object for Linux User Management,” on page 40
- Section 6.1.6, “Modifying a UNIX Config Object,” on page 43
- Section 6.1.7, “Modifying a UNIX Workstation Object,” on page 44
- Section 6.1.8, “Enabling an Existing User Object for Samba,” on page 45

6.1.1 Running iManager

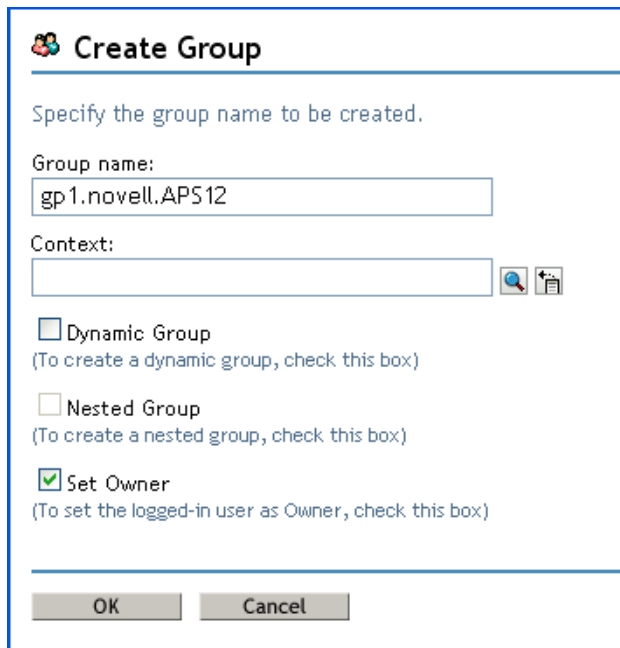
- 1 Open an Internet browser.
- 2 Enter the domain name or IP address of the server followed by `/nps/`. For example, if the server address is 10.10.1.1, specify the address as `http://10.10.1.1/nps/`
- 3 When prompted, provide the administrator name and password.
- 4 Click *Linux User Management*.

If you do not see the Linux User Management category of *Roles and Tasks*, the Linux User Management plug-in to iManager is not installed. You can download the Linux User Management plug-in for iManager from the [Novell Download Web site](http://download.novell.com/index.jsp). (<http://download.novell.com/index.jsp>)

6.1.2 Creating a New Group Object for Linux User Management Users

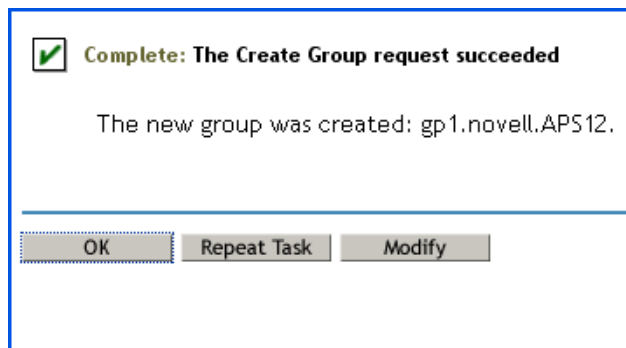
- 1 Launch iManager.

- 2 In *Roles and Tasks*, select *Groups > Create Group*.
- 3 On the Create Group page, specify the Group name and the Context for the group.
- 4 Select the group type.
 - ♦ Select *Dynamic Group* to make the new group a dynamic group, of the dynamic Group class. Otherwise, the group is created as a static group, or as the Group class.
 - ♦ Select *Nested Group* to make the new group a nested group so that the group is created with the auxiliary class *nestedGroupAux*.
 - ♦ Select *Set Owner* to make the creator of a group object the group owner. The group's Owner attribute is set to the DN of iManager's logged-in user. Deselect *Set Owner* to leave the Owner attribute undefined.



The 'Create Group' dialog box is shown. It has a title bar with a group icon and the text 'Create Group'. Below the title bar, it says 'Specify the group name to be created.' There are two input fields: 'Group name:' with the text 'gp1.novell.APS12' and 'Context:' which is empty. To the right of the 'Context:' field are two icons: a magnifying glass and a document with an arrow. Below the input fields are three checkboxes: 'Dynamic Group' (unchecked), 'Nested Group' (unchecked), and 'Set Owner' (checked). Each checkbox has a descriptive text below it: '(To create a dynamic group, check this box)', '(To create a nested group, check this box)', and '(To set the logged-in user as Owner, check this box)' respectively. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

- 5 Click *OK*. A message confirming that a new group object is successfully created is displayed.



The 'Complete: The Create Group request succeeded' message box is shown. It has a title bar with a green checkmark icon and the text 'Complete: The Create Group request succeeded'. Below the title bar, it says 'The new group was created: gp1.novell.APS12.' At the bottom of the message box are three buttons: 'OK', 'Repeat Task', and 'Modify'.

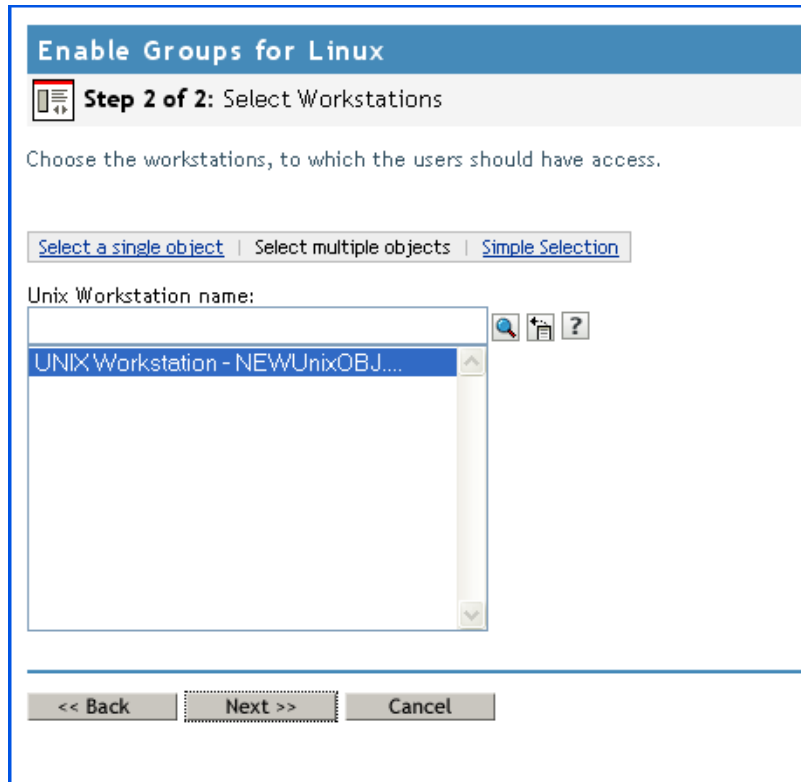
6.1.3 Enabling an Existing Group Object for Linux User Management

- 1 Launch iManager.

- 2 In *Roles and Tasks*, select *Linux User Management > Enable Groups for Linux*.
- 3 Select a group to be enabled for Linux User Management.
- 4 (Optional) Select *Linux-enable all users in these Groups* to enable all the users in the group for Linux User Management.

The screenshot shows a wizard window titled "Enable Groups for Linux". The subtitle is "Step 1 of 2: Select Groups". Below the subtitle, there is explanatory text: "Before an eDirectory group can be used with Linux, it must be enabled with Linux User Management. After you enable the group, a Linux Profile tab is available in Groups -> Modify Group." Below this text are three tabs: "Select a single object" (which is selected), "Select multiple objects", and "Simple Selection". A "Group name:" label is followed by a list box containing "LUMGroup1.novell", which is currently selected. To the right of the list box are three icons: a magnifying glass, a document with an arrow, and a question mark. Below the list box is a checkbox labeled "Linux-enable all users in these Groups", which is checked. At the bottom of the window are three buttons: "<< Back", "Next >>", and "Cancel".

- 5 Click *Next*.
- 6 Select a UNIX workstation to which the user has access.



- 7 Click *Next*.
- 8 Select a primary group to which the user belongs. You can select:
 - ♦ An existing eDirectory group.
 - ♦ An existing Linux-enabled group.
 - ♦ Create a new group. If you want to create a new group, specify a name and context for the group.
- 9 Click *Next*.
- 10 Select an UNIX workstation to which the user has access.
- 11 Click *Next*. A summary of the selected object and workstation is displayed.

Enable Groups for Linux

Summary

Currently Linux-Enabled

Group
LUMGroup1.novell

Workstation Access

User
UNIX Workstation - NEWUnixOBJ.novell

12 Click *Finish*.

6.1.4 Creating a User Object for Linux User Management

- 1 Launch iManager.
- 2 In *Roles and Tasks*, select *User > Create User*.

Novell iManager

Roles and Tasks

[All Categories]

Move Group

Rename Group

View My Groups

Help Desk

Kerberos Management

LDAP

Linux User Management

NMAS

Novell Certificate Access

Novell Certificate Server

Partitions and Replicas

Proxy Manager

Rights

Schema

SecureLogin SSO

SNMP

Users

Create User

Delete User

Disable Account

Enable Account

Modify User

Move User

Create User

Username: *

First name:

Last name: *

Full name:

Context: *

Password:

Retype password:

Note: Failure to enter a password will allow the user to login without a password.

☐ Set simple password

Note: Simple password is required for native file access for Windows and Macintosh users. (Not required when Universal password is enabled)

☐ Copy from template or user object

☐ Create home directory

Volume:

Path:

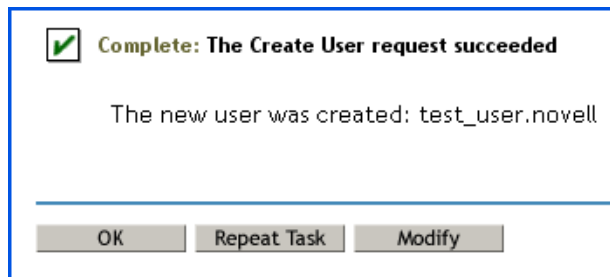
Note: Please enter an existing path where the user directory will be created.

- 3 On the Create User page, provide the username, first name, last name, full name, context, and password for the user object.

If you fail to specify a password, you are prompted to either allow the user to log in without a password, which is not recommended, or require a password for login.

Select *Set simple password* to define a simple password, which is required for native file access for Windows and Macintosh* users. It is not necessary when Universal Password is enabled.

- 4 Select *Copy from template or user object* to create a user based on an existing template or user object. When copying from a user object, iManager allows only a copy of the new object's eDirectory rights instead of a copy of all eDirectory rights, to prevent users from receiving the same rights as the administrator.
- 5 Select *Create home directory* to specify a location for the user's home directory, which is created when the user object is created. If you specify a path that doesn't exist, a message appears stating that the user's home directory has not been created.
- 6 (Optional) Add more details such as title, location, department, telephone, facsimile number, e-mail address, and a description.
- 7 Click *OK*. A message confirming that a new user object is created is displayed.



6.1.5 Enabling an Existing User Object for Linux User Management

Before an eDirectory user can be used with Linux, it must be enabled with Linux User Management.

- 1 Launch iManager.
- 2 In *Roles and Tasks*, select *Linux user Manager > Enable Users for Linux*.

Enable Users for Linux

Step 1 of 3: Select Users

Before an eDirectory user can be used with Linux, it must be enabled with Linux User Management.
After you enable the user, a Linux Profile tab is available in Users -> Modify User.
You may find users to Linux-enable by selecting the users or a group, to which they belong.

[Select a single object](#) | [Select multiple objects](#) | [Simple Selection](#)

Object name: [\(see list\)](#)

<< Back

Next >>

Cancel

3 Specify the users to be enabled.

You might be prompted to confirm if you want to enable users in the group for Linux User Management.

4 Click *Next*.

5 Select an primary group to which the Linux user belongs. You have three options:

- ♦ Select An Existing eDirectory Group
- ♦ Select An Existing Linux-Enabled Group
- ♦ Create a New Linux-enabled Group. If you choose this option, specify the group name and the context.

Enable Users for Linux

Step 2 of 3: Select Primary Group

Every Linux user must belong to a primary group.

Please select a primary group

☒

An Existing eDirectory Group. This group will be Linux-Enabled.

☐

An Existing Linux-Enabled Group

☐

Create a New Linux-Enabled Group

Group Name

Context

<< Back

Next >>

Cancel

- 6 Click *Next*.
- 7 Select a UNIX workstation to which the user has access.

Enable Users for Linux

Step 3 of 3: Select Workstations

Choose the workstations, to which the users should have access.

[Select a single object](#) |
 [Select multiple objects](#) |
 [Simple Selection](#)

Unix Workstation name:

<< Back

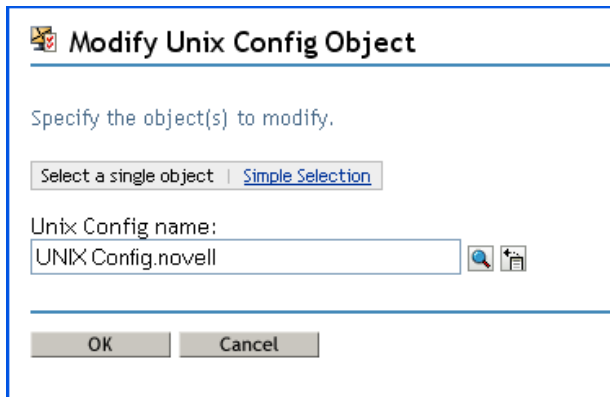
Next >>

Cancel

- 8 Click *Next*. A summary of the users who enabled for Linux is displayed.
- 9 Click *Finish*.


6.1.6 Modifying a UNIX Config Object

- 1 Launch iManager.
- 2 In *Roles and Tasks*, select *Linux User Management > Modify Unix Config Object*.
- 3 Specify the name of the object to modify.



The screenshot shows a dialog box titled "Modify Unix Config Object". Inside the dialog, there is a text prompt "Specify the object(s) to modify." followed by a button labeled "Select a single object" and a link labeled "Simple Selection". Below this, there is a text field labeled "Unix Config name:" containing the text "UNIX Config.novell". To the right of the text field are two small icons: a magnifying glass and a document icon. At the bottom of the dialog are two buttons: "OK" and "Cancel".

- 4 Click *OK*.
- 5 Make required configuration changes.



Modify Unix Config Object:  UNIX Config.novell

Linux Profile
Configuration

The information on this page is generally for tracking purposes. Before modifying any fields, be sure to click the question mark (?) icon and read the help file.

Workstation Contexts:
 novell

Description:

uamPosixGidNumberStart: 0	uamPosixUidNumberStart: 0
uamPosixGidNumberEnd: 65535	uamPosixUidNumberEnd: 65535
Last Assigned Group ID: 615	Last Assigned User ID: 602
<input type="checkbox"/> Reuse Group ID:	<input type="checkbox"/> Reuse User ID:
Group ID Deleted Map: 	User ID Deleted Map: 

OK Cancel Apply

- 6 Click *Apply* to apply the changes.
- 7 Click *OK* to save and exit.

6.1.7 Modifying a UNIX Workstation Object

- 1 Launch iManager.
- 2 In *Roles and Tasks*, select *Linux User Management > Modify Unix Workstation Object*.
- 3 Specify the name of the object to modify.

Modify Unix Workstation Object

Specify the object(s) to modify.

Select a single object | [Simple Selection](#)

Unix Workstation name:
 UNIX Workstation - NEWUnixOBJ.novell

OK Cancel

- 4 Click *OK*.
- 5 Make the required changes.
- 6 Click *OK*.

6.1.8 Enabling an Existing User Object for Samba

- 1 Click *Create Samba User*.
- 2 Specify the username of the Linux User Management user to enable for Samba.
- 3 Click *OK*.
- 4 Read the confirmation message and click *OK*.
- 5 Specify the requested information.

By using *Add* and *Remove*, you can add a new group or remove an existing group.

Click *LUM Enabled Services* to view a list of the LUM-enabled services on the UNIX workstation object.

Modify Unix Workstation Object: UNIX Workstation - NEWUnixOBJ.novell

Linux Profile

Groups | LUM Enabled Services

The following groups are associated with the selected UNIX Workstation object. Use the checkboxes and controls to add or remove LUM-enabled groups from this UNIX Workstation.

Groups with access to LUM-enabled Services

Add... | Remove 2 Item(s)

<input type="checkbox"/>	Name
<input type="checkbox"/>	pg0005.novell
<input type="checkbox"/>	pg0008.novell

OK Cancel Apply

6 Click *Apply* to apply your changes.

7 Click *OK* to save and exit.

6.2 Using Command Line Utilities to Manage Users and Groups

Command line utilities let you create, modify, delete, and list both user and group accounts. This section describes these utilities and explains their usage. It also describes how you can assign Linux attributes to objects by using Novell iManager.

- ♦ [Section 6.2.1, “Security Considerations,” on page 46](#)
- ♦ [Section 6.2.2, “nambulkadd,” on page 47](#)
- ♦ [Section 6.2.3, “namuseradd,” on page 49](#)
- ♦ [Section 6.2.4, “namgroupadd,” on page 51](#)
- ♦ [Section 6.2.5, “namusermod,” on page 52](#)
- ♦ [Section 6.2.6, “namgroupmod,” on page 53](#)
- ♦ [Section 6.2.7, “namuserdel,” on page 54](#)
- ♦ [Section 6.2.8, “namgroupdel,” on page 55](#)
- ♦ [Section 6.2.9, “namuserlist,” on page 56](#)
- ♦ [Section 6.2.10, “namgrouplist,” on page 56](#)

NOTE: The command line utilities read the necessary input parameters from the `/var/nam/namutilities.inp` configuration file `/var/nam/namutils.inp` if the parameters are not specified in the command line. If it is not present, this file is created by the utilities and uses system default values such as account expiry time, admin FDN, and the default Group object to which users are associated. The context under which User and Group objects is added is also set when any of the commands listed in the section are executed.

However, `namuserlist` and `namgrouplist` do not create this file. Refer to the following sections for more details.

6.2.1 Security Considerations

The `nambulkadd` command involves authentication to eDirectory as the Admin user. If your interaction with the server can be viewed by others, you must set an environment variable with the Admin password rather than specifying the password on a command line.

To set the required environment variable,

- 1 As `root`, enter the following at the shell prompt:

```
export LUM_PWD=AdminPassword
```

where *AdminPassword* is the password of the eDirectory Admin user.

6.2.2 nambulkadd

The nambulkadd utility is used to do the following:

- ♦ Create new groups that are enabled for Linux User Management.
- ♦ Enable existing eDirectory groups for Linux User Management.
- ♦ Enable existing eDirectory users for Linux User Management-enabled users.
- ♦ Enable existing eDirectory users for Linux User Management.

The nambulkadd utility was primarily designed to be used when copying data to an NSS volume on an OES for Linux server by using the Server Consolidation and Migration Toolkit, which helps you create the configuration files used by nambulkadd based on input from administrators at the time they run the utility.

For more information, see the *Novell Server Consolidation and Migration Toolkit Administration Guide*. (<http://www.novell.com/documentation/scmt/scmt12/index.html?page=/documentation/scmt/scmt12/data/hz8pck9v.html>)

- ♦ “Syntax” on page 47
- ♦ “Parameters” on page 47
- ♦ “Defaults” on page 48
- ♦ “Example” on page 48
- ♦ “Creating Customized Text Files for nambulkadd” on page 48
- ♦ “Considerations to Keep in Mind” on page 49

Syntax

The syntax of the nambulkadd command is as follows:

```
nambulkadd [-a adminFDN] [-w admin_password] [-u /path/userlistfile] [-g /path/grouplistfile]
```

Parameters

Table 6-1 nambulkadd Parameters

Parameter	Description
-a	Specify the fully distinguished name of the eDirectory administrator.
-w	Specify the password for eDirectory Admin user. (Optional) See “Security Considerations” on page 46.
-u	Specify the path and name of the userlist.txt file located in /sys/scu/lum on the Linux server. This file is created by the Server Consolidation utility as documented in the <i>Novell Server Consolidation and Migration Toolkit Administration Guide</i> . (http://www.novell.com/documentation/scmt/scmt12/index.html?page=/documentation/scmt/scmt12/data/hz8pck9v.html).

Parameter	Description
-g	Specify the path and name of the <code>grouplist.txt</code> file located in <code>/sys/scu/lum</code> on the Linux server. This file is created by the Server Consolidation utility as documented in the Novell Server Consolidation and Migration Toolkit Administration Guide . (http://www.novell.com/documentation/scmt/scmt12/index.html?page=/documentation/scmt/scmt12/data/hz8pck9v.html).

Defaults

There are no default values associated with this utility.

Example

```
nambulkadd -a cn=admin,o=novell -u /sys/scu/lum/job1-userlist.txt -g /sys/scu/lum/job1-grouplist.txt
```

This enables Linux User Management for all the Group objects listed in `job1-grouplist.txt` and all the User objects listed in `job1-userlist.txt`.

Creating Customized Text Files for nambulkadd

Normally, the `nambulkadd` command processes text files created by the Novell Server Consolidation utility. However, you can create customized files to bulk-enable system users and groups.

- 1 Using your favorite Linux text editor, create a text file for the eDirectory groups you want to enable for Linux User Management.

These can be either new groups you want to create or existing groups that have not been enabled for Linux User Management.

IMPORTANT: Do not use Windows editors to modify the list.

If your custom list or the list generated by the Server Consolidation utility is edited with a Windows editor such as Notepad, Wordpad, or OpenOffice, it adds an `^M` or `x0D` at the end of every line. If you run `nambulkadd` with a list edited and saved with one of these editors, it creates a new Linux User Management user with `x0D` in the username. Most utilities such as ConsoleOne® do not recognize the `x0D` at the end of the username, so it appears as a duplicate user object.

If Windows editors were previously used to edit the list, you need to run the DOS to UNIX cleanup utility to remove the `^M` or `x0D` character in the userlist.

- 2 On the first line in the file, include all the parameters you would normally use in connection with one instance of the `namgroupadd` command to create a group enabled for Linux User Management.

For example, if your system doesn't currently contain the eDirectory object `Group1.sales.example`, and the first line contains

```
-x ou=sales,o=example -W LinuxSrvr1 Group1
```

then when you run `nambulkadd`, the following occurs:

- ♦ `Group1` is created as a group enabled for Linux User Management in `sales.example`.

- ♦ Group1.sales.example is added to the members list of the LinuxSrvr1 UNIX Workstation object that already exists in the tree.
 - ♦ LinuxSrvr1 is added to the workstation list of the newly created Group1.sales.example group.
- 3** After creating a line in the file for each group you want to enable for Linux User Management, create a second file to contain information for the users you want to enable for Linux User Management.
- As with the group text file, the users in this file can be either new users that you want to create or existing users that have not been enabled for Linux User Management.
- 4** On the first line in the file, include all the parameters you would normally use in connection with one instance of the `namgroupadd` command to create a Linux User Management-enabled user.
- For example, if your system doesn't currently contain the eDirectory object John.sales.example, and the first line contains
- ```
-x ou=sales,o=example -g cn=Group1,ou=sales,o=example John
```
- then when you run `nambulkadd`, the following occurs:
- ♦ John is created as a Linux User Management-enabled user in sales.example.
  - ♦ John is added to the members list of the Linux User Management-enabled group Group1.sales.example.
- 5** After creating a line in the userlist file for each user you want to enable for Linux User Management, save the file and run the utility by using the syntax specified in [“Syntax” on page 47](#).

## Considerations to Keep in Mind

The `nambulkadd` utility is designed specifically for Linux User Management-enabling User and Group objects. Keep the following points in mind as you plan to use the utility.

- ♦ If a Group or User object already exists, then the object is Linux User Management-enabled and added to the appropriate member lists.
- ♦ If the Group or User objects are already Linux User Management-enabled, the operation fails. The `nambulkadd` utility is only designed to enable groups and users for Linux User Management and cannot be used to make other modifications after that enabling task is completed.
- ♦ The groups specified in the userlist text file must have been previously Linux User Management-enabled, or they must be included in the grouplist text file processed during the same `nambulkadd` session.

### 6.2.3 namuseradd

The `namuseradd` utility is used to create a Linux User object in eDirectory with the attributes you specify on the command line. If a User object with the same name already exists under the specified eDirectory context, `namuseradd` checks whether the user is a Linux user or an eDirectory user. If the user is a Linux user, a message indicates that a Linux user with the same name already exists.

## Syntax

The syntax of the `namuseradd` utility is as follows:

```
namuseradd [-a adminFDN] [-w bindpasswd] [-x user_context] [-c comment] [-d
directory] [-e expiry_date] [-g primary_groupFDN] [-G groupFDN] [-G
groupFDN]... [-m [-k skeldir]] [-n] [-s shell] [-D] [-P] [-p passwd] [-u uid] [-o]]
user_name
```

## Parameters

**Table 6-2** *namuseradd Parameters*

| Parameter | Description                                                                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -a        | Specify the fully distinguished name of the eDirectory administrator.                                                                                                     |
| -w        | Specify the password for simple authentication.                                                                                                                           |
| -x        | Specify the fully distinguished eDirectory context in which the User object is to be added.                                                                               |
| -c        | Any text string; generally a short description of the user login.                                                                                                         |
| -d        | Specify the home directory for the user. If used with the <b>-D</b> option, this is used as the default home directory prefix while creating logins.                      |
| -e        | Specify the expiry date after which no user can access this contact. Use the mm/dd/yy format.                                                                             |
| -g        | Specify the full eDirectory context of the primary group of the user.                                                                                                     |
| -G        | Specify the full eDirectory context of the secondary group to which the user belongs. Multiple groups can be specified by using the <b>-G</b> option multiple times.      |
| -m        | Create the home directory on the local machine.                                                                                                                           |
| -k        | A directory that contains skeleton information, such as user profile information, that can be copied into a new user's home directory. This directory must already exist. |
| -n        | Disallow upgrading a NetWare® user if a NetWare user with the same name already exists.                                                                                   |
| -s        | Specify the full pathname of the program used as the login shell for the user.                                                                                            |
| -D        | Set the default values in the <code>/var/nam/namutils.inp</code> file.                                                                                                    |
| -P        | Check for the uniqueness of the specified name at the domain root before adding the User object.                                                                          |
| -p        | Assign the specified password to the user while adding the User object.                                                                                                   |
| -u        | Specify a unique User ID for the user.                                                                                                                                    |
| -o        | Allow the specified User ID to be duplicated (non-unique).                                                                                                                |
|           | Specify the login name or User ID of the user you are creating.                                                                                                           |

## Defaults

The following default values are taken from the `/var/nam/namutils.inp` file, if they are not specified at the command line:

- ♦ **adminFDN:** Taken from the value provided with the `-a` option.
- ♦ **expiry\_date:** Taken from the value provided with the `-e` option.
- ♦ **directory:** Taken from the value provided with the `-d` option.
- ♦ **shell:** Taken from the value provided with the `-s` option.

## Examples

```
namuseradd -a cn=admin,o=novell -x ou=lum,o=novell - g
cn=other,ou=linux_groups,o=novell Dave
```

This adds a user, Dave, to the eDirectory context `ou=lum,o=novell` which has the primary group of `other`.

## 6.2.4 namgroupadd

The `namgroupadd` utility is used to create a Linux Group object in eDirectory, with the attributes you specify on the command line. If a Group object with the same name already exists under the specified eDirectory context, `namgroupadd` checks whether the group is a Linux group or a NetWare group. By default, if the group is a NetWare group, `namgroupadd` upgrades the group to a Linux group, unless otherwise specified in the parameter `-n`. If the group is a Linux group, a message indicates that a Linux group with the same name already exists.

## Syntax

The syntax of the `namgroupadd` utility is as follows:

```
namgroupadd [-a adminFDN] [-w bindpasswd] [-x group_context] [-A | -W
workstation_name [,workstation_name...]] [-g gid[-o]] [-P] [-n] group_name
```

## Parameters

**Table 6-3** *namgroupadd Parameters*

| Parameter | Description                                                                                                                                                                    |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -a        | Specify the fully distinguished name of the eDirectory administrator.                                                                                                          |
| -w        | Specify the password for simple authentication.                                                                                                                                |
| -x        | Specify the fully distinguished eDirectory context in which the Group object is to be added.                                                                                   |
| -A        | Include all workstations in the workstation list of the group.                                                                                                                 |
| -W        | Specify a comma-separated list of Workstation objects to be added to the workstation list of the group. The group is also added to the members list of the Workstation object. |
| -g        | Specify the Group ID for the group.                                                                                                                                            |

| Parameter | Description                                                                                       |
|-----------|---------------------------------------------------------------------------------------------------|
| -o        | Allow the specified Group ID to be duplicated (non-unique).                                       |
| -P        | Check for the uniqueness of the specified name at the domain root before adding the Group object. |
| -n        | Disallow upgrading a NetWare group if a NetWare group with the same name already exists.          |
|           | Specify the fully distinguished name of the group. This is a mandatory parameter.                 |

## Defaults

The following default value is taken from the `/var/nam/namutils.inp` file, if it is not specified at the command line:

```
adminFDN
```

## Examples

```
namgroupadd -W garfield -g 110 grp1
```

This adds a group named `grp1` to a workstation named `garfield` and assigns it the group ID 110.

```
namgroupadd -P -x ou=nam,o=novell -A grp2
```

This adds a group named `grp2` to the specified eDirectory context, after first checking that the group does not already exist under the partition root.

## 6.2.5 namusermod

The `namusermod` utility is used to modify a Linux user's login in eDirectory. It changes the definition of the specified login and updates all the login-related system files appropriately.

### Syntax

The syntax of the `namusermod` utility is as follows:

```
namusermod [-a adminFDN] [-w bindpasswd] [-c comment] [-d directory] [-e
expiry_date] [-p passwd] [-g primary_groupFDN] [-G groupFDN [-G groupFDN]...] [-D
groupFDN [-D groupFDN]...] [-u uid [-o]] [-s shell] userFDN
```

### Parameters

**Table 6-4** *namusermod Parameters*

| Parameter | Description                                                           |
|-----------|-----------------------------------------------------------------------|
| -a        | Specify the fully distinguished name of the eDirectory administrator. |
| -w        | Specify the password for simple authentication.                       |
| -c        | Any text string, generally a short description of the user login.     |

| Parameter | Description                                                                                                                                                                           |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -d        | Specify the home directory for the user. If used with the parameter <b>-D</b> , this is taken as the default home directory prefix while creating logins.                             |
| -e        | Specify the expiration date after which no user can access this account. Use the mm/dd/yy format.                                                                                     |
| -p        | Assign the specified password to the user while adding the User object.                                                                                                               |
| -g        | Specify the full eDirectory context of the primary group of the user.                                                                                                                 |
| -G        | Specify the full eDirectory context of the secondary group to which the user belongs. Multiple groups can be specified by using the -G option multiple times.                         |
| -D        | Specify the full eDirectory context of the secondary group to which the user belongs. Multiple groups can be specified by using the -G option multiple times.                         |
| -u        | Specify a unique User ID for the user.                                                                                                                                                |
| -o        | Allow the specified User ID to be duplicated (non-unique).                                                                                                                            |
| -s        | Specify the full pathname of the program used as the login shell for the user.<br><br>Specify the user's fully distinguished name (FDN) in eDirectory. This is a mandatory parameter. |

## Defaults

The following default value is taken from the `/var/nam/namutils.inp` file, if it is not specified at the command line:

```
adminFDN
```

## Examples

```
namusermod -g cn=hrd,ou=Linux_groups,o=novell -G cn=grp2,ou=nam,o=novell
cn=John,ou=unixuser,o=novell
```

This replaces the existing primary group of a user named John with a group named hrd whose fully distinguished eDirectory context is provided; it also adds John to another group named grp2.

## 6.2.6 namgroupmod

The `namgroupmod` utility is used to modify the attributes of a Linux Group object in eDirectory.

### Syntax

The syntax of the `namgroupmod` utility is as follows:

```
namgroupmod [-a adminFDN] [-w bindpasswd] [-W workstation_name [-W
workstation_name]...] [-d workstation_name] [-P] [-g gid] [-o] [-n name] groupFDN
```

## Parameters

**Table 6-5** *namgroupmod Parameters*

| Parameter | Description                                                                                                                                                                                                                                                                                 |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -a        | Specify the fully distinguished name of the eDirectory administrator.                                                                                                                                                                                                                       |
| -w        | Specify the password for simple authentication.                                                                                                                                                                                                                                             |
| -W        | Specify the name of the Workstation object to be added to the workstation list of the group. The group is also added to the members list of the Workstation object. Multiple workstations can be specified by using the -W option multiple times.                                           |
| -d        | Specify the fully distinguished eDirectory context of the Workstation object to be deleted from the workstation list of the group. The group is also deleted from the members list of the Workstation object. Multiple workstations can be specified by using the -d option multiple times. |
| -P        | Check for the uniqueness of the specified name at the domain root before modifying the Group object.                                                                                                                                                                                        |
| -g        | Specify the Group ID for the group.                                                                                                                                                                                                                                                         |
| -o        | Allow the specified Group ID to be duplicated (non-unique).                                                                                                                                                                                                                                 |
| -n        | Change the CommonName of the Linux Group object in eDirectory.<br><br>Specify the fully distinguished name of the group. This is a mandatory parameter.                                                                                                                                     |

## Defaults

The following default values are taken from the `/var/nam/namutils.inp` file, if they are not specified at the command line:

`adminFDN`

## Examples

```
namgroupmod -W linux10 -d garfield cn=grp1,ou=nam,o=novell
```

This adds a group named `grp1` to a workstation named `linux10` and also removes it from the workstation named `garfield`.

## 6.2.7 namuserdel

The `namuserdel` utility deletes a Linux user's login from eDirectory and updates all the login-related system files appropriately.

### Syntax

The syntax of the `namuserdel` utility is as follows:

```
namuserdel [-a adminFDN] [-w bindpasswd] [-r] userFDN
```

## Parameters

**Table 6-6** *namuserdel Parameters*

| Parameter | Description                                                           |
|-----------|-----------------------------------------------------------------------|
| -a        | Specify the fully distinguished name of the eDirectory administrator. |
| -w        | Specify the password for simple authentication.                       |
| -r        | Remove the user's home directory from the system.                     |

## Defaults

The following default values are taken from the `/var/nam/namutils.inp` file, if it is not specified at the command line:

```
adminFDN
```

## Examples

```
namuserdel cn=usr1,ou=nam,o=novell
```

This deletes the user named `usr1` from eDirectory.

## 6.2.8 namgroupdel

The `namgroupdel` utility deletes a Linux Group object from eDirectory and updates all the login-related system files appropriately.

## Syntax

The syntax of the `namgroupdel` utility is as follows:

```
namgroupdel [-a adminFDN] [-w bindpasswd] groupFDN
```

## Parameters

**Table 6-7** *namgroupdel Parameters*

| Parameter | Description                                                                                     |
|-----------|-------------------------------------------------------------------------------------------------|
| -a        | Specify the fully distinguished name of the eDirectory administrator.                           |
| -w        | Specify the password for simple authentication.                                                 |
|           | Specify the fully distinguished name of the group to be deleted. This is a mandatory parameter. |

## Defaults

The following default value is taken from the `/var/nam/namutils.inp` file, if it is not specified at the command line:

- ♦ adminFDN

## Examples

```
namgroupdel cn=grp1,ou=nam,o=novell
```

This removes the group named `grp1`.

## 6.2.9 namuserlist

The `namuserlist` utility lists the attributes of Linux User objects in eDirectory in `/etc/passwd` format. If you do not specify the user context, the attributes of all users in the current workstation are listed.

### Syntax

The syntax of the `namuserlist` utility is as follows:

```
namuserlist {-x user_context : user_name}
```

### Parameters

**Table 6-8** *namuserlist Parameters*

| Parameter | Description                                                                                                                 |
|-----------|-----------------------------------------------------------------------------------------------------------------------------|
| -x        | Specify the fully distinguished eDirectory context of the user. Specify the user's login name and CommonName in eDirectory. |

### Examples

```
namuserlist usr1
```

This displays the attributes of the user named `usr1`.

## 6.2.10 namgroupelist

The `namgroupelist` utility lists some of the attributes of Linux Group objects in eDirectory. Use iManager to see all of the attributes, including the UNIX Workstation objects associated with the Group.

### Syntax

The syntax of the `namgroupelist` utility is as follows:

```
namgroupelist{-x group_context : group_name}
```



## Parameters

**Table 6-9** *namgroup*list Parameters

| Parameter | Description                                                      |
|-----------|------------------------------------------------------------------|
| -x        | Specify the fully distinguished eDirectory context of the group. |
|           | Specify the fully distinguished name of the group.               |

## Examples

```
namgroup
```

list grp1

This lists the attributes of a group named grp1.



This section addresses issues you might encounter when working with Linux User Management technologies.

- ♦ [Section 7.1, “Troubleshooting Linux User Management,” on page 59](#)
- ♦ [Section 7.2, “Making Home Directories Private,” on page 62](#)
- ♦ [Section 7.3, “Troubleshooting Account Redirection Problems,” on page 62](#)
- ♦ [Section 7.4, “Changing the Name of the Original Container Passed to namconfig,” on page 62](#)

## 7.1 Troubleshooting Linux User Management

The following sections provide information about troubleshooting Linux User Management:

- ♦ [Section 7.1.1, “Linux User Management Returns Invalid UID and GID for Users and Groups,” on page 59](#)
- ♦ [Section 7.1.2, “namconfig Fails,” on page 60](#)
- ♦ [Section 7.1.3, “named Indicates That a Certificate Is Not Found,” on page 60](#)
- ♦ [Section 7.1.4, “Duplication of UIDs and GIDs,” on page 60](#)
- ♦ [Section 7.1.5, “A User Cannot Log In,” on page 60](#)
- ♦ [Section 7.1.6, “Password Expiration Information for the User Is Not Available,” on page 60](#)
- ♦ [Section 7.1.7, “ID Command Not Giving the Desired Results,” on page 61](#)
- ♦ [Section 7.1.8, “named Not Coming Up after a System Reboot,” on page 61](#)
- ♦ [Section 7.1.9, “Log Files for Linux User Management,” on page 61](#)
- ♦ [Section 7.1.10, “Missing Mandatory Attribute Error When Adding a User to a Linux User Management Group,” on page 61](#)
- ♦ [Section 7.1.11, “SUSE Linux Enterprise Desktops Configured as UNIX Workstation Objects,” on page 62](#)

### 7.1.1 Linux User Management Returns Invalid UID and GID for Users and Groups

Linux User Management returns invalid UID and GID for user and groups because of an incorrect schema mapping in LDAP Group Object.

To resolve,

- 1 Log in to iManager.
- 2 In Roles and Tasks, click *LDAP > LDAP Options*.
- 3 Browse to *Attribute Map* tab.
- 4 Change the mapping of UID (eDirectory attribute) to UniqueID (LDAP attribute).
- 5 Change the mapping of UID NDS attribute to the UniqueID LDAP attribute.

---

**NOTE:** Remove any mapping present for LDAP attribute uidNumber and gidNumber

---

- 6 Click *Apply* to save the changes.
- 7 Click *OK* to exit.

## 7.1.2 namconfig Fails

When Linux User Management is configured on a workstation, the base-name is specified in the `nam.conf` file. If Linux User Management is reconfigured with a new partition root without removing the existing configuration, the `namconfig` command fails with an error indicating Specified partition root and Partition root in the NDS configuration files doesn't match.

To resolve this issue, delete `nam.conf` and re-run `namconfig`.

## 7.1.3 namcd Indicates That a Certificate Is Not Found

When you start Linux User Management, in some scenarios, `namcd` displays an error indicating that a certificate is not found.

Linux User Management requires a server certificate to do SSL authentication to the LDAP server. A server certificate file for SSL authentication must be present in the `/var/lib/novell-lum/.preferred_server-name.filetype` directory where `.preferred_server-name.filetype` is the certificate file of the preferred server. If this file is deleted or is corrupt, import it by using `namconfig -k`.

## 7.1.4 Duplication of UIDs and GIDs

In a name-mapped Domain Services for Windows (DSfW) tree, if the tree is already enabled for Linux User Management and the UNIX config object is placed in a custom location other than the admin user context, YaST might not be able to find the UNIX config object. When this happens, it adds a new UNIX config object under `ou=novell, $domain`, which causes duplication of UIDs and GIDs.

To avoid this, change the range of the UIDs and GIDs in one of the UNIX config objects in the tree.

## 7.1.5 A User Cannot Log In

- ♦ If it takes more than 60 seconds to log in, the login utility times out. This is a limitation of Linux operating systems.

## 7.1.6 Password Expiration Information for the User Is Not Available

The `pam_nam` account management module should always be stacked only after the `pam_nam` authentication module. If it is stacked directly after any other module, the behavior of `pam_nam` might be unpredictable. You might not be able to extract the user's password and account expiration, or other authentication details.

### 7.1.7 ID Command Not Giving the Desired Results

If the ID command or the `getent` command is not displaying the desired result, one of the reasons might be that the entries are cached by `nscd` (name service caching daemon).

If you have changed the `/etc/nsswitch.conf` file, the `/etc/passwd` file, or the `/etc/group` file stop and restart `nscd` by using the following commands.

```
/etc/init.d/nscd stop

/etc/init.d/nscd start
```

### 7.1.8 namcd Not Coming Up after a System Reboot

If Linux User Management is configured against eDirectory in the same system, and the system is rebooted, `namcd` tries to bind to the LDAP server while the system is coming up. If the LDAP server (eDirectory) takes more than one minute to come up, `namcd` tries to contact the alternative LDAP servers, if any.

If replica servers do not exist or do not respond, `namcd` does not come up and must be restarted manually. This is also applicable for scenarios where eDirectory and `namcd` are started simultaneously or within a very short time.

The LDAP server startup status is logged into the `ndsd.log` file present in the server's `var` directory.

### 7.1.9 Log Files for Linux User Management

See the `/var/lib/novell-lum/nam.log` file for more details on the functioning of the corresponding components.

See the `/var/log/YaST/y2log` file for information on how `namconfig` is called by the installation program.

See the `/var/log/messages` file for runtime log information.

### 7.1.10 Missing Mandatory Attribute Error When Adding a User to a Linux User Management Group

If you are installing OES into an existing NDS8 tree and the new OES server doesn't contain an eDirectory replica, you might get a Missing Mandatory Attribute error when enabling an existing user for Linux User Management existing user in iManager.

In most cases you can modify the user at the command line by using the `nameusermod` command. If the command line utility doesn't work, you need to add a replica to the server. For more information, see *Adding Replicas* in the *Managing Partitions and Replicas* section of the [Novell eDirectory 8.8 Administration Guide](http://www.novell.com/documentation/edir88/) (<http://www.novell.com/documentation/edir88/>).

### 7.1.11 SUSE Linux Enterprise Desktops Configured as UNIX Workstation Objects

Although computers running SUSE® Linux Enterprise Desktop 10 can be configured as Workstation objects, their Linux User Management services might not appear when viewed in iManager. The services do not appear because the software infrastructure required for server management (OpenWBEM) is not automatically installed as part of SUSE Linux Enterprise Desktop.

## 7.2 Making Home Directories Private

During the Open Enterprise Server 2 installation, the Linux User Management page lets you decide whether to set the system umask so that all users can see all the directories and files in the `/home` directory.

On an already-installed system, you can modify the umask setting so that directories and files are visible only to their owners.

- 1 Access a shell prompt as the `root` user.
- 2 Open `/etc/login.defs` with an editor.
- 3 Change the umask value to 0077.
- 4 Save the file.

Directories and files are now only visible to their owners (and the root user, of course). If you want to restore the default settings, change the umask value to 0022.

---

**NOTE:** Changing the umask affects directories and files created after the change, but does not affect permissions on existing directories. Existing directories must be changed manually.

---

## 7.3 Troubleshooting Account Redirection Problems

- Because Account Management's name service switch provider, `nss_nam`, relies on the `namcd` daemon to query eDirectory, ensure that the `namcd` daemon is up and running.
- If the `/etc/nam.conf` file is changed, `namcd` should be stopped and restarted.
- `namcd` gets values from eDirectory, depending on the frequency specified for the cache-refresh period. If changes are made to existing User, Group, Linux Config, and Linux Workstation objects, `namcd` gets the values only after the interval specified for the cache-refresh period. Setting large values for this parameter increases cache hit rates and reduces mean response time, but increases problems with cache coherence.

---

**TIP:** To refresh the cache immediately, run `namconfig cache_refresh`.

---

## 7.4 Changing the Name of the Original Container Passed to namconfig

If you delete or change the name of the container originally passed to `namconfig`, you need to delete `nam.conf` and rerun `namconfig`.

When Linux User Management is configured on a workstation, the base-name field is specified in the `nam.conf` file. If the container that the base-name field references is deleted from the server or its name changed, the following problems result:

- ♦ Users enabled for Linux User Management are no longer able to access the assigned server.
- ♦ When a Workstation object is reconfigured by using the *YaST > Linux User Management* module, an error results stating that the configuration module is unable to connect to LDAP because the server or the specified user does not have rights to configure Linux User Management.

Deleting `nam.conf` and rerunning `namconfig` should fix the problems.





- ♦ Section 8.1, “Linux User Management Configuration for Domain Services for Windows,” on page 65
- ♦ Section 8.2, “Allocating User IDs and Group IDs,” on page 65
- ♦ Section 8.3, “RFC 2307 Schema Extension,” on page 65
- ♦ Section 8.4, “Running Linux User Management in a Virtualization Environment,” on page 66
- ♦ Section 8.5, “Configuring Linux User Management for Novell Cluster Services,” on page 66
- ♦ Section 8.6, “Security Considerations for Linux User Management,” on page 66
- ♦ Section 8.7, “Usernames for Linux User Management Users,” on page 66

## 8.1 Linux User Management Configuration for Domain Services for Windows

In Domain Services for Windows, when you install Linux User Management with a container admin, you must give read, write, and compare attribute rights on the UNIX Config object. You must give the rights if object is located in a container where the Admin does not have these rights.

If the UNIX Config object does not exist and you are creating it in a container where the user does not have rights, you must give the user read, write, and compare rights to the container where you want to create the object.

---

**TIP:** To reduce security risks, you can remove the rights to the container after the install and set them on UNIX Config object after it is created.

---

## 8.2 Allocating User IDs and Group IDs

In a DSfW tree or in a DSfW domain in a legacy tree, all the users are Linux User Management users. However, you can notice the following differences:

The pool of UID's and GIDs are different for DSfW and Linux User Management in a legacy tree.

In DSfW, the UIDs and GIDs are allocated from the rIDSet object. In a legacy eDirectory tree in which Linux User Management is configured, the UIDs and GIDs are allocated from the UNIX Config object.

## 8.3 RFC 2307 Schema Extension

In a DSfW environment, the RFC 2307 schema extension is extended by default.

## 8.4 Running Linux User Management in a Virtualization Environment

There are no documented issues related to running Linux User Management in a virtualization environment. Linux User Management runs in a virtualized environment just as it does on physical computers and requires no special configuration or other changes.

For information on virtualization, see [Novell Virtualization Technology \(http://www.novell.com/documentation/vmserver\)](http://www.novell.com/documentation/vmserver).

## 8.5 Configuring Linux User Management for Novell Cluster Services

There are no documented issues related to running Linux User Management and Novell Cluster Services™. Linux User Management runs in a cluster with no special configuration changes.

## 8.6 Security Considerations for Linux User Management

There are no documented security issues related to Linux User Management; however, you should review your security strategies to make sure that access rights and permissions are in compliance.

## 8.7 Usernames for Linux User Management Users

Although there is no need to enter a user's full context name when logging in through Linux User Management, there might be issues if two user IDs in eDirectory have the same username, even if the usernames are in different contexts.