

Planning and Implementation Guide

Novell® Open Enterprise Server

2 SP1

July 31, 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	15
1 What's New	17
1.1 New in OES 2 SP1	17
1.1.1 Links to What's New Sections	17
1.1.2 Other New Features and Changes	19
1.2 New in OES 2 (Initial Release)	21
1.2.1 Dynamic Storage Technology	21
1.2.2 OES 2 Migration Tools	21
1.2.3 Xen Virtualization Technology	21
2 Welcome to Open Enterprise Server 2	23
3 Planning Your OES 2 Implementation	25
3.1 What Services Are Included in OES 2?	25
3.2 Which Services Do I Need?	32
3.3 Exploring OES 2 services	33
3.4 Which OES 2 Platform Is Best for My Services?	33
3.5 Plan for eDirectory	33
3.6 Prepare Your Existing eDirectory Tree for OES 2	34
3.7 Identify a Purpose for Each Server	34
3.8 Understand Server Requirements	35
3.9 Understand User Restrictions and Linux User Management	35
3.10 Caveats to Consider Before You Install	35
3.10.1 AFP File Locking Requires Samba	36
3.10.2 Adding a Linux Node to a Cluster Ends Adding More NetWare Nodes	36
3.10.3 Do Not Create Local (POSIX) Users	36
3.10.4 Samba Enabling Disables SSH Access	36
3.10.5 Cluster Upgrades Must Be Planned Before Installing OES 2	37
3.10.6 Follow the Instructions for Your Chosen Platforms	37
3.10.7 iFolder 3.7 Considerations	37
3.10.8 Installing into an Existing eDirectory Tree	38
3.10.9 NetWare License Placement in the Tree	39
3.10.10 NetWare Licenses and OES 2 Linux Trees	39
3.10.11 NetWare 6.5 Servers Must Be Running SP3 or Later	39
3.10.12 If You've Ever Had OES 1 Linux Servers with LUM and NSS Installed	40
3.10.13 Novell Distributed Print Services Cannot Migrate to Linux	43
3.10.14 NSS Caveats	43
3.10.15 Unsupported Service Combinations	43
3.11 Consider Coexistence and Migration Issues	46
3.12 Understand Your Installation Options	47
3.12.1 OES 2 Linux Installation Overview	47
3.12.2 OES 2 NetWare Installation Overview	48

3.12.3	About Your Installation Options	49
3.12.4	Use Predefined Server Types (Patterns) When Possible	50
3.12.5	If You Want to Install in a Lab First	51
3.12.6	If You Want to Install NSS on a Single-Drive Linux Server	51
3.13	eGuide, IFolder 2, and Virtual Office Are Still Available on Netware	51
4	Getting and Preparing OES 2 Software	53
4.1	Do You Have Upgrade Protection?	53
4.2	Do You Want 32-Bit or 64-Bit OES Linux?	53
4.3	Do You Want to Purchase OES 2 or Evaluate It?	54
4.4	Evaluating OES 2 Software	54
4.4.1	Understanding OES 2 Software Evaluation Basics	55
4.4.2	Downloading OES 2 SP1 Software from the Novell Web Site	55
4.4.3	Preparing the Installation Media	56
4.4.4	Installing OES 2 for Evaluation Purposes	57
4.4.5	Evaluating OES 2	57
4.4.6	Installing Purchased Activation Codes after the Evaluation Period Expires	58
4.5	Licensing	58
4.5.1	The OES 2 Licensing Model	58
4.5.2	Licensing Services on OES 2 NetWare	58
4.5.3	OES 2 Linux Doesn't Support NLS	59
4.5.4	Configuring and Administering Licensing Services	59
5	Installing OES 2	61
5.1	Installing OES 2 Linux	61
5.1.1	What's Next	62
5.2	Installing OES 2 NetWare	62
5.2.1	What's Next	62
5.3	Installing OES 2 Servers in a Xen VM	62
6	Caveats for Implementing OES 2 Services	63
6.1	Avoiding POSIX and eDirectory Duplications	63
6.1.1	The Problem	63
6.1.2	Three Examples	64
6.1.3	Avoiding Duplication	65
6.2	ConsoleOne Can Cause JClient Errors	65
6.3	CUPS on OES 2 Linux	66
6.4	eDirectory	66
6.4.1	Avoid Uninstalling eDirectory	66
6.4.2	Avoid Renaming Trees and Containers	66
6.4.3	One Instance Only	66
6.4.4	Default Static Cache Limit Might Be Inadequate	67
6.4.5	Special Characters in Usernames and Passwords	67
6.5	iManager 2.7	67
6.6	IFolder 3.7	68
6.7	iPrint	68
6.7.1	Cluster Failover Between Mixed Platforms Not Supported	68

6.7.2	Printer Driver Uploading on OES 2 Linux Might Require a CUPS Administrator Credential	69
6.7.3	Printer Driver Uploading Support	69
6.7.4	iManager Plug-Ins Are Platform-Specific	69
6.7.5	iPrint Client for Linux Doesn't Install Automatically	69
6.7.6	iPrint Disables CUPS Printing on the OES 2 Linux Server	69
6.8	NCP Server (OES 2 Linux)	69
6.9	NSS (OES 2 Linux)	70
6.10	OpenLDAP on OES 2 Linux	70
6.11	Samba	70
6.12	Virtualization Issues	70
6.12.1	eDirectory Fails to Start Automatically	71
6.12.2	NSS Considerations	71
6.12.3	Always Use Timesync Rather Than NTP	71
6.13	Web Services	71
7	Upgrading to OES 2	73
7.1	Caveats to Consider Before Upgrading	73
7.1.1	About Previously Installed Packages (RPMs)	73
7.1.2	iManager 2.5 Replaced by iManager 2.7 on NetWare	73
7.1.3	OES 1 Linux to OES 2 Linux Service Differences	73
7.1.4	Only One eDirectory Instance Is Supported on OES Servers	74
7.1.5	Virtual Office from NetWare 6.5 to OES 2 NetWare	74
7.2	OES 2 SP1 Linux Upgrade Paths	74
7.3	OES 2 SP1 NetWare Upgrade Paths	74
8	Migrating and Consolidating Existing Servers and Data	77
8.1	Supported OES 2 SP1 Migration Paths	77
8.2	Migration Tools and Purposes	77
8.2.1	OES 2 SP1 Migration Tool	77
8.2.2	Migrate Windows Shares Utility	77
8.2.3	NetWare Migration Wizard	78
8.2.4	Server Consolidation Utility	78
9	Virtualization in OES 2	79
9.1	Graphical Overview of Virtualization in OES 2	79
9.2	Why Install OES Services on Your VM Host?	80
9.3	Services Supported on VM Hosts and Guests	80
10	Clustering and High Availability	83
11	Managing OES 2	85
11.1	Overview of Management Interfaces and Services	85
11.2	Using OES 2 Welcome Pages	86
11.2.1	The Welcome Site Requires JavaScript, Apache, and Tomcat	86
11.2.2	Accessing the Welcome Web Site	87

11.2.3	The Welcome Web Site Is Available to All Users	87
11.2.4	Administrative Access from the Welcome Web Site	87
11.3	OES Utilities and Tools	87
11.4	SSH Services on OES 2 Linux	100
11.4.1	Overview	100
11.4.2	Setting Up SSH Access for LUM-enabled eDirectory Users	102
12	Network Services	105
12.1	TCP/IP	105
12.1.1	Coexistence and Migration Issues	105
12.2	DNS and DHCP	106
12.2.1	DNS Differences Between NetWare and OES 2 Linux	106
12.2.2	DHCP Differences Between NetWare and OES 2 Linux	107
12.3	Time Services	108
12.3.1	Overview of Time Synchronization	108
12.3.2	Planning for Time Synchronization	112
12.3.3	Coexistence and Migration of Time Synchronization Services	115
12.3.4	Implementing Time Synchronization	117
12.3.5	Configuring and Administering Time Synchronization	118
12.3.6	Daylight Saving Time	119
12.4	Discovery Services (SLP, WinSock, Etc.)	119
12.4.1	Novell SLP and OpenSLP	120
12.4.2	WinSock and Discovery (NetWare only)	120
12.4.3	UDDI and Discovery	120
12.4.4	CIMOM and Discovery	120
12.5	SLP	120
12.5.1	Why SLP Is Needed	121
12.5.2	Comparing Each Platform's SLP Solution	121
12.5.3	Setting Up OpenSLP on OES 2 Networks	122
12.5.4	Using Novell SLP on OES 2 Networks	126
13	Storage and File Systems	129
13.1	Overview of OES 2 Storage	129
13.1.1	Databases	129
13.1.2	iSCSI	130
13.1.3	File System Support in OES	130
13.1.4	Storage Basics by Platform	132
13.1.5	Storage Options	132
13.1.6	NetWare Core Protocol Support (Novell Client Support) on Linux	134
13.2	Planning OES File Storage	134
13.2.1	Directory Structures	135
13.2.2	File Service Support Considerations	135
13.2.3	General Requirements for Data Storage	135
13.2.4	OES 2 Linux Storage Planning Considerations	135
13.2.5	NSS Planning Considerations	140
13.3	Coexistence and Migration of Storage Services	141
13.3.1	MySQL	141
13.3.2	OES 2 Linux Options	141

13.3.3	OES 2 NetWare Options	142
13.4	Initial Setup Is Required for NetWare.	143
13.5	Configuring and Maintaining Storage.	143
13.5.1	Managing Directories and Files	143
13.5.2	Managing NSS.	143
13.5.3	Optimizing Storage Performance.	145
13.5.4	Disk Management on NetWare	145
14	eDirectory, LDAP, and Domain Services for Windows	147
14.1	Overview of Directory Services	147
14.2	eDirectory	148
14.2.1	Installing and Managing eDirectory on OES	148
14.2.2	Planning Your eDirectory Tree	149
14.2.3	eDirectory Coexistence and Migration.	149
14.3	LDAP (eDirectory)	149
14.3.1	Overview of eDirectory LDAP Services	150
14.3.2	Planning eDirectory LDAP Services	150
14.3.3	Migration of eDirectory LDAP Services	150
14.3.4	eDirectory LDAP Implementation Suggestions	150
14.4	Domain Services for Windows	150
14.4.1	Graphical Overview of DSfW	151
14.4.2	Planning Your DSfW Implementation	154
14.4.3	Implementing DSfW on Your Network.	154
15	Users and Groups	157
15.1	Creating Users and Groups	157
15.2	Linux User Management: Access to Linux for eDirectory Users	157
15.2.1	Overview	158
15.2.2	Planning.	163
15.2.3	Coexistence and Migration	164
15.2.4	LUM Implementation Suggestions.	164
15.3	Identity Management Services.	166
15.4	Using the Identity Manager 3.5 Bundle Edition	167
15.4.1	What Am I Entitled to Use?	167
15.4.2	System Requirements	168
15.4.3	Installation Considerations.	168
15.4.4	Getting Started.	168
15.4.5	Activating the Bundle Edition.	168
15.4.6	Frequently Asked Questions about Activation.	169
16	Access Control and Authentication	173
16.1	Controlling Access to Services.	173
16.1.1	Overview of Access Control.	173
16.1.2	Planning for Service Access	180
16.1.3	Coexistence and Migration of Access Services.	183
16.1.4	Access Implementation Suggestions.	184
16.1.5	Configuring and Administering Access to Services	184

16.2	Authentication Services	186
16.2.1	Overview of Authentication Services	186
16.2.2	Planning for Authentication	189
16.2.3	Authentication Coexistence and Migration	189
16.2.4	Configuring and Administering Authentication	189
17	File Services	191
17.1	Overview of File Services	191
17.1.1	Using the File Services Overviews	192
17.1.2	FTP Services	192
17.1.3	Native File Access Protocols	192
17.1.4	NetWare Core Protocol	193
17.1.5	NetStorage	194
17.1.6	Novell AFP	199
17.1.7	Novell CIFS	200
17.1.8	Novell iFolder 3.7	201
17.1.9	Novell Samba	203
17.2	Planning for File Services	204
17.2.1	Deciding Which Components Match Your Needs	204
17.2.2	Comparing Your CIFS File Service Options	206
17.2.3	Planning Your File Services	207
17.3	Coexistence and Migration of File Services	208
17.3.1	Novell Client (NCP)	209
17.3.2	Native File Access Protocols	209
17.3.3	NetStorage	209
17.3.4	Novell AFP	209
17.3.5	Novell CIFS	210
17.3.6	Novell iFolder 3.7	210
17.3.7	Samba	210
17.4	Aligning NCP and POSIX File Access Rights	210
17.4.1	Managing Access Rights	211
17.4.2	Providing a Private Work Directory	212
17.4.3	Providing a Group Work Area	212
17.4.4	Providing a Public Work Area	213
17.4.5	Setting Up Rights Inheritance	213
17.5	Native File Access Protocols Implementation and Maintenance	213
17.6	NCP Implementation and Maintenance	214
17.6.1	NCP Services on NetWare	214
17.6.2	Novell NCP Server for Linux	214
17.6.3	Assigning File Trustee Rights	215
17.6.4	NCP Maintenance	215
17.7	NetStorage Implementation and Maintenance	215
17.7.1	About Automatic Access and Storage Locations	216
17.7.2	About SSH Storage Locations	216
17.7.3	Novell iFolder 2 Doesn't Use Storage Locations	216
17.7.4	Assigning User and Group Access Rights	217
17.7.5	Authenticating to Access Other Target Systems	217
17.7.6	NetStorage Authentication Is Not Persistent by Default	217
17.7.7	NetStorage Maintenance	218

17.8	Novell AFP Implementation and Maintenance	218
17.8.1	Implementing Novell AFP File Services	218
17.8.2	Maintaining Novell AFP File Services	218
17.9	Novell CIFS Implementation and Maintenance	218
17.9.1	Implementing Novell CIFS File Services	219
17.9.2	Maintaining Novell CIFS File Services	219
17.10	Novell iFolder 3.7 Implementation and Maintenance	219
17.10.1	Managing Novell iFolder 3.7	219
17.10.2	Configuring Novell iFolder 3.7 Servers	219
17.10.3	Creating and Enabling Novell iFolder 3.7 Users	219
17.10.4	Novell iFolder 3.7 Maintenance	220
17.11	Samba Implementation and Maintenance	220
17.11.1	Implementing Samba File Services	220
17.11.2	Maintaining Samba File Services	220
18	Print Services	221
18.1	Overview of Print Services	221
18.1.1	Using This Overview	221
18.1.2	iPrint Components	222
18.1.3	iPrint Functionality	222
18.2	Planning for Print Services	224
18.3	Coexistence and Migration of Print Services	224
18.4	Print Services Implementation Suggestions	224
18.4.1	Initial Setup	225
18.4.2	Implementation Caveats	226
18.4.3	Other Implementation Tasks	226
18.5	Print Services Maintenance Suggestions	226
19	Search Engine (QuickFinder)	227
20	Web Services	229
21	Security	231
21.1	Overview of OES Security Services	231
21.1.1	Application Security (AppArmor)	231
21.1.2	Auditing	231
21.1.3	Encryption (NICI)	231
21.1.4	General Security Issues	232
21.2	Planning for Security	232
21.2.1	Comparing the Linux and the NetWare Core Protocol (NCP) File Security Models	233
21.2.2	User Restrictions: Some OES 2 Linux Limitations	234
21.3	Configuring and Administering Security	235
21.4	Links to Product Security Considerations	235
22	Certificate Management	237
22.1	Overview	237
22.1.1	SLES Default Certificates	237

22.1.2	OES 2 Certificate Management	238
22.1.3	Multiple Trees Sharing a Common Root	240
22.2	Setting Up Certificate Management	240
22.2.1	Setting Up Automatic Certificate Maintenance	240
22.2.2	Eliminating Browser Certificate Errors	240
22.3	If You Don't Want to Use eDirectory Certificates	242
A	Adding Services to OES 2 Servers	245
B	Changing an OES 2 Linux Server's IP Address	247
B.1	Caveats and Disclaimers	247
B.2	Prerequisites	247
B.2.1	General	247
B.2.2	iPrint	248
B.2.3	Clustering	248
B.3	Changing the Server's Address Configuration	248
B.4	Reconfiguring the OES Services	248
B.5	Repairing the eDirectory Certificates	249
B.6	Completing the Server Reconfiguration	249
B.6.1	QuickFinder	250
B.6.2	DHCP	250
B.6.3	iPrint	250
B.6.4	NetStorage	250
B.7	Modifying a Cluster	251
B.8	Reconfiguring Services on Other Servers That Point to This Server	251
C	Updating/Patching OES 2 Servers	253
D	Backup Services	255
D.1	Services for End Users	255
D.2	System-Wide Services	255
D.2.1	Novell Storage Management Services (SMS)	255
D.2.2	SLES 10 Backup Services	256
E	Quick Reference to OES 2 User Services	257
F	OES 2 SP1 Browser Support	259
G	Client/Workstation OS Support	261
H	OES 2 Linux Service Scripts	263
I	System User and Group Management in OES 2 SP1	267
I.1	About System Users and Groups	267
I.1.1	Types of OES System Users and Groups	267
I.1.2	OES System Users and Groups by Name	268

I.2	Understanding Proxy Users	269
I.2.1	What Are Proxy Users?	269
I.2.2	Why Are Proxy Users Needed on OES Linux?	270
I.2.3	Which Services Require Proxy Users and Why?	270
I.2.4	What Rights Do Proxy Users Have?	271
I.3	Planning Your Proxy Users	274
I.3.1	About Proxy User Creation	274
I.3.2	Proxy User Impacts on User Connection Licenses	277
I.3.3	Limiting the Number of Proxy Users in Your Tree	277
I.3.4	Proxy Users and Passwords	279
I.4	Implementing Your Proxy User Plan	281
I.4.1	Tree-wide proxy users	281
I.4.2	Service-specific proxy users	282
I.4.3	Partition-wide proxy users	282
I.4.4	Server-wide proxy user	282
I.4.5	Individual proxy user per-server-per-service	282
I.5	Proxy Users and Domain Services for Windows	282
I.6	System Users	282
I.7	System Groups	284
J	Administrative Users in OES 2 SP1	287
K	Documentation Updates	289

About This Guide

Purpose

This guide provides:

- ♦ Planning and implementation instructions
- ♦ Service overviews
- ♦ Links to detailed information in other service-specific guides.

Audience

This guide is designed to help network administrators

- ♦ Understand Open Enterprise Server 2 services prior to installing them.
- ♦ Make pre-installation planning decisions.
- ♦ Understand installation options for each platform.
- ♦ Implement the services after they are installed.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with OES 2. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

Changes to this guide are summarized in a Documentation Updates appendix at the end of this guide. The lack of such an appendix indicates that no changes have been made since the initial product release.

Additional Documentation

The *OES2 SP2: Lab Guide for Linux and Virtualized NetWare* is the hands-on counterpart to this guide and helps network administrators:

- ♦ Set up a basic lab with an OES 2 Linux server, a virtualized NetWare® server, a test tree, and user objects that represent the different types of users in OES 2.
- ♦ Use the exercises in the guide to explore how OES 2 services work.
- ♦ Continue exploring to gain a sound understanding of how OES 2 can benefit their organization.

Additional documentation is also found on the [OES 2 Documentation Web site \(http://www.novell.com/documentation/oes2\)](http://www.novell.com/documentation/oes2).

Documentation Conventions

The terms OES 2 and OES 2 SP1 are both used in this guide. Generally, OES 2 SP1 is used to differentiate something that is new or changed for the SP1 release of OES 2. Unless otherwise indicated, all statements that refer to OES 2 also apply to OES 2 SP1.

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

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

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

What's New

This section summarizes the new features for each release of Novell® Open Enterprise Server (OES) 2.

- ♦ [Section 1.1, “New in OES 2 SP1,” on page 17](#)
- ♦ [Section 1.2, “New in OES 2 \(Initial Release\),” on page 21](#)

1.1 New in OES 2 SP1

- ♦ [Section 1.1.1, “Links to What's New Sections,” on page 17](#)
- ♦ [Section 1.1.2, “Other New Features and Changes,” on page 19](#)

1.1.1 Links to What's New Sections

The following table provides links to the What's New sections in the documentation for all OES 2 products.

Table 1-1 *What's New*

Product	Link to What's New Section
Archive and Version Services 2.1	Linux Administration Guide NetWare Administration Guide User Guide
DHCP	Linux Administration Guide
Distributed File Services	Administration Guide
DNS	Linux Administration Guide
Domain Services for Windows	Administration Guide
Dynamic Storage Technology	Administration Guide
Identity Manager 3.6	Getting Started Guide (http://www.novell.com/documentation/idm36/idm_install/data/be115dw.html)
iManager 2.7	Administration Guide
Installation	Linux Installation Guide NetWare Installation Guide
iPrint	Linux Administration Guide NetWare Administration Guide
Licensing (NetWare)	Administration Guide
Migration Tool	Administration Guide

Product	Link to What's New Section
Native File Access Protocols	Administration Guide
NCP Server for OES 2 Linux	Administration Guide
NetStorage	Linux Administration Guide NetWare Administration Guide
Novell AFP	Administration Guide Comparing the NetWare and Linux Solutions
Novell CIFS	Administration Guide Comparing the NetWare and Linux Solutions
Novell Client™	Linux Windows XP/2003 Administration Guide Windows Vista* Administration Guide
Novell Cluster Services™ (High Availability)	Administration Guide
Novell iFolder® 3.7	Administration Guide User Guide
Novell Remote Manager	Linux Administration Guide NetWare Administration Guide
Novell Storage Services (NSS)	Administration Guide
Nsure® Audit	Administration Guide
OES 2 Linux	Installation Guide
OES 2 NetWare	Memory Management Administration Guide Server OS Administration Guide
OpenWBEM	Administration Guide
QuickFinder™ 5	Administration Guide
RConsoleJ (NetWare)	Administration Guide
Samba (Linux)	Administration Guide
Server Health Monitoring	This is now available in various Novell Remote Manager dialog boxes on both platforms. For more information, see “Health Monitoring Services” on page 90.
Shadow Volumes	See “Overview of Dynamic Storage Technology” in the <i>OES 2 SP1: Dynamic Storage Technology Administration Guide</i> .
Storage Management Services (SMS)	Administration Guide
Virtualization (Xen*)	Virtualization Overview

1.1.2 Other New Features and Changes

- ♦ “YaST Install Changes” on page 19
- ♦ “Novell AFP” on page 19
- ♦ “Novell CIFS” on page 20
- ♦ “Novell Domain Services for Windows” on page 20
- ♦ “Migration Tool” on page 20

YaST Install Changes

The default behavior of the option to use eDirectory™ certificates for HTTPS services has changed in OES 2 SP1.

In OES 2, eDirectory certificates were only used by default if you were installing a new server.

In OES 2 SP1, eDirectory certificates are used by default in all installation and upgrade scenarios, except when you are upgrading to SP1 from OES 2. For an upgrade, the option that you selected for the initial installation is retained.

For a brief summary of what happens in each scenario, see [Table 22-2 on page 242](#).

Novell AFP

Novell® AFP is now available on the Linux platform to provide feature parity with NetWare®.

- ♦ Support for AFP v3.1 and AFP v3.2, providing network file services for Mac* OS X* and classic Mac OS workstations
- ♦ Support for Universal Password greater than 8 characters
- ♦ Integration with Novell eDirectory
- ♦ Integration with the Novell Storage Services™ (NSS) file system
- ♦ Support for Unicode* filenames
- ♦ Integration with the Novell Trustee Model for file access
- ♦ Support for regular eDirectory users (no LUM required)
- ♦ Cross-protocol file locking with NCP™

Novell AFP also offers the following features not available for NetWare:

- ♦ **DHX authentication mechanism:** Provides a secure way to transport passwords of up to 64 characters to the server.
- ♦ **Management:** You can use iManager to administer and configure the AFP server on OES 2 Linux. iManager support for AFP on NetWare is unchanged and includes only starting and stopping the server.
- ♦ **Auditing:** You can audit the AFP server to check on the authentication process and any changes that occur to the configuration parameters of the server.

For more information, see the [OES 2 SP1: Novell AFP For Linux Administration Guide](#).

Novell CIFS

Novell CIFS is now available on Linux to provide feature parity with the existing NetWare release. It offers the following features:

- ♦ Support for Windows* 2000, XP, 2003, and Windows Vista* 32-bit
- ♦ Support for Universal Password greater than 8 characters
- ♦ Support for NTLMv1 authentication mode
- ♦ Integration with Novell eDirectory
- ♦ Integration with the Novell Storage Services (NSS) file system
- ♦ Support for Unicode filenames
- ♦ Integration with the Novell Trustee Model for file access
- ♦ Support for regular eDirectory users (no LUM required)
- ♦ Cross-protocol file locking is planned for a future release

For more information, see the *OES 2 SP1: Novell CIFS for Linux Administration Guide*.

Novell Domain Services for Windows

This service creates seamless cross-authentication capabilities between Microsoft* Active Directory* on Windows servers and Novell eDirectory on OES 2 SP1 Linux servers, and offers the following functionality:

- ♦ Administrators with Windows networking environments can set up one or more “virtual” Active Directory domains in an eDirectory tree.
- ♦ Administrators can manage users and groups through MMC or iManager.
- ♦ eDirectory users can authenticate to the virtual domain from a Windows workstation without the Novell Client™ for Windows being installed.
- ♦ eDirectory users can also access file services on
 - ♦ Novell Storage Services (NSS) volumes on Linux servers by using Samba shares.
 - ♦ NTFS files on Windows servers that use CIFS shares.
 - ♦ Shares in trusted Active Directory forests.

For more information, see the *OES 2 SP1: Domain Services for Windows Administration Guide*.

Migration Tool

The new OES 2 SP1 Migration Tool uses a plug-in architecture and comprises multiple Linux command line utilities and a GUI wrapper.

The Migration Tool supports:

- ♦ A single, enhanced GUI interface for migrating all OES services
- ♦ Service migrations from either a single source server or multiple source servers (consolidation) to a target server.
- ♦ Transfer ID (server ID swap) migrations—transferring the services and identity from one server to another server.

For more information, see the *OES 2 SP1: Migration Tool Administration Guide*.

1.2 New in OES 2 (Initial Release)

Novell Open Enterprise Server 2 included the following major features and enhancements that were not included in OES 1. All features are retained in SP1 unless otherwise noted in [Section 1.1, “New in OES 2 SP1,” on page 17](#).

- ♦ [Section 1.2.1, “Dynamic Storage Technology,” on page 21](#)
- ♦ [Section 1.2.2, “OES 2 Migration Tools,” on page 21](#)
- ♦ [Section 1.2.3, “Xen Virtualization Technology,” on page 21](#)

1.2.1 Dynamic Storage Technology

OES 2 introduces Novell Dynamic Storage Technology, a unique storage solution that lets you combine a primary file tree and a shadow file tree so that they appear to NCP and Samba/CIFS users as one file tree. The primary and shadow trees can be located on different file systems, different servers, or even different types of storage.

This lets you manage storage costs in new and efficient ways that were not previously possible.

For more information, see the related sections in [Chapter 13, “Storage and File Systems,” on page 129](#) and the *OES 2 SP1: Dynamic Storage Technology Administration Guide*.

1.2.2 OES 2 Migration Tools

In addition to the legacy Server Consolidation and Migration Toolkit, OES 2 includes new migration tools for migrating data and services from NetWare to OES 2 Linux.

For more information, see [Chapter 8, “Migrating and Consolidating Existing Servers and Data,” on page 77](#).

1.2.3 Xen Virtualization Technology

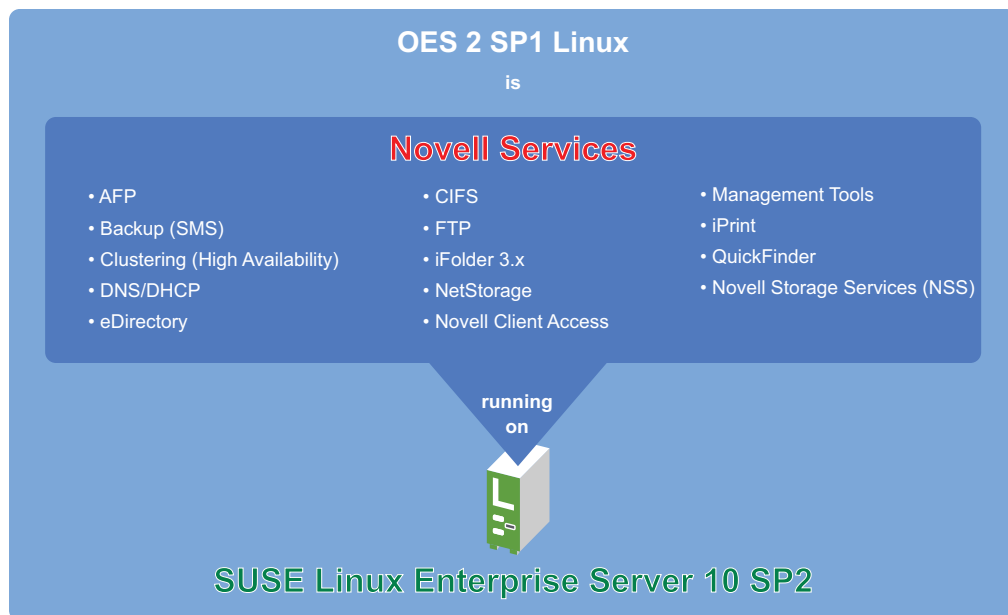
Both OES 2 Linux and OES 2 NetWare can run in virtual machines on either an OES 2 Linux or a SUSE® Linux Enterprise Server 10 SP1 or later server. This is especially valuable to those organizations that are deploying new hardware that doesn’t run NetWare as a physical installation.

For more information, see [Chapter 9, “Virtualization in OES 2,” on page 79](#).

Welcome to Open Enterprise Server 2

Novell® Open Enterprise Server 2 (OES 2) includes all the network services that organizations traditionally expect from Novell.

Figure 2-1 OES 2 Overview



NOTE: For a list of OES 2 services by platform, see [Table 3-1, “Service Comparison Between NetWare 6.5 SP8 and OES 2 SP1 Linux,”](#) on page 25.

Planning Your OES 2 Implementation

As you plan which services to install on which Open Enterprise Server platform, you probably have a number of questions. The following sections are designed to help answer your questions and alert you to the steps you should follow for a successful OES implementation.

- Section 3.1, “What Services Are Included in OES 2?,” on page 25
- Section 3.2, “Which Services Do I Need?,” on page 32
- Section 3.3, “Exploring OES 2 services,” on page 33
- Section 3.4, “Which OES 2 Platform Is Best for My Services?,” on page 33
- Section 3.5, “Plan for eDirectory,” on page 33
- Section 3.6, “Prepare Your Existing eDirectory Tree for OES 2,” on page 34
- Section 3.7, “Identify a Purpose for Each Server,” on page 34
- Section 3.8, “Understand Server Requirements,” on page 35
- Section 3.9, “Understand User Restrictions and Linux User Management,” on page 35
- Section 3.10, “Caveats to Consider Before You Install,” on page 35
- Section 3.11, “Consider Coexistence and Migration Issues,” on page 46
- Section 3.12, “Understand Your Installation Options,” on page 47
- Section 3.13, “eGuide, IFolder 2, and Virtual Office Are Still Available on Netware,” on page 51

3.1 What Services Are Included in OES 2?

Table 3-1 summarizes the services and technology support available on each platform and the differences in the way these services are provided.

Although extensive, this list is not exhaustive. If you are interested in a service or technology not listed, or for documentation for listed services, see the [OES Documentation Web site \(http://www.novell.com/documentation/oes2\)](http://www.novell.com/documentation/oes2).

Table 3-1 *Service Comparison Between NetWare 6.5 SP8 and OES 2 SP1 Linux*

Service	NetWare 6.5 SP8	OES 2 Linux	Platform Differences / Migration Issues
Access Control Lists	Yes	Yes	In combination with NCP™ Server, Linux supports the Novell® trustee model for file access on NSS volumes and NCP volumes on Linux.
AFP (Apple® File Protocol)	Yes - NFAP	Yes - Novell AFP	AFP services on NetWare and OES Linux are proprietary and tightly integrated with eDirectory™ and Novell Storage Services (NSS).

Service	NetWare 6.5 SP8	OES 2 Linux	Platform Differences / Migration Issues
Apache Web Server	Yes - NetWare® port of open source product	Yes - Standard Linux	<p>Administration Instance vs. Public Instance on NetWare (http://www.novell.com/documentation/oes2/web_apache_nw/data/aipcu6x.html#aipcu6x).</p> <p>What's Different about Apache on NetWare (http://www.novell.com/documentation/oes2/web_apache_nw/data/ail8hvj.html) .</p>
Archive and Version Services (Novell)	Yes	Yes	Setup varies slightly, but there are no functional differences.
Backup (SMS) <ul style="list-style-type: none"> ♦ SMS ♦ NSS-Xattr 	Yes	Yes	<p>SMS provides backup applications with a framework to develop complete backup and restore solutions. For information, see the <i>OES 2 SP1: Storage Management Services Administration Guide</i>.</p> <p>NSS provides extended attribute handling options for NSS on Linux. For information, see “Using Extended Attributes (xAttr) Commands (Linux)” in the <i>OES 2 SP1: NSS File System Administration Guide</i>.</p>
CIFS (Windows File Services)	Yes - NFAP	Yes - Novell CIFS and Novell Samba	<p>Both NFAP and Novell CIFS are Novell proprietary and tightly integrated with eDirectory and Novell Storage Services (NSS). For a feature comparison by platform, see “CIFS Comparison on NetWare and Linux” in the <i>OES 2 SP1: Novell CIFS for Linux Administration Guide</i>.</p> <p>Samba is an open source product distributed with SUSE® Linux Enterprise Server (SLES).</p> <p>Novell Samba is enhanced by Novell with configuration settings for eDirectory LDAP authentication via Linux User Management (LUM). Novell Samba is not tightly integrated with NSS on Linux and works with any of the supported file systems.</p>
Clustering	Yes	Yes	<p>“Product Features” in the <i>OES 2 SP1: Novell Cluster Services 1.8.6 for Linux Administration Guide</i>.</p> <p>“Product Features” in the <i>OES 2 SP1: Novell Cluster Services 1.8.5 for NetWare Administration Guide</i>.</p>

Service	NetWare 6.5 SP8	OES 2 Linux	Platform Differences / Migration Issues
DFS (Novell Distributed File Services)	Yes	Yes	In combination with NCP Server, DFS supports junctions and junction targets for NSS volumes on Linux and NetWare. DFS also supports junction targets for NCP volumes on non-NSS file systems such as Reiser and Ext3. The VLDB command offers additional options to manage entries in the VLDB for NCP volumes.
DHCP	Yes	Yes	<p>For a comparison between what is available on OES 2 Linux and NetWare, see Section 12.2.2, “DHCP Differences Between NetWare and OES 2 Linux,” on page 107.</p> <p>To plan your DHCP implementations, see “Planning a DHCP Strategy” in the <i>OES 2 SP1: Novell DNS/DHCP Administration Guide for Linux</i> and “Planning a DHCP Strategy” in the <i>OES2 SP1: Novell DNS/DHCP Services for NetWare Administration Guide</i>.</p>
DNS	Yes	Yes	<p>For a comparison between what is available on OES 2 Linux and NetWare, see Section 12.2.1, “DNS Differences Between NetWare and OES 2 Linux,” on page 106.</p> <p>See “Planning a DNS Strategy” in the <i>OES 2 SP1: Novell DNS/DHCP Administration Guide for Linux</i> and “Planning a DNS Strategy” in the <i>OES2 SP1: Novell DNS/DHCP Services for NetWare Administration Guide</i>.</p>
Dynamic Storage Technology	No	Yes	DST runs on OES 2 Linux. An NSS volume on NetWare is supported only as the secondary volume in a shadow pair. When using DST in a cluster, each of the NSS volumes in a shadow pair must reside on OES 2 Linux. DST also supports NCP volumes as shadow pairs and Linux POSIX* volumes as shadow pairs.
eDirectory 8.8	Yes	Yes	No functional differences.
eDirectory Certificate Server	Yes	Yes	No functional differences.
eGuide (White Pages)	Yes	No	This functionality is now part of the Identity Manager 3.6 User Application. For more information, see the Identity Manager 3.6 Documentation Web Site . (http://www.novell.com/documentation/idm36/index.html).

Service	NetWare 6.5 SP8	OES 2 Linux	Platform Differences / Migration Issues
FTP Server	Yes	Yes	<p>Support for eDirectory LDAP authentication has been added to PureFTP on OES 2 Linux. The FTP/SFTP gateway available on NetWare is not currently available on Linux. See Section 17.1.2, "FTP Services," on page 192.</p> <p>See "Features of the NetWare FTP Server" in the OES 2 : Novell FTP for NetWare Administration Guide.</p>
Health Monitoring Services	Yes	Yes	<p>The Health Monitoring Server, which was included in OES 1, has been removed in OES 2.</p> <p>This is now available in various Novell Remote Manager dialog boxes on both platforms.</p> <p>For more information, see "Health Monitoring Services" on page 90.</p>
Identity Manager 3.5 Bundle Edition	Yes	Yes	No functional differences.
iPrint	Yes	Yes	See "Overview" in the OES 2 SP1: iPrint for Linux Administration Guide , and "Overview" in the OES 2 SP1: iPrint Administration Guide for NetWare .
IPX™ (Internetwork Packet Exchange™) from Novell	Yes	No	Novell has no plans to port IPX to OES Linux.
iSCSI	Yes	Yes	<p>The iSCSI target for Linux does not support eDirectory access controls like the NetWare target does. Nor is the iSCSI initiator or target in OES 2 Linux integrated with NetWare Remote Manager management. You use YaST management tools instead.</p> <p>On the other hand, the iSCSI implementation for Linux is newer and performs better.</p> <p>See Linux-iSCSI Project on the Web (http://linux-iscsi.sourceforge.net).</p> <p>See "Overview" in the OES 2 SP 1: iSCSI 1.1.3 for NetWare Administration Guide.</p>
LDAP Server for eDirectory	Yes	Yes	No functional differences.
Multipath Device Management	Yes	Yes	NetWare uses NSS multipath I/O. Linux uses Device Mapper - Multipath that runs underneath other device management services.

Service	NetWare 6.5 SP8	OES 2 Linux	Platform Differences / Migration Issues
MySQL*	Yes - NetWare port of open source product	Yes - Standard Linux	See MySQL.com on the Web (http://www.mysql.com) . See “Overview: MySQL” in the <i>OES 2 SP1: Novell MySQL for NetWare Administration Guide</i> .
NCP Volumes	No	Yes	NCP Server on Linux supports creating NCP volumes on Linux POSIX file systems such as Reiser and Ext3. For information, see “Managing NCP Volumes” in the <i>OES 2 SP1: NCP Server for Linux Administration Guide</i> .
NCP Server	Yes	Yes	NCP services are native to OES NetWare and NSS volumes; to have NCP services on OES Linux, the NCP Server must be installed. See “Benefits of NCP Server” in the <i>OES 2 SP1: NCP Server for Linux Administration Guide</i> .
NetStorage	Yes	Yes	NetStorage on Linux offers connectivity to storage locations through the CIFS, NCP, and SSH protocols. NetWare uses only NCP. These and other differences are summarized in “NetStorage” on page 194.
NetWare Traditional File System	Yes	No	Novell has no plans to port the NetWare Traditional File System to Linux.
NetWare Traditional Volumes	Yes	N/A	
NFS	Yes - NFAP	Yes - native to Linux	For NetWare, see “Working with UNIX Machines” in the <i>OES 2 SP1: AFP, CIFS, and NFS for NetWare (NFAP) Administration Guide</i> .
NICl (Novell International Cryptography Infrastructure)	Yes	Yes	No functional differences.
NMAS™ (Novell Modular Authentication Services)	Yes	Yes	No functional differences.
Novell Audit	Yes	No	Novell Audit is not included with OES Linux. However, the Novell Audit 2.0 Starter pack is available for download at no cost on Novell.com (http://www.novell.com/downloads) .

Service	NetWare 6.5 SP8	OES 2 Linux	Platform Differences / Migration Issues
Novell Client™ for Windows and Linux support	Yes	Yes	Novell Client connectivity to OES 2 Linux requires that the NCP Server be installed.
Novell Cluster Services™	Yes	Yes	See “Product Features” in the <i>OES 2 SP1: Novell Cluster Services 1.8.6 for Linux Administration Guide</i> . See “Product Features” in the <i>OES 2 SP1: Novell Cluster Services 1.8.5 for NetWare Administration Guide</i> .
Novell iFolder® 2.x	Yes	No	For migration information, see “Migrating iFolder 2.x” in the <i>OES 2 SP1: Migration Tool Administration Guide</i> .
Novell iFolder 3.7	No	Yes	OES 2 SP1 Linux includes Linux, Macintosh*, and Windows clients.
Novell Licensing Services	Yes	No	See Section 4.5.3, “OES 2 Linux Doesn’t Support NLS,” on page 59.
NSS (Novell Storage Services™)	Yes	Yes	Most NSS services are available on both platforms. For a list of NSS features that are not used on Linux, see “Cross-Platform Issues for NSS” in the <i>OES 2 SP1: NSS File System Administration Guide</i> .
NTPv3	Yes	Yes	The <code>ntpd.conf</code> file on NetWare can replace an OES Linux server’s NTP configuration file without modification.
OpenSSH	Yes	Yes	Netware includes a port of the open source product. Linux includes the open source product itself. See “Functions Unique to the NetWare Platform” in the <i>OpenSSH Administration Guide</i> .
PAM (Pluggable Authentication Modules)	No	Yes	PAM is a Linux service that Novell leverages to provide eDirectory authentication. eDirectory authentication is native on NetWare.
Pervasive.SQL*	Yes	No	Pervasive.SQL is available for Linux from the Web (http://www.pervasive.com/support/technical/online_manuals.asp) .
PKI (Public Key Infrastructure)	Yes	Yes	No functional differences.
Printing	Yes	Yes	See <i>iPrint</i> .
QuickFinder™	Yes	Yes	See <i>Search</i> .
RADIUS	Yes	Yes	See the information on forge.novell.com (http://forge.novell.com/modules/xfmod/project/?edirfreeradius) .

Service	NetWare 6.5 SP8	OES 2 Linux	Platform Differences / Migration Issues
Samba	No	Yes	<p>Samba is an open source technology available on OES Linux. Novell provides automatic configuration for authentication through eDirectory. For more information, see the <i>OES2 SP1: Samba Administration Guide</i>.</p> <p>OES NetWare provides CIFS connectivity through NFAP. See Section 17.1.3, "Native File Access Protocols," on page 192.</p>
Search (QuickFinder)	Yes	Yes	<p>When indexing a file system, the QuickFinder engine indexes only what it has rights to see.</p> <p>On NetWare, it has full access to all mounted volumes. On Linux, it has rights to only the files that the novlwww user in the www group has rights to see.</p> <p>For more information, see "Security Characteristics" and "Generating an Index For a Linux-Mounted NSS Volume" in the <i>OES 2: Novell QuickFinder Server 5.0 Administration Guide</i>.</p>
SLP	Yes - Novell SLP	Yes - OpenSLP	<p>For OES 2 Linux, see "SLP Services in the Network" (http://www.novell.com/documentation/sles10/sles_admin/data/cha_slp.html) in the <i>SLES 10 SP2: Installation and Administration Guide</i> (http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html) and "Implementing the Service Location Protocol" (http://www.novell.com/documentation/edir87/edir87/data/a2iiimc.html).</p> <p>NetWare uses Novell SLP, which provides synchronization between Directory Agents (DAs) that are in the same eDirectory context. This provides service information beyond the local network.</p> <p>Novell SLP is not available on Linux. OpenSLP on Linux is not customized to provide DA synchronization. Therefore, DA synchronization is only available for eDirectory on NetWare.</p>
Software RAIDS (NSS volumes)	Yes (0, 1, 5, 10, 15)	Yes (0, 1, 5)	<p>See "Understanding Software RAID Devices" in the <i>OES 2 SP1: NSS File System Administration Guide</i>.</p>

Service	NetWare 6.5 SP8	OES 2 Linux	Platform Differences / Migration Issues
Storage Management Services™ (SMS)	Yes	Yes	<p>No functional differences, except that the SBCON backup engine is not supported on Linux.</p> <p>The nbackup engine is available for exploring SMS capabilities, but in a production environment, you should use a third-party, full-featured backup engine.</p>
TCP/IP	Yes	Yes	No functional differences.
Timesync NLM™	Yes	No	<p>Timesync will not be ported to Linux. However, NTPv3 is available on both Linux and NetWare.</p> <p>See “Time Services” on page 108.</p>
Tomcat	Yes	Yes	<p>NetWare includes Tomcat 4 and a Tomcat 5 servlet container for iManager 2.7. OES 2 Linux includes Tomcat 5. There is no impact to any of the OES 2 administration tools, which are tested and supported on both platforms.</p> <p>See “Administration Instance vs. Public Instance on NetWare” (http://www.novell.com/documentation/oes2/web_tomcat_nw/data/ahdyran.html#ahdyran)</p>
Virtual Office (Collaboration)	Yes	No	<p>Virtual Office has been replaced by Novell Teaming + Conferencing. A separate purchase is required. For more information, see the Novell Teaming + Conferencing Web Site (http://www.novell.com/products/teaming/index.html).</p>
WAN Traffic Manager	Yes	No	
Xen Virtualization Guest	Yes	Yes	<p>OES 2 NetWare (NetWare 6.5 SP 7) can run on a paravirtualized machine. OES 2 Linux can run on a paravirtualized machine or fully virtualized machine.</p>
Xen Virtualization Host Server	N/A	Yes	

3.2 Which Services Do I Need?

We recommend that you review the brief overviews included at the beginning of each service section in this guide to get a full picture of the solutions that OES 2 offers. It is not uncommon that administrators discover capabilities in OES that they didn't know existed.

3.3 Exploring OES 2 services

We also recommend that you explore the services by following the step-by-step instructions provided in the *OES2 SP2: Lab Guide for Linux and Virtualized NetWare*.

3.4 Which OES 2 Platform Is Best for My Services?

You can deploy OES 2 SP1 services on either

- ♦ OES 2 NetWare (NetWare 6.5 SP8) or later
- ♦ SUSE Linux Enterprise Server 10 SP2 or later

There are, of course, differences in the way OES provides services on Linux and NetWare (see [Section 3.1, “What Services Are Included in OES 2?”](#) on page 25).

To better assess which OES platform can best meet your network service needs, consider the following:

- ♦ Differences in the platform service offerings that are outlined in [Table 3-1 on page 25](#).
- ♦ Inherent Linux and NetWare strengths that are summarized in [Table 3-2 on page 33](#).

Table 3-2 Platform Comparison

	OES 2 NetWare	SUSE Linux Enterprise Server 10
Brief description	The Novell award-winning network-optimized operating system.	The Novell award-winning Linux operating system.
Industry-recognized strengths	<ul style="list-style-type: none"> ♦ Reliability ♦ Scalability ♦ Security 	<ul style="list-style-type: none"> ♦ Open application environment ♦ Flexibility ♦ Versatility
Business value propositions	<p>NetWare excels when the user population and management burden is highly distributed:</p> <ul style="list-style-type: none"> ♦ Increases network availability. ♦ Optimizes manageability. ♦ Enhances user productivity. ♦ Runs Apache, Tomcat, MySQL, and other open source applications. 	<p>SLES 10 is well suited as an application server running Linux-based solutions:</p> <ul style="list-style-type: none"> ♦ Runs thousands of programs available from the open source community. ♦ Delivers OES file and print services. ♦ Hosts open source Web servers, proxy servers, and mail servers.

3.5 Plan for eDirectory

eDirectory is the heart of OES network services and security.

If you are installing into an existing tree, be sure you understand the information in [Section 14.2.3, “eDirectory Coexistence and Migration,”](#) on page 149.

If you are creating a new eDirectory tree on your network, you must do some additional planning before you install the first server into the tree. The first server is important for two reasons:

- ♦ You create the basic eDirectory tree structure during the first installation
- ♦ The first server permanently hosts the Certificate Authority for your organization

To ensure that your eDirectory tree meets your needs, take time to plan the following:

- ♦ **Structure of the eDirectory tree:** A well-designed tree provides containers for servers, users, printers, etc. It is also optimized for efficient data transfer between geographically dispersed locations. For more information, see [“Designing Your Novell eDirectory Network”](#) in the *Novell eDirectory 8.8 Administration Guide*.
- ♦ **Time synchronization:** eDirectory requires that all OES 2 servers, both NetWare and Linux, be time synchronized. For more information, see [Chapter 12.3, “Time Services,”](#) on page 108.
- ♦ **Partitions and replicas:** eDirectory allows the tree to be partitioned for scalability. Replicas (copies) of the partitions provide fault tolerance within the tree. The first three servers installed into an eDirectory tree automatically receive replicas of the tree’s root partition. You might want to create additional partitions and replicas. For more information, see [“Managing Partitions and Replicas”](#) in the *Novell eDirectory 8.8 Administration Guide*.

For information on these and other eDirectory planning tasks, see the *Novell eDirectory 8.8 Administration Guide*.

The *OES2 SP2: Lab Guide for Linux and Virtualized NetWare* provides a basic introduction to creating container objects as well as Group and User objects in eDirectory.

3.6 Prepare Your Existing eDirectory Tree for OES 2

If you are installing OES 2 into an existing tree, you must use Deployment Manager (located on the NetWare 6.5 SP8 DVD) to see whether your tree requires any updates.

For instructions on running Deployment Manager, see [“Using Deployment Manager”](#) in the *OES 2 SP1: NetWare Installation Guide*.

3.7 Identify a Purpose for Each Server

Large networks usually have one or more servers dedicated to providing a single network service. For example, one or more servers might be designated to provide Novell iFolder file services to network users while other servers provide iPrint printing services for the same users.

For smaller organizations, it is often not practical or cost effective to dedicate servers to providing a single service. For example, the same server might provide both file and print services to network users.

Prior to installing a new server on your network, you should identify the service or services that it will provide.

3.8 Understand Server Requirements

OES 2 Linux and OES 2 NetWare both have specific hardware and software requirements.

Prior to installing OES, make sure your server machine and network environment meet the requirements outlined in the following sections:

- ♦ **OES 2 Linux Server (Physical):** “Preparing to Install OES 2 SP1 Linux” in the *OES 2 SP1: Linux Installation Guide*.
- ♦ **OES 2 Linux Server (Virtual):** “System Requirements” in the *OES 2 SP1: Linux Installation Guide*.
- ♦ **OES 2 NetWare Server (Physical):** “Meeting System Requirements” in the *OES 2 SP1: NetWare Installation Guide*.
- ♦ **OES 2 NetWare Server (Virtual):** “Planning for NetWare VM Guest Servers” in the *OES 2 SP1: NetWare Installation Guide*.

3.9 Understand User Restrictions and Linux User Management

If you plan to use Linux User Management, be sure you understand the security implications before you accept the default PAM-enabled service settings. The implications are explained in [Section 21.2.2, “User Restrictions: Some OES 2 Linux Limitations,” on page 234](#).

3.10 Caveats to Consider Before You Install

IMPORTANT: As support packs are released, there are sometimes new caveats identified. Be sure to always check the [OES Readme \(http://www.novell.com/documentation/oes2/oes_readme/data/readme.html\)](http://www.novell.com/documentation/oes2/oes_readme/data/readme.html) for items specific to each support pack.

This section discusses the following installation/migration caveats:

- ♦ [Section 3.10.1, “AFP File Locking Requires Samba,” on page 36](#)
- ♦ [Section 3.10.2, “Adding a Linux Node to a Cluster Ends Adding More NetWare Nodes,” on page 36](#)
- ♦ [Section 3.10.3, “Do Not Create Local \(POSIX\) Users,” on page 36](#)
- ♦ [Section 3.10.4, “Samba Enabling Disables SSH Access,” on page 36](#)
- ♦ [Section 3.10.5, “Cluster Upgrades Must Be Planned Before Installing OES 2,” on page 37](#)
- ♦ [Section 3.10.6, “Follow the Instructions for Your Chosen Platforms,” on page 37](#)
- ♦ [Section 3.10.7, “iFolder 3.7 Considerations,” on page 37](#)
- ♦ [Section 3.10.8, “Installing into an Existing eDirectory Tree,” on page 38](#)
- ♦ [Section 3.10.9, “NetWare License Placement in the Tree,” on page 39](#)
- ♦ [Section 3.10.10, “NetWare Licenses and OES 2 Linux Trees,” on page 39](#)
- ♦ [Section 3.10.11, “NetWare 6.5 Servers Must Be Running SP3 or Later,” on page 39](#)
- ♦ [Section 3.10.12, “If You’ve Ever Had OES 1 Linux Servers with LUM and NSS Installed,” on page 40](#)

- [Section 3.10.13, “Novell Distributed Print Services Cannot Migrate to Linux,”](#) on page 43
- [Section 3.10.14, “NSS Caveats,”](#) on page 43
- [Section 3.10.15, “Unsupported Service Combinations,”](#) on page 43

3.10.1 AFP File Locking Requires Samba

Cross-protocol file locking between AFP and NCP connections on an OES 2 Linux server requires that you install Samba on the server, even though Samba file services cannot be run concurrently with AFP on the same server. (See [“Novell AFP”](#) on page 44.) For more information, see the *OES 2 SP1: Novell AFP For Linux Administration Guide*

3.10.2 Adding a Linux Node to a Cluster Ends Adding More NetWare Nodes

After you add a Linux node to a cluster, you cannot add more NetWare nodes. For more information, see [“Converting NetWare 6.5 Clusters to OES 2 Linux”](#) in the *OES 2 SP1: Novell Cluster Services 1.8.6 for Linux Administration Guide*.

3.10.3 Do Not Create Local (POSIX) Users

During the OES 2 Linux install you are prompted by the SLES portion of the install to create at least one user besides `root` and you are warned if you bypass the prompt.

Creating local users is not recommended on OES 2 Linux servers because user management in OES 2 is managed entirely in eDirectory. The only local user you need on the server is the `root` user. Creating other local users can, in fact, cause unnecessary confusion and result in service-access problems that are difficult to troubleshoot.

eDirectory users are enabled for POSIX access through the Linux User Management (LUM) technology installed by default on every OES 2 Linux server.

Also be aware that not all OES services require that users are LUM-enabled. Novell Client users, for example, can access NCP and NSS volumes on OES 2 Linux servers just as they do on NetWare without any additional configuration.

For more information about this topic, see [Section 15.2, “Linux User Management: Access to Linux for eDirectory Users,”](#) on page 157.

3.10.4 Samba Enabling Disables SSH Access

Enabling users for Samba automatically disables SSH access for them. However, this default configuration can be changed. For more information, see [Section 11.4, “SSH Services on OES 2 Linux,”](#) on page 100.

3.10.5 Cluster Upgrades Must Be Planned Before Installing OES 2

Because of differences between Novell Cluster Services on OES 2 NetWare and OES 2 Linux, there are important issues to consider before combining them into a mixed node cluster, as explained in the following sections.

- ♦ “Service Failover in a Mixed Cluster” on page 37
- ♦ “Working with Mixed Node Clusters” on page 37

Service Failover in a Mixed Cluster

The only cluster-enabled service that can fail over cross-platform (run on either OES 2 Linux or OES 2 NetWare) is cluster-enabled NSS pools. All other services (iPrint, iFolder, etc.) can only fail over between servers that are the same platform. For example, an iPrint service that is running on an OES 2 Linux server can fail over to another OES 2 Linux server in the cluster, but the service cannot fail over to an OES 2 NetWare server.

Working with Mixed Node Clusters

The following points apply to working with mixed NetWare and OES Linux clusters:

- ♦ You cannot use EVMSGUI to create a Linux POSIX file system as a cluster resource until the entire cluster is migrated to Linux.
- ♦ You cannot migrate or fail over a Linux POSIX file system cluster resource to a NetWare cluster node.
- ♦ Only NSS pool cluster resources that are created on a NetWare cluster node can be failed over between Linux and NetWare nodes.
- ♦ NetWare NSS to Linux NSS failover requires that the Linux node be configured for NSS and that the version of NSS supports the NSS media format and features being used by the NSS pool cluster resource.
- ♦ The new NSS media format in OES 2 is not available for OES 1 SP2 Linux and earlier. After a volume has been upgraded to the new media format, you cannot fail it over to a node that is running OES 1 SP2 Linux or earlier.

3.10.6 Follow the Instructions for Your Chosen Platforms

Although installing OES 2 services on Linux or NetWare is a straightforward process, the installation processes are platform-specific, requiring different sets of media and different installation programs.

3.10.7 iFolder 3.7 Considerations

For best results, be sure you read and carefully follow the instructions in the *OES 2 SP1: Novell iFolder 3.7 Administration Guide*, starting with “Deploying iFolder Server.” This is especially critical if you plan to use NSS for your iFolder 3.7 data volume.

3.10.8 Installing into an Existing eDirectory Tree

Novell Support has reported a significant number of installation incidents related to eDirectory health and time synchronization. To avoid such problems, do the following prior to installing OES:

- ♦ “Consider Coexistence and Migration Issues” on page 38
- ♦ “Do Not Add OES to a Server That Is Already Running eDirectory” on page 38
- ♦ “Be Sure That eDirectory Is Healthy” on page 38
- ♦ “Be Sure That Network Time Is Synchronized” on page 38
- ♦ “Be Sure that OpenSLP on OES 2 Linux Is Configured Properly” on page 38

Consider Coexistence and Migration Issues

If you are installing a new OES 2 server into an existing eDirectory tree, be sure to read and follow the instructions in these sections:

- ♦ “Preparing eDirectory for OES 2 SP1” in the *OES 2 SP1: Linux Installation Guide*
- ♦ “Installing the Server into an Existing eDirectory Tree” in the *OES 2 SP1: NetWare Installation Guide*.

Do Not Add OES to a Server That Is Already Running eDirectory

Although you can add OES to an existing SLES 10 server if needed, you cannot install OES on a SLES 10 server that is already running eDirectory.

eDirectory must be installed in conjunction with the installation of OES services.

Be Sure That eDirectory Is Healthy

Review and follow the guidelines in “Keeping eDirectory Healthy” in the *Novell eDirectory 8.8 Administration Guide*.

Be Sure That Network Time Is Synchronized

OES2 Linux and OES 2 NetWare servers can receive network time from either an existing eDirectory server or from an NTP time source. The critical point is that the entire tree must be synchronized to the same time source. For example, do not set your new OES 2 server to receive time from an NTP source unless the whole tree is synchronized to the same NTP source.

For an in-depth explanation of OES time synchronization, see [Chapter 12.3, “Time Services,” on page 108](#).

Be Sure that OpenSLP on OES 2 Linux Is Configured Properly

Novell SLP (NetWare) and OpenSLP (Linux) can coexist, but there are differences between the services that you should understand before deciding which to use or before changing your existing SLP service configuration. For more information, see [Section 12.5, “SLP,” on page 120](#).

3.10.9 NetWare License Placement in the Tree

By default, NetWare licenses are installed in the same eDirectory container as NetWare servers. Because these licenses also apply to user connections, it is important to install them at or above the location of both servers and users.

For example, if your tree has containers named SERVERS and USERS that are siblings in the tree, you should install the NetWare licenses in a parent or higher container of these two containers.

3.10.10 NetWare Licenses and OES 2 Linux Trees

OES 2 Linux doesn't use the traditional Novell Licensing Services ([Section 4.5, "Licensing," on page 58](#)). As a result, OES Linux servers don't need a license container in eDirectory as part of the server installation.

Therefore, when the first NetWare server is installed in the tree, it needs to add a license container, and to do this it must have a Read/Write replica of eDirectory accessible on the server. If the NetWare server is either the second or third server installed in the tree, it automatically has a replica added. If not, a replica is not added, the license container cannot be created at install time, and a license cannot be installed.

Unlicensed NetWare servers allow only two user connections. To be usable, therefore, the server needs the MLA license installed that is included on the NetWare installation media. For information about the MLA license, see "[OES NetWare Includes MLA License Files](#)" in the *OES2 SPI: Licensing Services for NetWare Administration Guide*.

To install the license, you must do the following:

- 1 Install iManager on the NetWare server, or use iManager Workstation.
You can do this during initial installation or later as described in "[Installing iManager](#)" in the *Novell iManager 2.7 Installation Guide*.
- 2 Add a Read/Write replica to the server as described in "[Adding a Replica](#)" in the *Novell eDirectory 8.8 Administration Guide*.
- 3 Install the NetWare license as described in "[Installing and Removing License Certificates](#)" in the *OES2 SPI: Licensing Services for NetWare Administration Guide*.

The iManager Licensing plug-in is not installed on OES 2 Linux. If you have configured Role-Based Services, you need to make sure the plug-in is installed and added to the RBS collection. For more information, see "[Upgrading iManager](#)" in the *Novell iManager 2.7 Installation Guide*.

NOTE: This is only required for the first NetWare server in the tree. After the container exists, additional licenses can be installed as required.

3.10.11 NetWare 6.5 Servers Must Be Running SP3 or Later

If you are installing OES 2 Linux servers into a tree containing NetWare 6.5 servers, be sure that the following server types have been updated to SP3 or later prior to installing OES 2 Linux:

- ♦ **SLP Directory Agents:** If the SLP Directory Agents on your network are not running NetWare 6.5 SP3 or later, installing an OES 2 Linux server into the tree can cause the DA servers to abend.

- ♦ **LDAP Servers:** If the LDAP servers referenced in your installation are not running NetWare 6.5 SP3 or later, the servers mightabend during a schema extension operation.

3.10.12 If You’ve Ever Had OES 1 Linux Servers with LUM and NSS Installed

Having NSS volumes on OES Linux servers requires certain system-level modifications, most of which are automatic. For more information, see [Appendix I, “System User and Group Management in OES 2 SP1,” on page 267](#).

However, as OES has evolved, some initially defined conventions regarding system Users have needed adjustment. Be sure to read the information and follow the instructions in this section if your network has ever included an OES 1 Linux server with both LUM and NSS installed.

- ♦ [“NetStorage, XTier, and Their System Users” on page 40](#)
- ♦ [“An NSS Complication” on page 40](#)
- ♦ [“eDirectory Solves the Basic Problem” on page 40](#)
- ♦ [“ID Mismatches on OES 1” on page 41](#)
- ♦ [“The OES 1 Solution: The nssid.sh Script” on page 41](#)
- ♦ [“OES 2 SP1 Requires a New Approach” on page 41](#)
- ♦ [“The OES 2 Solution: Standardizing the UIDs on all OES servers” on page 41](#)

NetStorage, XTier, and Their System Users

By default, certain OES services, such as NetStorage, rely on a background Novell service named XTier.

To run on an OES Linux server, XTier requires two system-created users (named `novlxsrvd` and `novlxregd`) and one system-created group that the users belong to (named `novlxtier`).

An NSS Complication

The two system users and their group are created on the local system when XTier is installed. For example, they are created when you install NetStorage, and their respective UIDs and GID are used to establish ownership of the service’s directories and files.

For NetStorage to run, these XTier users and group must be able to read data on all volume types that exist on the OES Linux server.

As long as the server only has Linux traditional file systems, such as Ext3 and Reiser, NetStorage runs without difficulties.

However, if the server has NSS volumes, an additional requirement is introduced. NSS data can only be accessed by eDirectory users. Consequently, the local XTier users can’t access NSS data, and NetStorage can’t run properly.

eDirectory Solves the Basic Problem

Therefore, when NSS volumes are created on the server, the XTier users are moved to eDirectory and enabled for Linux User Management (LUM). See [Section 15.2, “Linux User Management: Access to Linux for eDirectory Users,” on page 157](#).

After the move to eDirectory, they can function as both eDirectory and POSIX users, and they no longer exist on the local system.

ID Mismatches on OES 1

Problems with OES 1 occurred when additional OES NetStorage servers with NSS volumes were installed in the same eDirectory container. Because the UIDs and GID were assigned by the Linux system, unless the installation process was exactly the same for each OES 1 Linux server, the UIDs and GID didn't match server-to-server.

When the local XTier UIDs and GID on subsequently installed servers didn't match the XTier UIDs and GID in eDirectory, NetStorage couldn't access the NSS volumes on the server.

The OES 1 Solution: The `nssid.sh` Script

To solve this problem, the OES 1 installation program looked for XTier ID conflicts, and if the IDs on a newly installed server didn't match the IDs in eDirectory, the program generated a script file named `nssid.sh`. The documentation instructed installers to always check for an `nssid.sh` file on a newly installed server, and if the file was found, to run it. The `nssid.sh` script synchronized all of the XTier IDs with those that had already been stored in eDirectory.

This solution remained viable through the first release of OES 2.

OES 2 SP1 Requires a New Approach

Unfortunately, system-level changes in SUSE Linux Enterprise Server 10 SP2 have invalidated the `nssid.sh` script solution for OES 2 SP1. Synchronizing the XTier IDs with an OES 1 installation can now cause instability in other non-OES components. Therefore, starting with OES 2 SP1, you should standardize all XTier IDs on existing servers before installing a new OES 2 SP1 server with XTier-dependent services.

The OES 2 Solution: Standardizing the UIDs on all OES servers

If your eDirectory tree has ever contained an OES 1 Linux server with NSS and LUM installed, do the following on each server (including OES 2) that has NSS and LUM installed:

- 1 Log in as `root` and open a terminal prompt. Then enter the following commands:

```
id novlxregd
```

```
id novlxsrvd
```

The standardized XTier IDs are UID 81 for `novlxregd`, UID 82 for `novlxsrvd`, and GID 81 for `novlxtier`.

- 2 (Conditional) If you see the following ID information, the XTier IDs are standardized and you can start over with [Step 1](#) for the next server:

```
uid=81(novlxregd) gid=81(novlxtier) groups=81(novlxtier)
uid=82(novlxsrvd) gid=81(novlxtier) groups=81(novlxtier),8(www)
```

- 3 (Conditional) If you see different IDs than those listed above, such as 101, 102, 103, etc., record the numbers for both XTier users and the `novlxtier` group, then continue with [Step 4](#).

You need these numbers to standardize the IDs on the server.

4 Download the following script file:

- ♦ `fix_xtier_ids.sh` (http://www.novell.com/documentation/oes2/scripts/fix_xtier_ids.sh)

5 Customize the template file by replacing the variables marked with angle brackets (<>) as follows:

- ♦ **<server_name>**: The name of the server object in eDirectory.

This variable is listed on line 38 in the file. Replace it with the server name.

For example, if the server name is myserver, replace `<server_name>` with *myserver* so that the line in the settings section of the script reads

```
server=myserver
```

- ♦ **<context>**: This is the context of the XTier user and group objects.

Replace this variable with the fully distinguished name of the context where the objects reside.

For example, if the objects are an Organizational Unit object named servers, replace `ou=servers,o=company` with the fully distinguished name.

- ♦ **<admin_fdn>**: The full context of an eDirectory admin user, such as the Tree Admin, who has rights to modify the XTier user and group objects.

Replace this variable with the admin name and context, specified with comma-delimited syntax.

For example, if the tree admin is in an Organization container named company, the full context is `cn=admin,o=company` and the line in the settings section of the script reads

```
admin_fdn="cn=admin,o=company"
```

- ♦ **<novlxregd_uid>**: This is the UID that the system assigned to the local `novlxregd` user. It might or might not be the same on each server, depending on whether the `nssid.sh` script ran successfully.

Replace this variable with the UID reported for the `novlxregd` user on this server as listed in [Step 1 on page 41](#).

For example, if the UID for the `novlxregd` user is 101, change the line to read

```
novlxregd_uid=101
```

- ♦ **<novlxsrvd_uid>**: This is the UID that the system assigned to the local `novlxsrvd` user. It might or might not be the same on each server, depending on whether the `nssid.sh` script ran successfully.

Replace this variable with the UID reported for the `novlxsrvd` user on this server as listed when you ran the commands in [Step 1 on page 41](#).

For example, if the UID for `novlxsrvd_uid` is 102, change the line to read

```
novlxsrvd_uid=102
```

- ♦ **<novlxtier_gid>**: This is the GID that the system assigned to the local `novlxtier` group. It might or might not be the same on each server, depending on whether the `nssid.sh` script ran successfully.

Replace this variable with the GID reported for the `novlxtier` group on this server as listed when you ran the commands in [Step 1 on page 41](#).

For example, if the GID for `novlxtier_gid` is 101, change the line to read

```
novlxtier_gid=101
```

- 6 Make the script executable and then run it on the server.

IMPORTANT: Changes to the XTier files are not reported on the terminal.

Error messages are reported, but you can safely ignore them. The script scans the entire file system, and some files are locked because the system is running.

- 7 Repeat from **Step 1** for each of the other servers in the same context.

3.10.13 Novell Distributed Print Services Cannot Migrate to Linux

NDPS® clients are not supported on Linux. You must therefore migrate any NDPS clients to iPrint before you migrate your print services to OES 2 Linux. For more information, see “**Migrating NDPS Printers to iPrint**” in the *OES 2 SP1: iPrint Administration Guide for NetWare*.

3.10.14 NSS Caveats

- ♦ “**About New Media Support and Clusters**” on page 43
- ♦ “**Removable Media Cannot Be Mounted on OES 2 Linux**” on page 43

About New Media Support and Clusters

The new media support for hard links on OES 2 NSS volumes was not available for OES 1 SP2 Linux and earlier, but it was available for NetWare 6.5 SP4 and OES 1 NetWare SP1 and later.

If you've already upgraded the media format of the volume, you cannot fail over to a node that is running OES 1 SP2 Linux until you have upgraded the node to OES 2 Linux.

Removable Media Cannot Be Mounted on OES 2 Linux

CD and DVD media and image files cannot be mounted as NSS volumes on Linux; instead, they are mounted as Linux POSIX file systems.

For more details about NSS compatibility, see “**Cross-Platform Issues for NSS Volumes**” in the *OES 2 SP1: NSS File System Administration Guide*.

3.10.15 Unsupported Service Combinations

Do not install any of the following service combinations on the same server. Although not all of the combinations shown in **Table 3-3** cause pattern conflict warnings, Novell does not support any of them.

Table 3-3 *Unsupported Service Combinations*

Service	Unsupported on the Same Server
Novell AFP	<ul style="list-style-type: none"> ♦ File Server (Samba) ♦ Netatalk ♦ Novell Domain Services for Windows ♦ Novell Samba <p>There is an exception if NCP server is installed on the same server as Novell AFP.</p> <p>To support cross-protocol file locking between Novell AFP and NCP, Samba must be installed on the server, but it cannot be used for providing file services to CIFS or SMB clients.</p> <ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server
Novell Archive and Version Services	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows (DSfW) ♦ Xen Virtual Machine Host Server
Novell Backup / Storage Management Services	No restrictions
Novell CIFS	<ul style="list-style-type: none"> ♦ File Server (Samba) ♦ Novell Domain Services for Windows ♦ Novell Samba ♦ Xen Virtual Machine Host Server
Novell Cluster Services (NCS)	<ul style="list-style-type: none"> ♦ High Availability ♦ Novell Domain Services for Windows <p>DSfW can actually be installed and run on the same server as NCS, but DSfW cannot run as a clustered service.</p>
Novell DHCP	<ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server
Novell DNS	<ul style="list-style-type: none"> ♦ DHCP and DNS Server ♦ Xen Virtual Machine Host Server

Service	Unsupported on the Same Server
Novell Domain Services for Windows	<ul style="list-style-type: none"> ♦ File Server (Samba) ♦ Novell AFP ♦ Novell Archive and Version Services ♦ Novell CIFS ♦ Novell Cluster Services (NCS) <p>NCS can actually be installed and run on the server, but DSfW cannot run as a clustered service.</p> <ul style="list-style-type: none"> ♦ Novell FTP ♦ Novell iFolder ♦ Novell NetStorage ♦ Novell Pre-Migration Server ♦ Novell QuickFinder ♦ Novell Samba ♦ Xen Virtual Machine Host Server
Novell eDirectory	<ul style="list-style-type: none"> ♦ Directory Server (LDAP) ♦ Xen Virtual Machine Host Server
Novell FTP	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell iFolder	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell iManager	<ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server
Novell iPrint	<ul style="list-style-type: none"> ♦ Print Server (CUPS) <p>CUPS components are actually installed, but CUPS printing is disabled. For more information, see Section 6.7.6, "iPrint Disables CUPS Printing on the OES 2 Linux Server," on page 69.</p> <ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server
Novell Linux User Management (LUM)	No restrictions
Novell NCP Server / Dynamic Storage Technology	<ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server
Novell NetStorage	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell Pre-Migration Server	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell QuickFinder	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell Remote Manager (NRM)	<ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server

Service	Unsupported on the Same Server
Novell Samba	<ul style="list-style-type: none"> ◆ File Server (Samba) ◆ Novell CIFS ◆ Novell Domain Services for Windows ◆ Xen Virtual Machine Host Server
Novell Storage Services (NSS)	<ul style="list-style-type: none"> ◆ Xen Virtual Machine Host Server
Xen Virtual Machine Host Server	<ul style="list-style-type: none"> ◆ File Server (Samba) ◆ Novell AFP ◆ Novell Archive and Version Services ◆ Novell CIFS ◆ Novell DHCP ◆ Novell DNS ◆ Novell Domain Services for Windows ◆ Novell eDirectory ◆ Novell FTP ◆ Novell iFolder ◆ Novell iManager ◆ Novell iPrint ◆ Novell NCP Server / Dynamic Storage Technology ◆ Novell NetStorage ◆ Novell Pre-Migration Server ◆ Novell QuickFinder ◆ Novell Remote Manager (NRM) ◆ Novell Samba ◆ Novell Storage Services ◆ Print Server (CUPS)

3.11 Consider Coexistence and Migration Issues

You probably have a network that is already providing services to network users. In many cases, the services you are currently running will influence your approach to implementing OES 2. In some cases, there are specific paths to follow so that the OES 2 integration process is as smooth as possible.

Novell has invested considerable effort in identifying service coexistence and migration issues you might face. We understand, however, that we can't anticipate every combination of services that you might have. Therefore, we intend to continue developing coexistence and migration information after each OES product release, and we plan to update the Web-based documentation regularly with the newly developed information.

For information about coexistence of OES 2 servers with existing NetWare and Linux networks, see [Chapter 8, “Migrating and Consolidating Existing Servers and Data,” on page 77](#).

3.12 Understand Your Installation Options

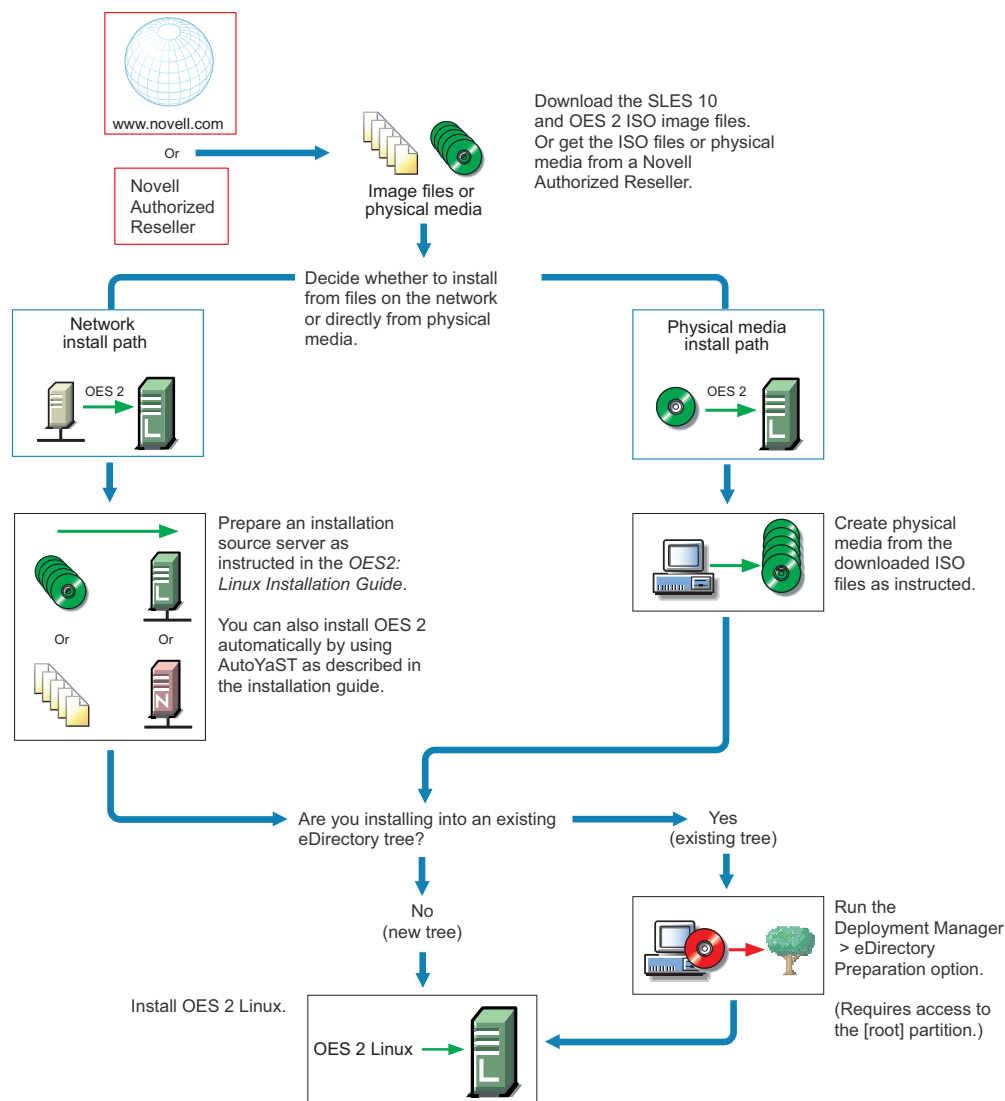
Before installing OES, you should be aware of the information in the following sections:

- ♦ [Section 3.12.1, “OES 2 Linux Installation Overview,” on page 47](#)
- ♦ [Section 3.12.2, “OES 2 NetWare Installation Overview,” on page 48](#)
- ♦ [Section 3.12.3, “About Your Installation Options,” on page 49](#)
- ♦ [Section 3.12.4, “Use Predefined Server Types \(Patterns\) When Possible,” on page 50](#)
- ♦ [Section 3.12.5, “If You Want to Install in a Lab First,” on page 51](#)
- ♦ [Section 3.12.6, “If You Want to Install NSS on a Single-Drive Linux Server,” on page 51](#)

3.12.1 OES 2 Linux Installation Overview

The software and network preparation processes required to install OES 2 Linux are outlined in [Figure 3-1](#).

NOTE: [Chapter 4, “Getting and Preparing OES 2 Software,” on page 53](#) contains instructions for obtaining the ISO image files and the network install script referred to in the following illustration.

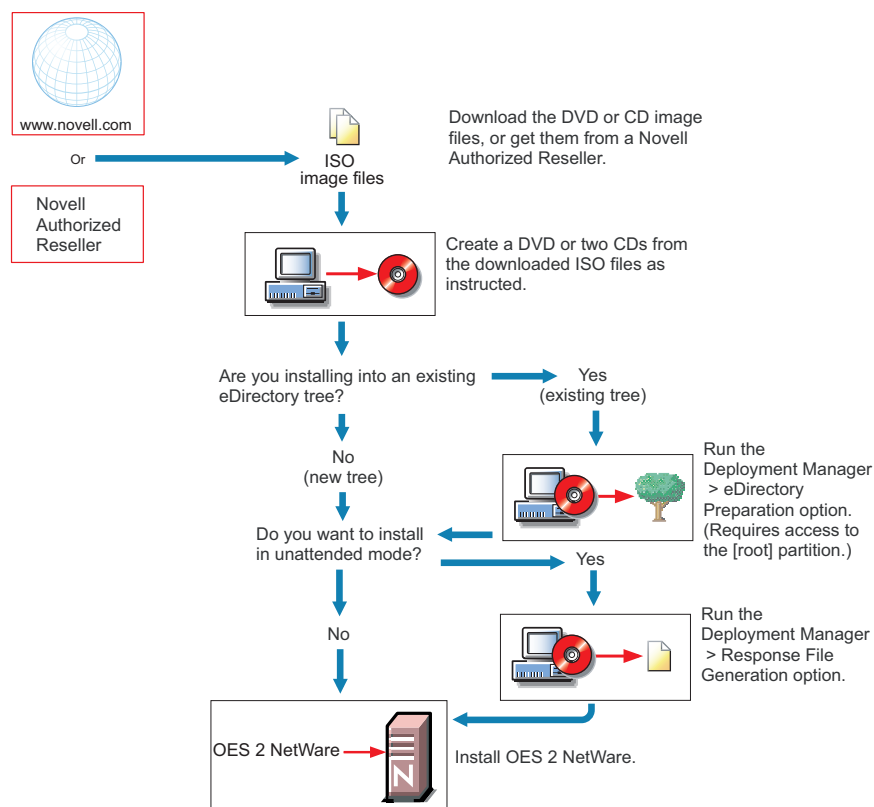
Figure 3-1 OES 2 Linux Install Preparation

For detailed instructions, see “[Setting Up an Installation Source](#)” in the *OES 2 SP1: Linux Installation Guide*.

3.12.2 OES 2 NetWare Installation Overview

The software and network preparation processes required to install OES 2 NetWare are outlined in [Figure 3-2](#). Specific instructions for the steps shown are referenced in the sections that follow.

NOTE: Chapter 4, “[Getting and Preparing OES 2 Software](#),” on page 53 contains instructions for obtaining the ISO image files referred to in the following illustration.

Figure 3-2 OES 2 NetWare Install Preparation

For detailed instructions, see “Installing OES 2 SP1 NetWare (Physical)” in the *OES 2 SP1: NetWare Installation Guide*.

3.12.3 About Your Installation Options

As illustrated in the two previous sections, OES 2 Linux lets you install from physical media or from files on the network, but NetWare requires physical media.

- ♦ “OES 2 Linux Options” on page 50
- ♦ “OES 2 NetWare Options” on page 50
- ♦ “Virtual Machine Installation Options” on page 50

OES 2 Linux Options

OES 2 Linux includes numerous installation options as documented in the *OES 2 SP1: Linux Installation Guide*.

- ♦ **CD/DVD Install:** You can install SLES 10 SP1 by using CDs or a DVD and then install OES 2 Linux from a CD, all of which can be either obtained from a Novell Authorized Reseller or created from downloaded ISO image files.

See “Preparing Physical Media for a New Server Installation or an Upgrade” in the *OES 2 SP1: Linux Installation Guide*.

- ♦ **Network Install:** You can install from the network by using the NFS, FTP, or HTTP protocol. Installing from the network saves you from swapping CDs on the server during the installation. See “Preparing a Network Installation Source” in the *OES 2 SP1: Linux Installation Guide*.

- ♦ **Automated Install:** You can install from the network by using an AutoYaST file.

This lets you install without providing input during the installation process. It is especially useful for installing multiple servers with similar configurations.

See “Using AutoYaST to Install and Configure Multiple OES 2 SP1 Linux Servers” in the *OES 2 SP1: Linux Installation Guide*.

OES 2 NetWare Options

OES 2 NetWare installation options are documented in the *OES 2 SP1: NetWare Installation Guide*.

- ♦ **CD/DVD Install:** You can install by using CDs or a DVD obtained from a Novell Authorized Reseller, or you can create CDs or a DVD from downloaded ISO image files.

See “Accessing the Installation Files” in the *OES 2 SP1: NetWare Installation Guide*.

Virtual Machine Installation Options

Virtual machine installations offer additional options. For more information, see

- ♦ “Installing, Upgrading, or Updating OES 2 SP1 Linux on a Xen-based Virtual Machine” in the *OES 2 SP1: Linux Installation Guide*
- ♦ “Installing and Managing OES 2 SP1 NetWare on a Xen-based VM Host Server” in the *OES 2 SP1: NetWare Installation Guide*.

3.12.4 Use Predefined Server Types (Patterns) When Possible

Both OES 2 Linux and OES 2 NetWare include predefined server installation options that install only the components required to provide a specific set of network services. In the OES 2, these server types are called *patterns*.

For example, if you want to install an OES 2 server that provides enterprise level print services, you should select the *Novell iPrint Server* pattern during the installation.

You should always choose a predefined server type if one fits the intended purpose of your server. If not, you can choose to install a customized OES 2 server with only the service components you need.

More information about server patterns is available in the installation guides:

- ♦ **OES 2 Linux:** “OES Services Pattern Descriptions” in the *OES 2 SP1: Linux Installation Guide*
- ♦ **OES 2 NetWare:** “Choosing a Server Pattern” in the *OES 2 SP1: NetWare Installation Guide*

3.12.5 If You Want to Install in a Lab First

Many organizations prefer to install products on smaller servers for testing in a lab prior to full deployment. The *OES2 SP2: Lab Guide for Linux and Virtualized NetWare* walks you through installing and exploring all the basic OES 2 services.

3.12.6 If You Want to Install NSS on a Single-Drive Linux Server

Many are interested in Novell Storage Services (NSS) running on Linux. If you plan to experiment with NSS on a single-drive server, be sure to follow the instructions in “Installing Linux with EVMS as the Volume Manager of the System Device” in the *OES 2 SP1: Linux Installation Guide*.

3.13 eGuide, iFolder 2, and Virtual Office Are Still Available on Netware

Contrary to the direction announced for the initial release of OES 2, Novell has decided that eGuide, iFolder 2, and Virtual Office will not be removed from NetWare 6.5 (OES 2 NetWare). There are no plans to make them available on OES 2 Linux.

The designated replacement services are as follows:

- ♦ **eGuide:** Replaced in the Identity Manager 3.6 User Application by the functionality in the *Self-Service* tab. A separate purchase is required. See “Using the Identity Self-Service Tab” (<http://www.novell.com/documentation/idmr36/ugpro/data/ugpropartidentity.html>) in the *Identity Manager 3.6 User Application Documentation on the Web* (<http://www.novell.com/documentation/idmr36/ugpro/data/bookinfo.html>).
- ♦ **Folder 2:** Replaced by iFolder 3.7, which is included in OES 2 SP1 Linux. For more information, see *Section 17.10, “Novell iFolder 3.7 Implementation and Maintenance,” on page 219*.
- ♦ **Virtual Office:** Replaced by Novell Teaming + Conferencing. A separate purchase is required. For more information, see the *Novell Teaming + Conferencing Web Site* (<http://www.novell.com/products/teaming/index.html>).

Documentation for these components on NetWare is available on the *OES 1 Documentation Web site* (<http://www.novell.com/documentation/oes>).

Getting and Preparing OES 2 Software

This section contains instructions for getting and preparing Open Enterprise Server 2 software and discusses the following topics:

- ♦ Section 4.1, “Do You Have Upgrade Protection?,” on page 53
- ♦ Section 4.2, “Do You Want 32-Bit or 64-Bit OES Linux?,” on page 53
- ♦ Section 4.3, “Do You Want to Purchase OES 2 or Evaluate It?,” on page 54
- ♦ Section 4.4, “Evaluating OES 2 Software,” on page 54
- ♦ Section 4.5, “Licensing,” on page 58

If you have not already done so, we recommend that you review the information in [Section 3.12, “Understand Your Installation Options,”](#) on page 47.

4.1 Do You Have Upgrade Protection?

If you have Novell® Upgrade Protection, you can upgrade to OES 2 and the associated support packs, free of charge until your upgrade protection expires. After your protection expires, the OES 2 upgrade link disappears from your account page.

For more information and to start the upgrade process, do the following:

- 1 Using your Novell account information, log in to the [Novell Web Site \(http://www.novell.com/nps\)](http://www.novell.com/nps).
- 2 Click *Customer Center* and log in, using your Novell account username and password to access the Novell Customer Center home page.
- 3 Follow the instructions on the page to obtain the upgrade to Open Enterprise Server 2.

4.2 Do You Want 32-Bit or 64-Bit OES Linux?

Compatibility is the first thing to consider as you start planning which software to download and install.

OES NetWare® (NetWare 6.5) is a 32-bit operating system that you can install on both 32-bit and 64-bit server hardware.

OES Linux, on the other hand, is a set of services or an “add-on product” that runs on SUSE® Linux Enterprise Server (SLES 10) and is available in both 32-bit and 64-bit versions. These two versions are required for compatibility with SLES 10 and the server hardware that it runs on. Having two versions of OES Linux introduces a little more complexity into your planning, as illustrated in [Table 4-1](#).

Table 4-1 OES 2, SLES 10, and Server Hardware Compatibility Matrix

OES 2 SP1 Version	SLES 10 SP2	Server Hardware	Notes
32-bit (i386)	32-bit (i386)	32-bit	The 32-bit version of OES 2 SP1 requires the 32-bit version of SLES 10 SP2.
		64-bit	<p>Attempting to install the 32-bit version of OES as an add-on product to the 64-bit version of SLES 10 generates numerous dependency errors because the 32-bit OES 2 install is looking for 32-bit SLES 10 packages.</p> <p>32-bit software (OES and SLES) can be installed on either 32-bit or 64-bit hardware.</p>
64-bit (x86_64)	64-bit (x86_64)	64-bit	The 64-bit version of OES 2 SP1 requires the 64-bit version of SLES 10 SP2, and they can only be installed on 64-bit hardware.

4.3 Do You Want to Purchase OES 2 or Evaluate It?

If you want to evaluate OES prior to purchasing it, skip to the next section, [Evaluating OES 2 Software](#).

If you have decided to purchase OES 2, visit the Novell [How to Buy OES 2 Web page](http://www.novell.com/products/openenterpriseserver/howtobuy.html) (<http://www.novell.com/products/openenterpriseserver/howtobuy.html>).

When you purchase OES 2, you receive two activation codes for OES 2 Linux (one for OES 2 services and one for SUSE Linux Enterprise Server 10). Both codes are required for registering an OES 2 Linux system in the Novell Customer Center. After it is registered, your server can receive online updates, including the latest support pack.

NOTE: Purchasing OES 2 also lets you obtain OES 2 NetWare support packs at no charge as they become available on the [Novell Support Web site](http://support.novell.com/filefinder/) (<http://support.novell.com/filefinder/>)

As part of the purchase process, it is important that you understand the OES 2 licensing model. For a brief description, see [Section 4.5, “Licensing,” on page 58](#). A more thorough explanation of Novell Licensing Services (NLS) is contained in the *OES2 SP1: Licensing Services for NetWare Administration Guide*.

After completing your purchase, the installation process goes more smoothly if you understand your installation options for each OES 2 platform. If you haven’t already done so, be sure to review the information in [Section 3.12, “Understand Your Installation Options,” on page 47](#) and then skip to [Chapter 5, “Installing OES 2,” on page 61](#).

4.4 Evaluating OES 2 Software

This section walks you through the OES 2 software evaluation process and discusses the following topics:

- ♦ [Section 4.4.1, “Understanding OES 2 Software Evaluation Basics,” on page 55](#)

- ♦ [Section 4.4.2, “Downloading OES 2 SP1 Software from the Novell Web Site,” on page 55](#)
- ♦ [Section 4.4.3, “Preparing the Installation Media,” on page 56](#)
- ♦ [Section 4.4.4, “Installing OES 2 for Evaluation Purposes,” on page 57](#)
- ♦ [Section 4.4.5, “Evaluating OES 2,” on page 57](#)
- ♦ [Section 4.4.6, “Installing Purchased Activation Codes after the Evaluation Period Expires,” on page 58](#)

4.4.1 Understanding OES 2 Software Evaluation Basics

You can evaluate the full OES 2 product on both product platforms (Linux and NetWare). The evaluation software is the complete, fully functional OES 2 product.

As you install each server, you are required to accept an end user license agreement (EULA). Your rights to evaluate and use the OES 2 product are limited to the rights set forth in the EULA, which are, briefly, the following:

- ♦ The evaluation period for OES 2 Linux servers is 60 days. To receive software updates during this time, you must have or create an account with the Customer Center, receive evaluation codes for OES 2 and SLES 10 while downloading the software, and use these codes to register your server. No software updates can be downloaded after the 60-day evaluation period expires until you purchase the product.
- ♦ The evaluation period for OES 2 NetWare servers is 90 days, after which Novell expects you to either purchase OES 2 or uninstall OES 2 NetWare.

4.4.2 Downloading OES 2 SP1 Software from the Novell Web Site

If you already have OES 2 SP1 ISO image files, skip to [Section 4.4.3, “Preparing the Installation Media,” on page 56](#).

If you have OES 2 SP1 product media (CDs and DVDs), skip to [Section 4.4.4, “Installing OES 2 for Evaluation Purposes,” on page 57](#).

To download ISO image files from the Web:

- 1 If you don't already have a Novell account, register for one on the [Web \(https://secure-www.novell.com/selfreg/jsp/createAccount.jsp?\)](https://secure-www.novell.com/selfreg/jsp/createAccount.jsp?).
- 2 Access the [Novell Downloads Web page \(http://download.novell.com\)](http://download.novell.com).
- 3 Do a keyword search for *Open Enterprise Server 2 SP1*, then click the *Open Enterprise Server 2 SP1 e-Media Kit* link.
- 4 Click the *proceed to download* button (upper right corner of the first table).
- 5 If you are prompted to log in, type your *Novell Account > username* and *password*, then click *login*.
- 6 Accept the *Export Agreement* (required for first downloads only) and answer the survey questions about your download (optional).
- 7 Print the download page. You need the listed MD5 verification numbers to verify your downloads.
- 8 Scroll down to the *Download Instructions* section and click the *Download Instructions* link.

- 9 Print the Download Instructions page for future reference.
- 10 Use the information on the Download Instructions page to decide which files you need to download for the platforms you plan to evaluate, then mark them on the MD5 verification list on the page you printed in [Step 7](#).
- 11 On the download page, start downloading the files you need by clicking the *download* button for each file.
- 12 If you have purchased OES 2 previously and received purchased OES 2 and SLES 10 activation codes, skip to [Step 15](#).
Otherwise, in the *Evaluating Open Enterprise Server 2* section, click the *Get Activation Codes* link in the *Novell Open Enterprise Server 2—Linux* paragraph.
60-day evaluation codes are sent in separate e-mail messages to the e-mail address associated with your Novell account.
- 13 Access your e-mail account and print the messages or write down the activation codes.
Both the OES 2 and the SLES codes are required for product registration and downloading software updates.
- 14 Click *Back* to return to the download page.
- 15 In the download table at the top of the page, click the *Install Instructions > View* link at the end of the list of files to download.
Although you might have printed this file earlier, the online version is required for the steps that follow.
- 16 Scroll past the download decision tables; while you wait for the downloads, read through the brief installation instructions, clicking the links for more information.
- 17 Verify the integrity of each downloaded file by running an MD5-based checksum utility on it and comparing the values against the list you printed in [Step 15](#).
For example, on a Linux system you can enter the following command:

```
md5sum filename
```


where *filename* is the name of the *.iso* file you are verifying.
For a Windows system, you need to obtain a Windows-compatible MD5-based checksum utility from the Web and follow its usage instructions.
- 18 (Optional) If you plan to install OES 2 Linux from files on your network, see the instructions in “[Preparing a Network Installation Source](#)” in the *OES 2 SP1: Linux Installation Guide*.

4.4.3 Preparing the Installation Media

IMPORTANT: If you have downloaded *.iso* image files from the Web, it is critical that you verify the integrity of each file as explained in [Step 17 on page 56](#). Failure to verify file integrity can result in failed installations, especially in errors that report missing files.

Instructions for preparing installation media are located in

- ♦ “[Setting Up an Installation Source](#)” in the *OES 2 SP1: Linux Installation Guide*.
- ♦ “[Preparing the NetWare Installation Software](#)” in the *OES 2 SP1: NetWare Installation Guide*.

4.4.4 Installing OES 2 for Evaluation Purposes

The following sections explain how to activate your OES 2 servers for evaluation purposes. Detailed instructions are found in the platform-specific installation guides.

- ♦ “OES 2 Linux” on page 57
- ♦ “OES 2 NetWare” on page 57

OES 2 Linux

If you followed the instructions in [Section 4.4.2, “Downloading OES 2 SP1 Software from the Novell Web Site,” on page 55](#), you now have two activation codes (for the purchased product and for a 60-day evaluation). As you install OES 2 Linux, you should register with the Novell Customer Center and use these activation codes to enable your server for online updates.

IMPORTANT: Always download the current patches during an installation.

Instructions for using the activation codes during an installation are found in “[To register the server during the installation:](#)” in the *OES 2 SP1: Linux Installation Guide*.

Use the same activation codes for each OES 2 Linux server you install during the evaluation period.

OES 2 NetWare

All OES 2 NetWare installation media contains a `\LICENSE` folder with a non-expiring MLA license file in it. You should select this license when you install the first OES 2 NetWare evaluation server in a new tree. Subsequent NetWare installations use the same license.

For an explanation of why an MLA license is now included and to understand the benefits and limitations associated with this change, see “[OES NetWare Includes MLA License Files](#)” in the *OES2 SP1: Licensing Services for NetWare Administration Guide*.

Instructions for installing NetWare licenses are contained in “[Licensing the NetWare Server](#)” in the *OES 2 SP1: NetWare Installation Guide*.

4.4.5 Evaluating OES 2

During the evaluation period, we recommend that you fully explore the many services available in OES 2.

To help you get started with the process, we have prepared a lab guide for OES 2 that explores both OES 2 Linux and virtualized OES 2 NetWare on a second OES 2 Linux server. The sections in this guide introduce eDirectory™, walk you through server installations, and provide brief exercises you can complete to get started using OES 2 Services. After completing the exercises in the guide, you can use the lab setup to further explore OES 2 and learn about its many powerful services.

For more information, see the *OES2 SP2: Lab Guide for Linux and Virtualized NetWare*.

After working through the lab guide, we recommend that you review all of the information in this guide to gain a comprehensive overview of OES 2 and the planning and implementation processes you will follow to fully leverage its network services.

4.4.6 Installing Purchased Activation Codes after the Evaluation Period Expires

After purchasing Open Enterprise Server, use the instructions in “[Registering the Server in the Novell Customer Center \(Command Line\)](#)” in the *OES 2 SP1: Linux Installation Guide* to enter the purchased activation codes that you received with your purchase. After logging in as `root`, complete the step where you enter the activation codes, replacing the evaluation codes with the purchased codes.

4.5 Licensing

This section explains the following:

- ♦ [Section 4.5.1, “The OES 2 Licensing Model,” on page 58](#)
- ♦ [Section 4.5.2, “Licensing Services on OES 2 NetWare,” on page 58](#)
- ♦ [Section 4.5.3, “OES 2 Linux Doesn’t Support NLS,” on page 59](#)
- ♦ [Section 4.5.4, “Configuring and Administering Licensing Services,” on page 59](#)

4.5.1 The OES 2 Licensing Model

The only licensing restriction is the number of user connections allowed to use OES 2 services on your network. You are authorized to install as many OES 2 servers (both Linux and NetWare) as you need to provide OES 2 services to those users.

For example, if your OES 2 license is for 100 user connections, you can install as many OES 2 NetWare and/or OES 2 Linux servers as desired. Up to 100 users can then connect to and use the services provided by those OES 2 servers. When you install OES 2 on either platform, you must accept an end user license agreement (EULA). Your rights to use the OES 2 product are limited to the rights set forth in the EULA. Violators of the Novell license agreements and intellectual property are prosecuted to the fullest extent of the law.

NOTE: SUSE Linux Enterprise Server entitlements in OES 2 have changed from OES 1. For more information, refer to the EULA.

To report piracy and infringement violations, please call 1-800-PIRATES (800-747-2837) or send e-mail to pirates@novell.com.

For more information on OES 2 licensing, see the [OES 2 Licensing page on the Novell Web site \(http://www.novell.com/licensing/oes_licensing.html\)](http://www.novell.com/licensing/oes_licensing.html).

4.5.2 Licensing Services on OES 2 NetWare

When you install or upgrade NetWare, the server installation software automatically installs the Novell Licensing Services (NLS) software. During the installation of the first NetWare server in a tree, you are prompted for a license/key file pair (*.nlf and *.nfk).

Starting with OES 2, a non-expiring MLA NetWare license file is included on the installation media in the `\LICENSE` folder. Installing this license effectively removes the NLS-based enforcement of user connection limitations as it existed in earlier versions of NetWare. However, user connection limitations are still in force as defined in each license agreement (referred to as a *paper license*) issued by Novell when you purchase OES 2.

For an explanation of why an MLA license is now included and to understand the benefits and limitations associated with this change, see “**OES NetWare Includes MLA License Files**” in the *OES2 SPI: Licensing Services for NetWare Administration Guide*.

After installing OES 2, you can use Novell iManager to install and manage license certificates in your eDirectory tree and to monitor NetWare usage. You can also monitor usage of Novell Licensing Services-enabled products.

4.5.3 OES 2 Linux Doesn't Support NLS

Novell Licensing Services (NLS) are not available on OES 2 Linux, nor does an OES 2 Linux installation require a license/key file pair (*.nlf and *.nfk).

4.5.4 Configuring and Administering Licensing Services

See the related topics in “**Licensing**” in the OES online documentation.

Installing OES 2

IMPORTANT: Before you install Open Enterprise Server 2, be sure to review the information in Chapter 3, “Planning Your OES 2 Implementation,” on page 25, especially Section 3.10, “Caveats to Consider Before You Install,” on page 35.

This section briefly covers the following:

- ♦ Section 5.1, “Installing OES 2 Linux,” on page 61
- ♦ Section 5.2, “Installing OES 2 NetWare,” on page 62
- ♦ Section 5.3, “Installing OES 2 Servers in a Xen VM,” on page 62

5.1 Installing OES 2 Linux

The OES 2 Linux installation leverages the SUSE® Linux YaST graphical user interface. You can install OES 2 Linux services on an existing SUSE Linux Enterprise Server 10 server, or you can install both OES 2 and SLES 10 at the same time, making the installation of SLES 10 and OES 2 services a seamless process.

To ensure a successful installation:

1. Read and follow any instructions in the [OES 2 Readme \(http://www.novell.com/documentation/oes2/oes_readme/data/oes_readme.html#bsen7me\)](http://www.novell.com/documentation/oes2/oes_readme/data/oes_readme.html#bsen7me).
2. Carefully follow the instructions in the *OES 2 SP1: Linux Installation Guide*, especially those found in
 - ♦ “Preparing to Install OES 2 SP1 Linux”
 - ♦ “Installing Open Enterprise Server 2 SP1 Linux”
3. Make sure you always download the latest patches as part of the Customer Center configuration during the install. This ensures the most stable configuration and installation process and prevents some issues that are documented in the product Readme.
4. After updating the server, red text appears under the *CA Management* section, indicating that the CA must be configured before proceeding.

This happens because the `root` password is no longer in memory after the server reboots.

Click *CA Management*, type and confirm the `root` password in the indicated fields, then click *Next*. The installation proceeds.

5. During the installation, you have the option to disable each service configuration. However, we recommend that you configure all services at install time simply because the process is more streamlined.

For more information on configuring services later, see “Installing or Configuring OES 2 Services on an Existing OES 2 SP1 Linux or SLES 10 SP2 Server” in the *OES 2 SP1: Linux Installation Guide*.

5.1.1 What's Next

After installing OES 2 and before starting to use your new OES 2 Linux server, be sure to review the information in **Chapter 6, “Caveats for Implementing OES 2 Services,”** on page 63.

The various service sections in this guide contain information about completing your OES 2 services implementation. See the sections for the services you have installed, beginning with **Chapter 11, “Managing OES 2,”** on page 85.

5.2 Installing OES 2 NetWare

Installing OES 2 NetWare® (NetWare 6.5) directly on a physical server involves the NetWare graphical user interface.

To ensure a successful installation:

1. Read and follow any instructions in the **OES 2 Readme** (http://www.novell.com/documentation/oes2/oes_readme/data/oes_readme.html#bsfagt4).
2. Carefully follow the instructions in the *OES 2 SP1: NetWare Installation Guide*, especially those found in
 - ♦ “Preparing to Install OES 2 SP1 NetWare”
 - ♦ “Installing OES 2 SP1 NetWare (Physical)”

5.2.1 What's Next

After installing OES 2 and before starting to use your new OES 2 NetWare server, be sure to follow the instructions in **Chapter 6, “Caveats for Implementing OES 2 Services,”** on page 63.

The various service sections in this guide contain information about completing your OES 2 services implementation. See the sections for the services you have installed, beginning with **Chapter 11, “Managing OES 2,”** on page 85.

5.3 Installing OES 2 Servers in a Xen VM

Installing OES 2 servers on a Xen virtual machine involves installing an OES 2 SP1 Linux or SUSE® Linux Enterprise Server (SLES) 10 SP2 VM host server, creating a VM, and then installing an OES 2 server (NetWare or Linux) in the VM.

To get started with Xen virtualization in OES 2, see the following:

- ♦ “Introduction to Xen Virtualization (http://www.novell.com/documentation/sles10/xen_admin/data/sec_xen_basics.html)” in the *Virtualization with Xen* (http://www.novell.com/documentation/sles10/xen_admin/data/bookinfo.html) guide.
- ♦ “Installing OES 2 SP1 Linux as a Xen VM Host Server” in the *OES 2 SP1: Linux Installation Guide*.
- ♦ “Installing, Upgrading, or Updating OES 2 SP1 Linux on a Xen-based Virtual Machine” in the *OES 2 SP1: Linux Installation Guide*.
- ♦ “Installing and Managing OES 2 SP1 NetWare on a Xen-based VM Host Server” in the *OES 2 SP1: NetWare Installation Guide*.

Caveats for Implementing OES 2 Services

This section presents a few pointers for avoiding common Open Enterprise Server 2 implementation problems.

The list that follows is not comprehensive. Rather, it simply outlines some of the more common problems reported by network administrators. To ensure successful service implementations, you should always follow the instructions in the documentation for the services you are implementing.

- ♦ [Section 6.1, “Avoiding POSIX and eDirectory Duplications,” on page 63](#)
- ♦ [Section 6.2, “ConsoleOne Can Cause JClient Errors,” on page 65](#)
- ♦ [Section 6.3, “CUPS on OES 2 Linux,” on page 66](#)
- ♦ [Section 6.4, “eDirectory,” on page 66](#)
- ♦ [Section 6.5, “iManager 2.7,” on page 67](#)
- ♦ [Section 6.6, “iFolder 3.7,” on page 68](#)
- ♦ [Section 6.7, “iPrint,” on page 68](#)
- ♦ [Section 6.8, “NCP Server \(OES 2 Linux\),” on page 69](#)
- ♦ [Section 6.9, “NSS \(OES 2 Linux\),” on page 70](#)
- ♦ [Section 6.10, “OpenLDAP on OES 2 Linux,” on page 70](#)
- ♦ [Section 6.11, “Samba,” on page 70](#)
- ♦ [Section 6.12, “Virtualization Issues,” on page 70](#)
- ♦ [Section 6.13, “Web Services,” on page 71](#)

6.1 Avoiding POSIX and eDirectory Duplications

OES 2 Linux servers can be accessed by

- ♦ Local (POSIX) users that are created on the server itself.
- ♦ eDirectory users that are given local access through Linux User Manager (LUM).

However, there are some issues you need to consider:

- ♦ [Section 6.1.1, “The Problem,” on page 63](#)
- ♦ [Section 6.1.2, “Three Examples,” on page 64](#)
- ♦ [Section 6.1.3, “Avoiding Duplication,” on page 65](#)

6.1.1 The Problem

There is no cross-checking between POSIX and eDirectory™ to prevent the creation of users or groups with duplicate names.

When duplicate names occur, the resulting problems are very difficult to troubleshoot because everything on both the eDirectory side and the POSIX side appears to be configured correctly. The most common problem is that LUM-enabled users can't access data and services as expected but other errors could surface as well.

Unless you are aware of the users and groups in both systems, especially those that are system-created, you might easily create an invalid configuration on an OES 2 Linux server.

6.1.2 Three Examples

The following examples illustrate the issue.

- ♦ “The shadow Group” on page 64
- ♦ “The users Group” on page 64
- ♦ “Other Non-System Groups” on page 64

The shadow Group

There is a default **system-created group** named `shadow` that is used by certain Web-related services, including the OES 2 QuickFinder™ server, but it has no relationship with Dynamic Storage Technology (DST) and shadow volumes.

Because `shadow` is a local POSIX group, there is nothing to prevent you from creating a LUM-enabled second group in eDirectory that is also named `shadow`. In fact, this could be a logical name choice for many administrators in conjunction with setting up shadow volume access for Samba/CIFS users.

However, using this group name results in LUM-enabled users being denied access by POSIX, which looks first to the local `shadow` group when determining access rights and only checks eDirectory for a group named `shadow` if no local group is found.

The users Group

There is another default system-created group named `users` that is not used by OES 2 services but is nevertheless created on all SLES 10 (and therefore, OES 2 Linux) servers.

Creating an eDirectory group named `users` would seem logical to many administrators. And as with the shadow group, nothing prevents you from using this name.

Unfortunately, having a LUM-enabled eDirectory group named `users` is not a viable configuration for services requiring POSIX access. The local `users` group is always checked first, and the LUM-enabled `users` group in eDirectory won't be seen by POSIX.

NOTE: Do not confuse eDirectory Group objects with Organizational Unit (OU) container objects.

Creating an OU container in eDirectory named `users` is a valid option and does not create conflicts with POSIX.

Other Non-System Groups

Conflicts between group and user names also occur when administrators create local and eDirectory groups with the same name.

For example, one administrator creates a group named `myusers` on the local system and another creates a LUM-enabled group in eDirectory with the same name. Again, the LUM-enabled users who are members of the eDirectory group won't have access through POSIX.

This is why we recommend that, as a general rule, administrators should not create local users or groups on OES 2 Linux servers. You should only make exceptions when you have determined that using LUM-enabled users and groups is not a viable option and that objects with the same names as the POSIX users and groups will not be created in eDirectory in the future.

6.1.3 Avoiding Duplication

Having duplicate users and groups is easily avoided by following these guidelines:

- ♦ “Use YaST to List All System-Created Users and Groups” on page 65
- ♦ “Create Only eDirectory Users and Groups” on page 65

Use YaST to List All System-Created Users and Groups

We recommend that you use the YaST Group Management/User Management module to check for names you might duplicate by mistake.

1. Open the YaST Control Center.
2. Click either *Group Management* or *User Management*.
3. Click *Set Filter > Customize Filter*.
4. Select both options (*Local* and *System*), then click *OK*.

All users or groups as displayed, including those that exist only in eDirectory and are LUM-enabled.

5. To avoid duplication, keep this list in mind as you create eDirectory users and groups.

NOTE: The list of users and groups in [Appendix I, “System User and Group Management in OES 2 SP1,” on page 267](#) is not exhaustive. For example, the `users` group is not listed.

Create Only eDirectory Users and Groups

For OES 2 Linux services, the LUM technology eliminates the need for local users and groups. We recommend, therefore, that you avoid the problems discussed in this section by not creating local users and groups.

6.2 ConsoleOne Can Cause JClient Errors

If you need to use ConsoleOne® to manage services on OES 2, make sure you have installed version 1.3.6h or later.

Earlier versions of ConsoleOne cause JClient errors in iManager.

6.3 CUPS on OES 2 Linux

iPrint is the print solution for OES 2 Linux and offers more robust and scalable print services than a CUPS installation can. iPrint actually uses CUPS to render print jobs prior to sending them to the printer, but for scalability and performance, printing from the server itself is disabled during iPrint installation.

If you plan to use iPrint, deselect *Print Server* in the *Primary Functions* category during the install and don't configure CUPS on the OES 2 Linux server.

6.4 eDirectory

- ♦ [Section 6.4.1, “Avoid Uninstalling eDirectory,” on page 66](#)
- ♦ [Section 6.4.2, “Avoid Renaming Trees and Containers,” on page 66](#)
- ♦ [Section 6.4.3, “One Instance Only,” on page 66](#)
- ♦ [Section 6.4.4, “Default Static Cache Limit Might Be Inadequate,” on page 67](#)
- ♦ [Section 6.4.5, “Special Characters in Usernames and Passwords,” on page 67](#)

6.4.1 Avoid Uninstalling eDirectory

OES services are tightly integrated with eDirectory and do not function without it.

Although the eDirectory 8.8 documentation describes how to remove and reinstall eDirectory, the processes described do not cleanly decouple OES services, nor do they restore service connections. As a result, not only does uninstalling eDirectory break OES services, reinstalling eDirectory does not restore them.

If you have an issue that you believe can only be resolved by uninstalling eDirectory, make sure you consult with Novell Technical Services before you attempt to do so.

6.4.2 Avoid Renaming Trees and Containers

The configuration files for many OES services point to configuration data stored within eDirectory.

Although eDirectory tracks all changes internally, OES services do not. Therefore, if you rename your eDirectory tree or one of the containers below [Root], you should expect that one or more of your OES services will break.

If you need to rename a container or tree, make sure that you

1. Identify all of the configuration files for your OES services.
2. Assess whether the changes that you are planning impact any of your service configurations.
3. Understand and articulate the changes that are required to restore your services after renaming.

There are no automated tools in OES for resolving the configuration errors and other problems that are caused by renaming a tree or its containers.

6.4.3 One Instance Only

OES 2 supports only one instance of eDirectory (meaning one tree instance) per server.

If you need two or more instances running on a single server, you must install them on a non-OES server, such as SLES 10.

6.4.4 Default Static Cache Limit Might Be Inadequate

The eDirectory install in OES 2 SP1 Linux sets a default static cache of 64 MB if an `_ndsdb.ini` file is not present in the `dib` directory.

To improve performance, you can adjust the cache parameter in the `_ndsdb.ini` file after the install to meet your eDirectory performance requirements, depending on the database size and available system RAM. We recommend setting the cache to 200 MB on a 2 GB RAM system and 512 MB on 4 GB RAM system.

6.4.5 Special Characters in Usernames and Passwords

Using special characters in usernames and passwords can create problems when the values are passed during an eDirectory installation or schema extension.

If the username or password contains special characters, such as \$, #, and so on, escape the character by preceding it with a backslash (\). For example, an administrator username of

```
cn=admin$name.o=container
```

must be passed as

```
cn=admin\$name.o=container
```

When entering parameter values at the command line, you can either escape the character or place single quotes around the value. For example:

```
cn=admin\$name.o=container
```

or

```
'cn=admin$name.o=container'
```

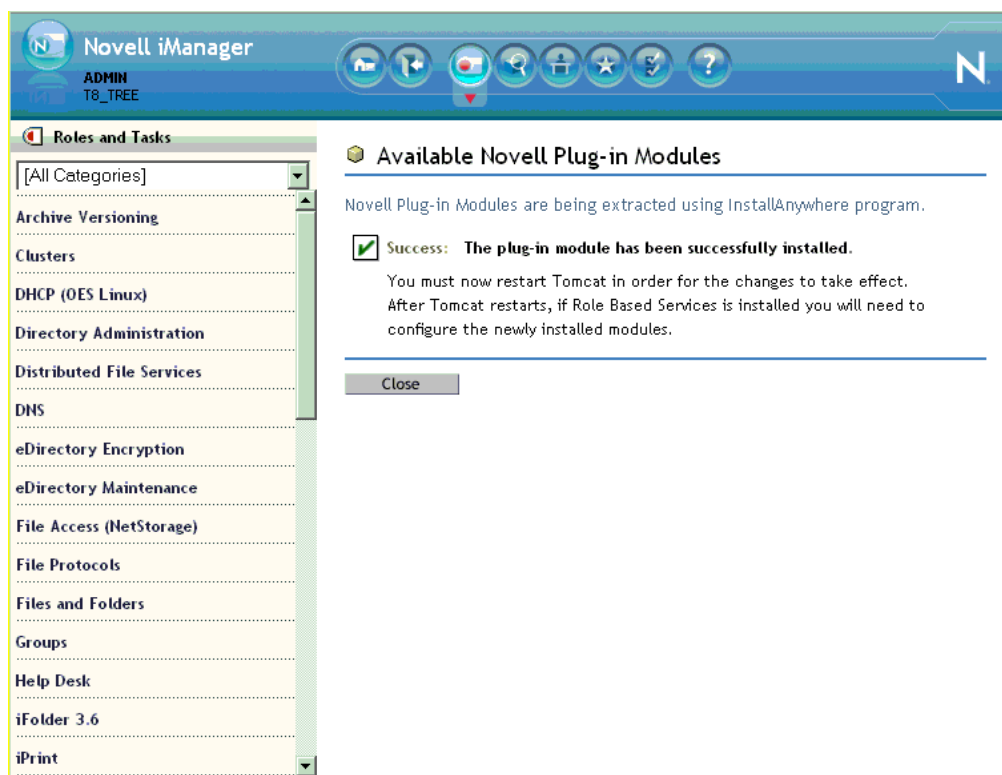
6.5 iManager 2.7

In “Installing RBS” in the *Novell iManager 2.7.2 Administration Guide*, you are instructed to run the iManager Configuration Wizard before using iManager.

When iManager is installed in connection with OES 2, various roles and tasks are configured, as shown in [Figure 6-1](#).

These roles and tasks are available to all the users you create until you run the configuration wizard. After that, the roles and tasks are available only to the Admin user and other users or groups you specifically designate.

Figure 6-1 iManager Roles and Tasks



For more information on iManager, see the *Novell iManager 2.7.2 Administration Guide*.

6.6 iFolder 3.7

Implementation caveats for iFolder 3.7 are documented in “Caveats for Implementing iFolder 3.7 Services” in the *OES 2 SP1: Novell iFolder 3.7 Administration Guide*.

6.7 iPrint

iPrint has the following implementation caveats:

- ♦ Section 6.7.1, “Cluster Failover Between Mixed Platforms Not Supported,” on page 68
- ♦ Section 6.7.2, “Printer Driver Uploading on OES 2 Linux Might Require a CUPS Administrator Credential,” on page 69
- ♦ Section 6.7.3, “Printer Driver Uploading Support,” on page 69
- ♦ Section 6.7.4, “iManager Plug-Ins Are Platform-Specific,” on page 69
- ♦ Section 6.7.5, “iPrint Client for Linux Doesn't Install Automatically,” on page 69
- ♦ Section 6.7.6, “iPrint Disables CUPS Printing on the OES 2 Linux Server,” on page 69

6.7.1 Cluster Failover Between Mixed Platforms Not Supported

Clustered iPrint services can only fail over to the same OES 2 platform (Linux or NetWare).

6.7.2 Printer Driver Uploading on OES 2 Linux Might Require a CUPS Administrator Credential

A PPD is the Linux equivalent of a printer driver on Windows.

There are two versions of the iPrint Client: high security and low security. By default, end users and administrators install the high-security client when using the iPrint Printer List Web page.

This means that administrators are prompted for a CUPS administrator credential when uploading PPDs. However, the prompt doesn't specify that a CUPS administrator credential is needed and the `root` user credential does not work.

6.7.3 Printer Driver Uploading Support

Uploading PPD printer drivers from a Linux workstation requires a Mozilla*-based browser. Only the *Add From System* button works for uploading drivers. Non-Mozilla-based browsers, such as Konqueror, cannot be used to upload drivers.

Uploading PPD printer drivers from a Windows workstation requires Internet Explorer* 5.5 or later. Other browsers running on Windows do not work for uploading drivers.

Windows printer drivers cannot be uploaded by using Mozilla-based or other browsers on any platform.

6.7.4 iManager Plug-Ins Are Platform-Specific

The iManager plug-ins are different for each server platform. Therefore, if you have both OES 2 Linux and OES 2 NetWare servers running iPrint services, you need two instances of iManager to manage iPrint—one on each platform.

6.7.5 iPrint Client for Linux Doesn't Install Automatically

Users who are used to installing the Windows iPrint Client expect to choose an *Open* option and have the client install automatically. However, installing the client on Linux workstations requires you to save the RPM package and then install it manually if a package manager is not already installed and configured as it is in the Novell Linux Desktop. For more information, see “**Linux: iPrint Client**” in the *OES 2 SP1: iPrint for Linux Administration Guide*.

6.7.6 iPrint Disables CUPS Printing on the OES 2 Linux Server

iPrint uses CUPS to render print jobs before sending the print job to the Print Manager. For performance and scalability, printing from the server itself is disabled during the OES installation of iPrint.

6.8 NCP Server (OES 2 Linux)

NSS file attributes and NCP™ services tend to get mixed together in the minds of NetWare administrators. It is important to remember that file and directory attributes are supported and enforced by the file system that underlies an NCP volume, not by the NCP server.

For example, even though the Rename Inhibit attribute appears to be settable in the NCP client interface, if the underlying file system is Linux POSIX (Reiser, etc.) there is no support for the attribute and it cannot be set.

Salvage (undelete) and Purge are other features that are available only on NSS and only where the Salvage attribute has been set (the NSS default). They can be managed in the NCP client and through NetStorage, but they are not available on NCP volumes where the underlying file system is Linux POSIX.

Some administrators assume they can provide NSS attribute support by copying or migrating files, directories, and metadata from an NSS volume to a defined NCP volume on a Linux POSIX partition. However, this doesn't work, because NSS file attributes are only supported on NSS volumes.

6.9 NSS (OES 2 Linux)

EVMS is the only supported volume manager for NSS volumes on OES 2 Linux.

Although some administrators have successfully created NSS volumes on hard disks managed by non-EVMS volume managers, there are serious management and configuration limitations associated with this unsupported implementation. For more information, see [“Using NSS on Devices Managed by Non-EVMS Volume Managers \(Linux\)”](#) in the *OES 2 SP1: NSS File System Administration Guide*.

NOTE: EVMS support is automatic and requires no manual configuration unless NSS is being installed on the device that contains the boot (`/boot`) and root (`/`) partitions (the system device). In that case only you must follow the instructions in [“Installing Linux with EVMS as the Volume Manager of the System Device”](#) in the *OES 2 SP1: Linux Installation Guide*.

6.10 OpenLDAP on OES 2 Linux

You cannot run OpenLDAP on an OES 2 Linux server with eDirectory installed. eDirectory LDAP is required for OES 2 services and uses the same ports as OpenLDAP.

6.11 Samba

For Samba implementation caveats, see [“Samba Caveats”](#) in the *OES2 SP1: Samba Administration Guide*.

6.12 Virtualization Issues

The following are caveats for setting up OES 2 server in Xen VMs:

- ♦ [Section 6.12.1, “eDirectory Fails to Start Automatically,” on page 71](#)
- ♦ [Section 6.12.2, “NSS Considerations,” on page 71](#)
- ♦ [Section 6.12.3, “Always Use Timesync Rather Than NTP,” on page 71](#)

6.12.1 eDirectory Fails to Start Automatically

Although it is somewhat rare, if you install and configure OES 2 (specifically eDirectory) at the command prompt rather than through YaST, eDirectory might fail to start. If this happens, enter the following command at the command prompt:

```
chkconfig -a ndsd
```

6.12.2 NSS Considerations

Make sure you follow these guidelines for using NSS volumes in connection with OES 2 servers running in Xen VMs:

- ♦ **Both Linux and NetWare Platforms:** NSS pools and volumes must be created on only SCSI or Fibre Channel devices. You cannot use a file-based disk image, LVM-based disk image, or an SATA/IDE disk for the virtual machine.
- ♦ **OES 2 Linux:** Data shredding is not supported.

6.12.3 Always Use Timesync Rather Than NTP

Time synchronization problems have been observed when virtualized NetWare servers are running the XNTPD NLM™. Therefore, Novell strongly recommends using Timesync and also configuring the service to communicate through NTP.

6.13 Web Services

The `novell-tomcat` package is installed for Novell service use only. It is an embedded part of Novell services, not a generic application platform.

If you want to deploy a Web application on Tomcat on an OES server, install and use the Tomcat package that comes with SLES 10, not the `novell-tomcat` package.

Upgrading to OES 2

This section provides information and links for upgrading to Open Enterprise Server.

- ♦ [Section 7.1, “Caveats to Consider Before Upgrading,” on page 73](#)
- ♦ [Section 7.2, “OES 2 SP1 Linux Upgrade Paths,” on page 74](#)
- ♦ [Section 7.3, “OES 2 SP1 NetWare Upgrade Paths,” on page 74](#)

7.1 Caveats to Consider Before Upgrading

Be aware of the following caveats when upgrading an OES server:

- ♦ [Section 7.1.1, “About Previously Installed Packages \(RPMs\),” on page 73](#)
- ♦ [Section 7.1.2, “iManager 2.5 Replaced by iManager 2.7 on NetWare,” on page 73](#)
- ♦ [Section 7.1.3, “OES 1 Linux to OES 2 Linux Service Differences,” on page 73](#)
- ♦ [Section 7.1.4, “Only One eDirectory Instance Is Supported on OES Servers,” on page 74](#)
- ♦ [Section 7.1.5, “Virtual Office from NetWare 6.5 to OES 2 NetWare,” on page 74](#)

7.1.1 About Previously Installed Packages (RPMs)

Other Novell® products, such as GroupWise®, and third-party applications that you have installed are treated differently by default when you upgrade an OES Linux server, depending on the version of the server you are upgrading:

- ♦ **OES 1:** Applications are deleted by default during an upgrade.
- ♦ **OES 2:** Applications installed on an OES 2 server are retained, but might not work after upgrading.

To learn more and for instructions on manually changing these options, see “[Planning for the Upgrade to OES 2 SP1](#)” in the *OES 2 SP1: Linux Installation Guide*.

7.1.2 iManager 2.5 Replaced by iManager 2.7 on NetWare

If iManager 2.5 is installed on a NetWare server, and you apply OES 2 NetWare (NetWare 6.5 Support Pack 8), iManager and its associated plug-ins are automatically updated to version 2.7. For more information about iManager 2.7, see the *Novell iManager 2.7.2 Administration Guide*.

If you are using iManager 2.02, iManager is not upgraded.

7.1.3 OES 1 Linux to OES 2 Linux Service Differences

eGuide, Novell iFolder® 2, and Virtual Office are not supported on OES 2 Linux. If you upgrade an OES 1 Linux server with any of these installed to OES 2 SP1 Linux, the services cease to function.

7.1.4 Only One eDirectory Instance Is Supported on OES Servers

If your OES server has multiple instances of eDirectory™ running (multiple trees), any attempt to upgrade the server fails.

You must remove all instances, except the one that uses port 524, prior to an upgrade.

For more information, see [Section 6.4.3, “One Instance Only,” on page 66](#).

7.1.5 Virtual Office from NetWare 6.5 to OES 2 NetWare

All releases of OES NetWare to this point (except OES 1 SP1) have included Virtual Office 1.6. When you upgrade a NetWare 6.5 SP2 or earlier server to one of these support packs, any Virtual Office installations are automatically upgraded to version 1.6.

When you upgrade an existing Virtual Office installation, all data, teams, configurations, etc. are retained with the following exceptions:

- ♦ User Bookmarks are lost
- ♦ E-mail notifications might need to be reconfigured
- ♦ Team File Share credentials might need to be re-created.

7.2 OES 2 SP1 Linux Upgrade Paths

The following are supported upgrade paths for OES 2 SP1 Linux:

Table 7-1 *Supported OES 2 SP1 Linux Upgrade Paths*

Source	Destination
OES 1 SP2 32-bit (Latest Patch Level) (Physical only)	OES 2 SP1 32-bit (Physical only)
OES 2 32-bit (Physical or virtual)	OES 2 SP1 32-bit (Physical or virtual)
OES 2 64-bit (Physical or virtual)	OES 2 SP1 64-bit (Physical or virtual)

NOTE: Physical installations cannot be upgraded to virtual installations, and the reverse is also true. Only physical to physical and virtual to virtual upgrades are supported.

For complete upgrade instructions, see “[Upgrading to OES 2 SP1 Linux](#)” in the *OES 2 SP1: Linux Installation Guide*.

In addition to upgrading the server itself, data and service migrations from OES 1 to OES 2 Linux are also supported. For more information, see the *OES 2 SP1: Migration Tool Administration Guide*.

7.3 OES 2 SP1 NetWare Upgrade Paths

The following are supported upgrade paths to OES 2 SP1 NetWare.

Table 7-2 *Supported OES 2 SP1 NetWare Upgrade Paths*

Source	Destination
Physical NetWare 5.1 SP8	<ol style="list-style-type: none"> 1. Upgrade to OES 1 SP2 NetWare (6.5 SP6). See “Upgrading to NetWare 6.5 SP6” in the <i>OES 2 SP1: NetWare Installation Guide</i>. 2. Upgrade to OES 2 SP1 NetWare (6.5 SP8). See “Upgrading to OES 2 SP1 NetWare” in the <i>OES 2 SP1: NetWare Installation Guide</i>.
Physical OES 1 SP2 or OES 2 NetWare (6.5 SP6 or SP7)	Physical OES 2 SP1 NetWare (6.5 SP8). See “ Upgrading to OES 2 SP1 NetWare ” in the <i>OES 2 SP1: NetWare Installation Guide</i> .
Virtual OES 2 NetWare (6.5 SP7)	Virtual OES 2 SP1 NetWare (6.5 SP8). See “ Upgrading an OES 2 NetWare Guest on a Xen-based VM Host Server ” in the <i>OES 2 SP1: NetWare Installation Guide</i> .

In addition to upgrading the physical server itself, data and service migrations from NetWare to OES 2 Linux are also supported. For more information, see the *OES 2 SP1: Migration Tool Administration Guide*.

Migrating and Consolidating Existing Servers and Data

This section briefly outlines the following migration topics:

- [Section 8.1, “Supported OES 2 SP1 Migration Paths,” on page 77](#)
- [Section 8.2, “Migration Tools and Purposes,” on page 77](#)

8.1 Supported OES 2 SP1 Migration Paths

For a complete list of Open Enterprise Server 2 SP1 migration scenarios and paths, see “[Migration Scenarios](#)” in the *OES 2 SP1: Migration Tool Administration Guide*.

8.2 Migration Tools and Purposes

The following sections briefly explain the purpose of each migration tool/utility included in OES 2 SP1:

- [Section 8.2.1, “OES 2 SP1 Migration Tool,” on page 77](#)
- [Section 8.2.2, “Migrate Windows Shares Utility,” on page 77](#)
- [Section 8.2.3, “NetWare Migration Wizard,” on page 78](#)
- [Section 8.2.4, “Server Consolidation Utility,” on page 78](#)

8.2.1 OES 2 SP1 Migration Tool

The OES 2 SP1 Migration Tool lets you migrate and/or consolidate data and services from one or more NetWare, OES 1, or OES 2 source servers to an OES 2 SP1 Linux target server. The source servers must each be running the same platform. Cross-platform consolidations are not directly supported, but can be facilitated as explained in “[Cross-Platform Data Consolidations](#)” in the *OES 2 SP1: Migration Tool Administration Guide*.

You can also transfer a complete server identity, including its IP address, hostname, eDirectory identity, NICI keys, and certificates. For more information, see “[Transfer ID](#)” in the *OES 2 SP1: Migration Tool Administration Guide*.

8.2.2 Migrate Windows Shares Utility

To help you migrate data from Windows NT*, 2000, or 2003 servers to OES 2 SP1 Linux, OES 2 SP1 includes the Migrate Windows Shares utility.

For more information, see “[Migrating Data from Windows to OES 2 SP1 Linux](#)” in the *OES 2 SP1: Migration Tool Administration Guide*.

8.2.3 NetWare Migration Wizard

The primary purposes of the Novell® NetWare® Migration Wizard are

- ♦ To migrate NetWare servers to OES 2 SP1 NetWare (6.5 SP8) and/or to new hardware.
- ♦ To facilitate migrations from older versions of NetWare to NetWare 5.1 SP8, in preparation for migrating to OES 2 SP1 Linux.

After migrating to NetWare 5.1 SP8, servers can then be migrated using the OES 2 SP1 Migration Tool.

When the migration is complete, the new NetWare server replaces and assumes the identity of the old NetWare server on the network.

The supported migration paths to OES 2 SP1 NetWare (6.5 SP8) are listed in “**NetWare Migration Wizard**” in the *Novell Server Consolidation and Migration Toolkit Administration Guide*.

8.2.4 Server Consolidation Utility

The primary purpose of the Server Consolidation Utility is to migrate and consolidate:

- ♦ Users
- ♦ File permissions
- ♦ Passwords
- ♦ File Systems

from existing NetWare servers to OES 2 NetWare (6.5 SP8) servers.

NOTE: If you are moving a NetWare server to new hardware, use the NetWare Migration Wizard instead.

The Server Consolidation Utility can also be used to

- ♦ Migrate NetWare servers to OES 2 SP1 Linux. However, the primary tool for this purpose is the **OES 2 SP1 Migration Tool**.
- ♦ Migrate and consolidate some Windows servers. However, certain restrictions apply as explained in “**Server Consolidation Utility**” in the *Novell Server Consolidation and Migration Toolkit Administration Guide*. The primary tool for migrating Windows shares to OES 2 SP1 Linux is the **Migrate Windows Shares Utility**.

For more information, see “**Server Consolidation and Migration Overview**” in the *Novell Server Consolidation and Migration Toolkit Administration Guide*.

Virtualization in OES 2

In Open Enterprise Server 2, you can host multiple OES 2 servers on Xen virtual machines (VMs) on a single Xen host server (either OES 2 Linux or SUSE[®] Linux Enterprise Server 10 SP1).

For information about installing and running OES 2 services on Xen-based virtual machines, see the links on the [Virtualization page of the OES 2 Online Documentation](#).

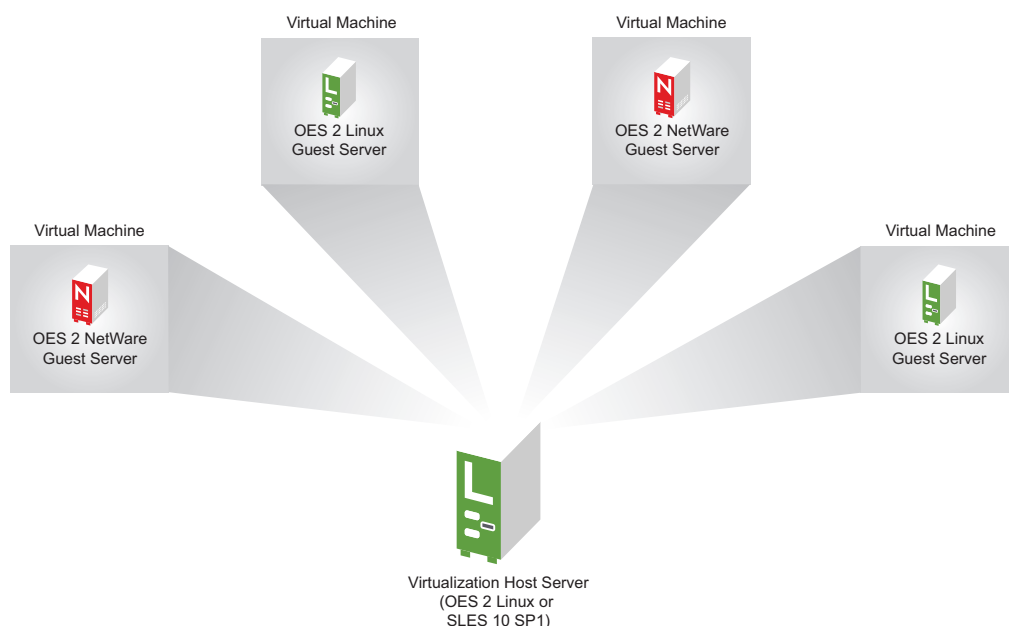
- ♦ [Section 9.1, “Graphical Overview of Virtualization in OES 2,” on page 79](#)
- ♦ [Section 9.2, “Why Install OES Services on Your VM Host?,” on page 80](#)
- ♦ [Section 9.3, “Services Supported on VM Hosts and Guests,” on page 80](#)

IMPORTANT: Although OES 2 NetWare[®] and NetWare 6.5 share the same code base and are the same in every way, virtualized NetWare in Xen is an OES 2 product feature. Support for NetWare on a Xen virtual machine is available only to OES 2 registered customers.

9.1 Graphical Overview of Virtualization in OES 2

Figure 9-1 illustrates how a single VM host server can support multiple VM guest servers that in turn provide OES services.

Figure 9-1 *Xen-Based Virtualization in OES 2*



9.2 Why Install OES Services on Your VM Host?

Novell supports three OES 2 services running on a Xen VM host server: Novell Linux User Management, Novell Storage Management Services, and Novell Cluster Services™. Additionally, whenever you specify OES 2 as an add-on product, the YaST-based NetWare Response File Utility is automatically installed, whether you install any services or not.

Having these components installed on a Xen VM host server provides the following benefits:

- ♦ **Linux User Management (LUM):** Lets you SSH into the server for management purposes by using an eDirectory™ user account.

This functionality requires that you

- ♦ Enable SSH communications through any firewalls that are running on the server
- ♦ Configure LUM to allow SSH as a LUM-enabled service. For more information see “[SSH Services on OES 2 Linux](#)” in the *OES 2 SP1: Planning and Implementation Guide*
- ♦ **Storage Management Services (SMS):** Lets you back up the VM host server and all of the VM guests.
- ♦ **Novell Cluster Services (NCS):** Lets you cluster the VM guests running on the VM host.
- ♦ **NetWare Response File Utility:** Lets you pre-answer the same questions as you would during a physical NetWare installation. When the time comes to run the NetWare Install program, the installation reads your responses from the file and proceeds without requiring further intervention.

9.3 Services Supported on VM Hosts and Guests

As you plan your virtualization configurations, you will want to consider which services are supported where [Table 9-1](#) and which combinations of services are supported (see [Section 3.10.15](#), “[Unsupported Service Combinations](#),” on page 43).

Table 9-1 *Services Supported on VM Hosts and Guests*

OES 2 Service	Linux VM Host	Linux VM Guest	NetWare VM Guest
AFP (Novell AFP)		✓	✓
Backup/SMS	✓	✓	✓
CIFS (Novell CIFS)		✓	✓
Cluster Services	✓ (non-NSS and Xen templates only)	✓	✓
DHCP		✓	✓
DNS		✓	✓
Domain Services for Windows (DSfW)		✓	
eDirectory		✓	✓
FTP		✓	✓

OES 2 Service	Linux VM Host	Linux VM Guest	NetWare VM Guest
Novell iFolder®		✓ (3.7)	✓ (2.1x)
iManager		✓	✓
iPrint		✓	✓
Linux User Management ✓		✓	
NCP Server/Dynamic Storage Technology		✓	
NetStorage		✓	✓
Novell Remote Manager (NRM)		✓	✓
Novell Storage Services™ (NSS)		✓	✓
QuickFinder™		✓	✓
Samba		✓	

IMPORTANT: Adding OES services to a Xen VM host requires that you boot the server with the regular kernel prior to adding the services. See the instructions in the Important note in “[Installing or Configuring OES Services on an Existing Server](#)” in the *OES 2 SP1: Linux Installation Guide*.

Clustering and High Availability

Open Enterprise Server 2 includes support for a two-node Novell® Cluster Services™ cluster.

The full Novell Cluster Services product (available through a separate purchase) is a multinode clustering product that

- ♦ Can include up to 32 servers.
- ♦ Is available for both NetWare® and Linux.
- ♦ Is eDirectory™ enabled for single-point ease of management.
- ♦ Supports failover, failback, and migration (load balancing) of individually managed cluster resources.
- ♦ Supports shared SCSI, iSCSI, and Fibre Channel storage area networks.

For more information, see the topics in “[clustering \(high availability\)](#)” in the OES 2 online documentation.

Managing OES 2

This section includes the following topics:

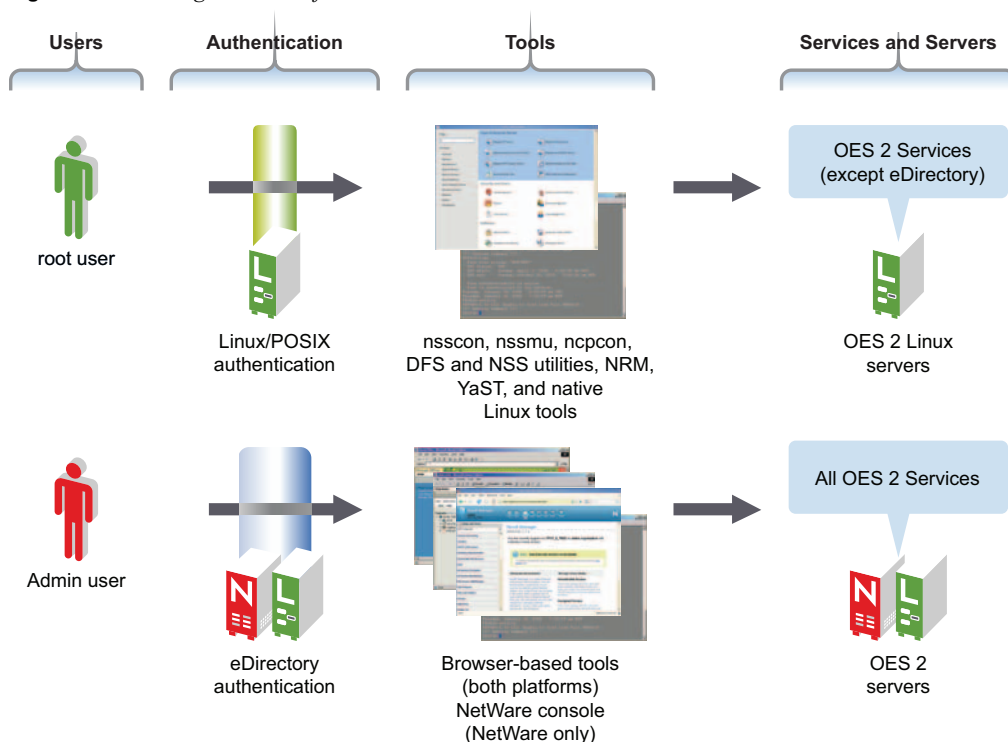
- [Section 11.1, “Overview of Management Interfaces and Services,”](#) on page 85
- [Section 11.2, “Using OES 2 Welcome Pages,”](#) on page 86
- [Section 11.3, “OES Utilities and Tools,”](#) on page 87
- [Section 11.4, “SSH Services on OES 2 Linux,”](#) on page 100

11.1 Overview of Management Interfaces and Services

As shown in [Figure 11-1](#), Open Enterprise Server provides a rich set of service-management and server-management tools, including browser-based and server-based interfaces that help you implement and maintain your network. Access to most of these management interfaces is controlled through eDirectory™. However, a few interfaces, such as YaST on SUSE® Linux Enterprise Server 10 servers, require local authentication.

For more information, see [Section 11.3, “OES Utilities and Tools,”](#) on page 87.

Figure 11-1 Management Interfaces and Services



11.2 Using OES 2 Welcome Pages

After you install an OES 2 server, anyone with browser access to the server can access its Welcome Web site, which is a collection of dynamic Web pages that provides the features illustrated and explained in [Figure 11-2](#).

Figure 11-2 The Default OES Welcome Page



This section explains OES Welcome Web Site features, and discusses:

- [Section 11.2.1, “The Welcome Site Requires JavaScript, Apache, and Tomcat,” on page 86](#)
- [Section 11.2.2, “Accessing the Welcome Web Site,” on page 87](#)
- [Section 11.2.3, “The Welcome Web Site Is Available to All Users,” on page 87](#)
- [Section 11.2.4, “Administrative Access from the Welcome Web Site,” on page 87](#)

11.2.1 The Welcome Site Requires JavaScript, Apache, and Tomcat

Browsers accessing the Welcome site must have JavaScript* enabled to function correctly.

Additionally, it is possible to install OES 2 on either supported platform without including the Apache Web Server or the Tomcat Servlet Container. For example, if you install OES 2 NetWare® by using the *Customized NetWare Server* option, neither of these components is selected by default. For OES 2 Linux, the Apache server and Tomcat container are included with many of the server patterns, but not all of them.

If you are unable to access the Welcome Web site, your server is probably missing one or both of these required components. To make the site available, you need to add the components to the OES 2 server.

11.2.2 Accessing the Welcome Web Site

Anyone with browser access to an OES 2 server can access the Welcome site by doing the following:

- 1 Open a **supported Web browser** that has a TCP connection to the network where the OES 2 server is installed.
- 2 Enter the URL to the server, using HTTP.

For example:

```
http://server.example.com/welcome
```

or

```
http://192.168.1.206/welcome
```

IMPORTANT: By default, the Welcome site is accessible by entering only the DNS name or IP address without the path to /welcome as the URL. However, this behavior changes as follows:

- On NetWare, the `sys:/apache2/htdocs/index.html` file redirects requests to the Welcome site page. If the file is changed, then the behavior reflects the changes made.
- On Linux, the Welcome site displays only when there is no `index.html` file in `/srv/www/htdocs`. For example, installing the Web and LAMP Server pattern installs a page that says “It Works!” and the Welcome site is not displayed.

In these cases the complete path is required (including /welcome) to access the Welcome site.

11.2.3 The Welcome Web Site Is Available to All Users

Although the Welcome Web site is designed primarily for administrators, it can also be accessed and used by end users. For example, if iPrint is installed on the server, users can install the iPrint Client by clicking the *Client Software* link and selecting the appropriate client.

11.2.4 Administrative Access from the Welcome Web Site

Administrators can access any of the administrative tools installed on the server by clicking the Management Services link, selecting the tool they want to use, and entering the required authentication information.


11.3 OES Utilities and Tools

Novell® OES 2 includes several administration utilities that let you manage everything in your network, from configuring and managing eDirectory to setting up network services and open source software. This section lists and briefly explains the most common utilities.

Whenever possible, we recommend that all OES management be performed by using browser-based tools. This ensures that all the system commands required to execute various tasks are performed in proper order and that none of them is skipped by mistake.

Table 11-1 is a quick reference for accessing information about the OES management tools. Specific instructions for the tasks listed are located in the administration guides and other documentation for the services that each tool manages.

Table 11-1 OES Management Tool Quick Reference

Tool	Tasks	Access Method or URL/ Username	Notes
Apache Manager	<ul style="list-style-type: none"> ♦ Control one or many Apache Web servers on any platform from a single management interface. ♦ Greatly reduce the risk of configuration errors. 	<p>To access Apache Manager from the Welcome Web site:</p> <ol style="list-style-type: none"> 1. Open the Welcome Web site on an OES 2 NetWare server using your server's URL. For example, <code>http://myserver.example.com</code>. 2. Log in as the eDirectory Admin user. 3. In the left frame, click the  icon next to Open Source, then click <i>Apache 2.0</i>. 4. After the Apache 2.0 Welcome page loads, in the upper right link box, click either <i>Administer Single Apache Server</i> or <i>Administer Multiple Apache Servers</i>. 	<p>Runs only from NetWare, but can configure Apache Web servers on multiple platforms.</p> <p>For more information on using Apache Manager, see the <i>Apache Web Server for NetWare Administration Guide for OES</i>.</p>
bash (Linux)	<ul style="list-style-type: none"> ♦ Manage the Linux server. ♦ Manage many services running on the server. 	Access a command prompt on the Linux server.	For more information or help understanding and using bash, search the Web for any of the numerous articles and tutorials on using the shell.

Tool	Tasks	Access Method or URL/ Username	Notes
BASH (NetWare)	<ul style="list-style-type: none"> Perform a subset of BASH commands. 	<p>To start the shell at a NetWare console prompt, enter</p> <pre>bash.nlm</pre>	<p>To learn more about using the BASH commands on NetWare, see the man pages available at the command prompt by entering</p> <pre>man bash</pre> <p>For more information, see “BASH” in the <i>OES 2 SP1: Utilities Reference for NetWare</i>.</p> <p>To obtain the source files for this version of BASH on NetWare, visit forge.novell.com (http://forge.novell.com).</p>
ConsoleOne® (NetWare)	<ul style="list-style-type: none"> Manage eDirectory objects, schema, partitions, and replicas. Manage NetWare server resources. 	<ol style="list-style-type: none"> Do either of the following: From a workstation, map a drive to the NetWare server and run <code>consoleone.exe</code> from <code>sys:\public\mgmt\consoleone\1.2\bin.</code> or From a NetWare server console, click the Novell menu and select ConsoleOne from the list of options. Specify the eDirectory Admin username and password. 	<p>IMPORTANT: If you are running ConsoleOne on a server that runs iManager 2.7, you must install ConsoleOne 1.3.6h or later. Otherwise, iManager will experience JClient errors.</p> <p>For more information about ConsoleOne, see the <i>ConsoleOne 1.3.x User Guide</i>.</p>

Tool	Tasks	Access Method or URL/ Username	Notes
Health Monitoring Services	<ul style="list-style-type: none"> ♦ Monitor the health of Linux or NetWare servers. 	<ol style="list-style-type: none"> 1. In a supported Web browser, access Novell Remote Manager by entering <code>http://IP_Address:8008</code> 2. Specify the eDirectory Admin username and password, or on Linux you can use the <code>root</code> user and password if needed. 3. Click <i>Health Monitor</i> under <i>Diagnose Server</i>. 	<p>Functionality is limited for non-Admin or non-<code>root</code> users on both platforms.</p> <p>NRM on Linux doesn't include all the functionality of NRM on NetWare.</p> <p>For more information, see the <i>OES 2 SP1: Novell Remote Manager for NetWare Administration Guide</i> or the <i>OES 2 SP1: Novell Remote Manager for Linux Administration Guide</i>.</p> <p>Health Monitoring Services on OES 2 Linux use a Common Information Model (CIM) provided by the Web-Based Enterprise Management (WBEM) Initiative. For more information on WBEM, visit the DMTF Web site (http://www.dmtf.org/standards/wbem).</p>
iManager 2.7	<ul style="list-style-type: none"> ♦ Access various other management tools and plug-ins. ♦ Configure OES network services. ♦ Create and manage users, groups, and other objects. ♦ Delegate administration through Role-Based Services (RBS). ♦ Manage eDirectory objects, schema, partitions, and replicas. ♦ Manage NetWare 6.5 servers. ♦ Manage OES 2 services on both Linux and NetWare. ♦ Set up and manage your Novell eDirectory tree. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: <code>http://IP_or_DNS/iManager.html</code> 2. Specify the eDirectory Admin username and password. 	<p>Requires an SSL connection (HTTPS).</p> <p>Both HTTP and HTTPS requests establish the SSL connection.</p> <p>For more information on using iManager, see the <i>Novell iManager 2.7.2 Administration Guide</i>.</p> <p>See also <i>iManager Workstation</i>.</p>

Tool	Tasks	Access Method or URL/ Username	Notes
iManager Workstation (formerly Mobile iManager)	<ul style="list-style-type: none"> ♦ Manage eDirectory. ♦ Create and manage users, groups, and other objects. ♦ Manage OES 2 services. ♦ Access various other management tools and plug-ins. 	<p>On a Linux workstation:</p> <ol style="list-style-type: none"> 1. At the <code>bin</code> directory of the expanded <code>iMan_25_Mobile_iManager_linux.tar</code> directory, run <code>imanager.sh</code>. 2. Log in, using the eDirectory Admin username, password, and eDirectory tree name. <p>On a Windows workstation:</p> <ol style="list-style-type: none"> 1. At the <code>bin</code> directory of the unzipped <code>iMan_25_Mobile_iManager_win</code> directory, run <code>imanager.bat</code>. 2. Log in, using the eDirectory Admin username, password, and eDirectory tree name. 	<p>Requires an SSL connection (HTTPS).</p> <p>Both HTTP and HTTPS requests establish the SSL connection.</p> <p>For more information on using iManager Workstation, see “Accessing iManager Workstation” in the <i>Novell iManager 2.7.2 Administration Guide</i>.</p> <p>See also iManager.</p>
iMonitor	<ul style="list-style-type: none"> ♦ Monitor and diagnose all the servers in your eDirectory tree. ♦ Examine eDirectory partitions, replicas, and servers. ♦ Examine current tasks taking place in the tree. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter one of the following URLs: (On NetWare) <code>http://IP_or_DNS:81/nds</code> (On Linux) <code>https://IP_or_DNS:8030/nds</code> 2. Specify the eDirectory Admin username and password. 	<p>iMonitor provides a Web-based alternative to tools such as DSBrowse, DSTrace, DSdiag, and the diagnostic features available in DSRepair.</p> <p>Because of this, iMonitor's features are primarily server focused, meaning that they report the health of individual eDirectory agents (running instances of the directory service) rather than the entire eDirectory tree.</p> <p>For more information, see “Using Novell iMonitor 2.4” in the <i>Novell eDirectory 8.8 Administration Guide</i>.</p>

Tool	Tasks	Access Method or URL/ Username	Notes
INETCFG (NetWare)	<ul style="list-style-type: none"> ♦ Manage network and server TCP/IP communications. ♦ Manage IP addresses. ♦ Bind boards on a NetWare server. 	<ol style="list-style-type: none"> 1. Load the inetcfg NLM™ at a NetWare System Console prompt. 2. Access the server console. 3. Toggle to the screen. 	For more information, see “INETCFG” in the <i>OES 2 SP1: Utilities Reference for NetWare</i> .
IP Address Manager (NetWare)	<ul style="list-style-type: none"> ♦ Manage the IP address-application association when changing the NetWare server’s IP address. ♦ Resolve IP address and port conflicts. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: https:// IP_or_DNS:8009/ ipmcfg 2. Specify the eDirectory Admin username and password. 	For more information, see the <i>OES 2 SP1: Novell IP Address Management for NetWare Administration Guide</i> .
iPrint Map Designer	<ul style="list-style-type: none"> ♦ Create a printer map to aid in printer selection/installation. ♦ Edit an existing printer map. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: http:// IP_or_DNS/ ippdocs/ maptool.htm 2. Specify the eDirectory Admin username and password. 	<p>For OES 2 Linux server instructions, see “Setting Up Location-Based Printing” in the <i>OES 2 SP1: iPrint for Linux Administration Guide</i>.</p> <p>For OES 2 NetWare server instructions, see “Setting Up Location-Based Printing” in the <i>OES 2 SP1: iPrint Administration Guide for NetWare</i>.</p>
MySQL 4.0 (phpMyAdmin) (NetWare)	<ul style="list-style-type: none"> ♦ Create and manage MySQL databases. ♦ Monitor processes. ♦ Export databases. ♦ Create and manage user accounts. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: https:// IP_or_DNS:2200/ phpMyAdmin/ index.php 2. Specify the eDirectory Admin username and password. 	For more information, see the <i>OES 2 SP1: Novell MySQL for NetWare Administration Guide</i> .

Tool	Tasks	Access Method or URL/ Username	Notes
NetStorage Web Interface	<ul style="list-style-type: none"> ♦ Manage file system access. ♦ Manage file system space restrictions. ♦ Salvage and purge deleted files. 	Use the NetStorage Web interface.	<p>As an Admin user (or equivalent), you can set directory and user quotas for NSS data volumes. You can also set file system trustees, trustee rights, and attributes for directories and files on NSS volumes. And you can salvage and purge deleted files.</p> <p>For more information, see either of the following:</p> <ul style="list-style-type: none"> ♦ “Viewing or Modifying Directory and File Attributes and Rights” in the <i>OES 2 SP1: NetStorage for Linux Administration Guide</i>. ♦ “Viewing or Modifying Directory and File Attributes and Rights” in the <i>OES 2: NetStorage for NetWare Administration Guide</i>.
NetWare Command Line Utilities	<ul style="list-style-type: none"> ♦ Manage and configure all aspects of the NetWare operating system. ♦ Manage many of the network services that NetWare hosts. 	Enter the commands at the server console or through a remote connection.	For more information, see the <i>OES 2 SP1: Utilities Reference for NetWare</i> .
Novell Client	<ul style="list-style-type: none"> ♦ Manage file system access. ♦ Manage File System Space Restrictions. ♦ Salvage and purge deleted files. 	Use the Novell N icon to access these and other tasks.	<p>As an Admin user (or equivalent), you can set directory and user quotas for NSS data volumes. You can also set file system trustees, trustee rights, and attributes for directories and files on NSS volumes. And you can salvage and purge deleted files.</p> <p>For more information, see “Managing File Security and Passwords” in the <i>Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide</i>.</p>

Tool	Tasks	Access Method or URL/ Username	Notes
Novell iFolder® 3.7	<ul style="list-style-type: none"> ♦ Manage various aspects of iFolder 3.7. 	<ol style="list-style-type: none"> 1. In iManager 2.7, click <i>iFolder 3.7 > Launch iFolder Admin Console</i>. 	<p>For more information on managing iFolder 3.7, see the following in the <i>OES 2 SP1: Novell iFolder 3.7 Administration Guide</i>:</p> <ul style="list-style-type: none"> ♦ <i>iFolder Enterprise Server</i> ♦ <i>iFolder Services via Web Admin</i> ♦ <i>iFolder Users</i> ♦ <i>iFolder Web Access Server</i> ♦ <i>Managing iFolders</i>
Novell Remote Manager (NRM)	<ul style="list-style-type: none"> ♦ Manage file system access and attributes for the NetWare Traditional File System and the NSS File System on NetWare. ♦ Manage the NCP™ Server (Linux) ♦ Manage NCP connections to NSS and NCP volumes (Linux) ♦ Manage Dynamic Storage Technology (Linux) ♦ Manage NetWare Traditional File Systems (NetWare). ♦ Manage OES 2 servers from a remote location. ♦ Monitor your server's health. ♦ Change server configurations. ♦ Perform diagnostic and debugging tasks. ♦ View volume inventories (Linux) 	<ol style="list-style-type: none"> 1. In a <i>supported Web browser</i>, enter the following URL: <code>https:// IP_or_DNS:8009</code> 2. Do one of the following: <ul style="list-style-type: none"> ♦ On NetWare, specify the eDirectory username and password. ♦ On Linux, specify either the eDirectory username and password or a Linux (POSIX) username and password. 	<p>Functionality is limited for non-Admin or non-root users on both platforms.</p> <p>NRM on Linux doesn't include all the functionality of NRM on NetWare.</p> <p>For more information, see the <i>OES 2 SP1: Novell Remote Manager for NetWare Administration Guide</i> or the <i>OES 2 SP1: Novell Remote Manager for Linux Administration Guide</i>.</p>

Tool	Tasks	Access Method or URL/ Username	Notes
NSS Management Utility (NSSMU)	<ul style="list-style-type: none"> Manage the Novell Storage Services™ file system. 	<p>At the NetWare System Console prompt:</p> <ol style="list-style-type: none"> 1. Load the NSSMU NLM. 2. Access the server console. 3. Toggle to the screen. <p>At the Linux command prompt:</p> <ol style="list-style-type: none"> 1. Load NSSMU by entering /opt/novell/ nss/sbin/nssmu 	<p>NSS Management Utility (NSSMU) is a server console application used to manage the Novell Storage System (NSS) logical file system.</p> <p>The Snapshot function in NSSMU on Linux is not available in NSSMU on NetWare. Use iManager to create snapshots for NetWare or Linux.</p> <p>For more information, see “NSS Management Utility (NSSMU) Quick Reference” in the OES 2 SP1: NSS File System Administration Guide.</p>
OpenSSH (client access)	<ul style="list-style-type: none"> Securely run commands on remote servers. Securely copy files and directories to and from other servers using SSH utilities. 	<p>Connect to the server using your favorite SSH client.</p>	<p>On Linux, OpenSSH is installed by default and is accessed by eDirectory users as a LUM-enabled service. For more information, see Section 11.4, “SSH Services on OES 2 Linux,” on page 100.</p> <p>On OES 2 NetWare, load <code>sshd.nlm</code> at the server console.</p> <p>To use OpenSSH from a workstation on your network, you must download one of several available third-party SSH utilities, such as PuTTY. For more information, see “Setting Up SSH at Workstations” in the OpenSSH Administration Guide.</p>
OpenSSH (Linux)	<ul style="list-style-type: none"> Manage a SLES 10 SP1 (OES 2) server by using OpenSSH. 	<ol style="list-style-type: none"> 1. Use standard SSH connection and management options. 	<p>Requirements:</p> <ul style="list-style-type: none"> The firewall must allow for SSH access. eDirectory users must be enabled for SSH access. For more information, see Section 11.4, “SSH Services on OES 2 Linux,” on page 100.

Tool	Tasks	Access Method or URL/ Username	Notes
OpenSSH Advanced Admin (NetWare)	♦ Manage OpenSSH servers as server groups.	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: https:// IP_or_DNS:2200/ sshdadmin/ main.htm 2. Specify the eDirectory Admin username and password. 	For more information, see “Setting Up OpenSSH in Your Network” in the <i>OpenSSH Administration Guide</i> .
OpenSSH Simple Admin (NetWare)	♦ Manage all aspects of a single OpenSSH server.	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: https:// IP_or_DNS:2200/ sshdadmin/ WebMan?file=webman.xml 2. Specify the eDirectory Admin username and password. 	For more information, see “Setting Up OpenSSH in Your Network” in the <i>OpenSSH Administration Guide</i> .
OpenWBEM	♦ Perform tasks instrumented by specific providers.	<p>On NetWare, access sys\system\cimom\etc\openwbem\openwbem.conf.</p> <p>On Linux, access /etc/openwbem.</p>	For more information, see the <i>OES 2 SP1: OpenWBEM Services Administration Guide</i> .
Perl	<p>A programming language developed by Larry Wall that</p> <ul style="list-style-type: none"> ♦ Runs faster than shell script programs. ♦ Reads and writes binary files. ♦ Processes very large files. ♦ Lets you quickly develop CGI applications. 	<p>On Linux, install the associated RPM files.</p> <p>On NetWare, refer to the instructions on the Novell Developer Web site (http://developer.novell.com/wiki/index.php/Perl_for_NetWare).</p>	For more information or help understanding and using Perl, search the Web. There are numerous articles and tutorials on using this versatile programming language.

Tool	Tasks	Access Method or URL/ Username	Notes
QuickFinder™ Server Manager	<ul style="list-style-type: none"> ♦ Create search indexes for any Web site or attached file systems. ♦ Modify the search dialog look-and-feel to match your corporate design. Create full-text indexes of HTML, XML, PDF, Word, OpenOffice.org, and many other document formats. ♦ Configure and maintain your indexes remotely from anywhere on the Net. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: http:// IP_or_DNS/ qfsearch/admin 2. Do one of the following: <ul style="list-style-type: none"> ♦ On NetWare, specify the eDirectory Admin user and password. ♦ On Linux, specify the root or other user as documented. 	<p>Local users and any eDirectory users that are enabled for Linux access (LUM) can be assigned rights to manage QuickFinder.</p> <p>For more information, see the <i>QuickFinder 5.0 Server Administration Guide</i>.</p>
RConsoleJ (NetWare)	<ul style="list-style-type: none"> ♦ Access NetWare servers remotely. ♦ Run server utilities from a workstation. 	<ol style="list-style-type: none"> 1. Load the rconag6 NLM™ on the NetWare server. 2. At a workstation, map a drive to the server and run rconj.exe from sys:\public\mgmt\consoleone\1.2. 3. When prompted, enter the server's IP address or DNS name (with no leading protocol identifier, such as http or https) and your administrator password, then click <i>Connect</i>. 	<p>For more information, see “Managing NetWare Servers Remotely” in the <i>OES 2: Remote Server Management for NetWare Administration Guide</i>.</p>
Remote Manager			See Novell Remote Manager .

Tool	Tasks	Access Method or URL/ Username	Notes
SNMP for eDirectory	<p>Lets you use standard SNMP tools to</p> <ul style="list-style-type: none"> ♦ Monitor an eDirectory server. ♦ Track the status of eDirectory to verify normal operations. ♦ Spot and react to potential problems when they are detected. ♦ Configure traps and statistics for selective monitoring. ♦ Plot a trend on the access of eDirectory. ♦ Store and analyze historical data that has been obtained through SNMP. ♦ Use the SNMP native master agent on all eDirectory platforms. 	<ol style="list-style-type: none"> 1. Configure SNMP for eDirectory as documented for your platform. 2. Access SNMP for eDirectory services using the SNMP management interface of your choice. 3. Specify the eDirectory Admin username and password. 	<p>SNMP support is installed with eDirectory.</p> <p>For more information on SNMP for eDirectory, see “SNMP Support for Novell eDirectory” in the <i>Novell eDirectory 8.8 Administration Guide</i>.</p>
SUSE® Linux Monitoring Utilities	<ul style="list-style-type: none"> ♦ Manage the Linux server and standard Linux services from the command prompt. 	Enter the desired command at the command prompt.	<p>For more information, see “System Monitoring Utilities” (http://www.novell.com/documentation/sles10/sles_admin/data/cha_util.html) in the <i>SLES 10 SP2: Installation and Administration Guide</i> (http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html).</p>

Tool	Tasks	Access Method or URL/ Username	Notes
TCP/IP Configuration (NetWare - NRM)	<ul style="list-style-type: none"> ♦ Add a new network card. ♦ Associate TCP/IP with a specific network card. ♦ Edit system files. ♦ Enable and configure TCP/IP. ♦ Configure network management parameters. ♦ Copy configuration information to or from a diskette. ♦ Modify the hardware parameters of an existing network card. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: https:// IP_or_DNS:8009/ webcfg 2. Specify the eDirectory Admin username and password. 	For more information, see "Monitoring TCP/IP Information" in the <i>OES 2 SP1: Novell TCP/ IP for NetWare Administration Guide</i> .
TCP/IP Protocol Information (NetWare - NRM)	<ul style="list-style-type: none"> ♦ Monitor protocol information. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: https:// IP_or_DNS:8009/ protocols 2. Specify the eDirectory Admin username and password. 	For more information, see "Web-Based TCP/IP Monitoring" in the <i>OES 2 SP1: Novell TCP/ IP for NetWare Administration Guide</i> .
Tomcat Admin (NetWare)	<ul style="list-style-type: none"> ♦ Manage the Tomcat servlet container on a NetWare server. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: https:// IP_or_DNS/ tomcat/admin/ index.jsp 2. Specify the eDirectory Admin username and password. 	For more information, see "Managing Web Applications and Servlets" in the <i>Tomcat for NetWare Administration Guide for OES</i> .

Tool	Tasks	Access Method or URL/ Username	Notes
Tomcat Manager (NetWare)	<ul style="list-style-type: none"> Install and deploy Web applications. 	<ol style="list-style-type: none"> In a supported Web browser, enter the following URL: <pre>http:// IP_or_DNS/ tomcat/manager/ html/list</pre> Specify the eDirectory Admin username and password. 	For more information, see “ Managing Tomcat with Tomcat Admin ” in the <i>Tomcat for NetWare Administration Guide for OES</i> .
YaST (SUSE Linux)	<ul style="list-style-type: none"> Install OES 2 Linux. Configure the server and standard Linux services. Install OES components and services. 	<p>To access YaST from the GNOME* interface, start the YaST Control Center by clicking <i>Computer</i> > <i>YaST</i>.</p> <p>To access YaST at a command prompt, enter <i>yast</i>.</p>	For more information, see “ Installation with YaST ” (http://www.novell.com/documentation/sles10/sles_admin/data/cha_inst.html) and “ System Configuration with YaST ” (http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast2.html) in the <i>SLES 10 SP2: Installation and Administration Guide</i> (http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html).

11.4 SSH Services on OES 2 Linux

This section documents the following topics:

- [Section 11.4.1, “Overview,” on page 100](#)
- [Section 11.4.2, “Setting Up SSH Access for LUM-enabled eDirectory Users,” on page 102](#)

11.4.1 Overview

SSH (<http://www.novell.com/company/glossary.html#4187>) services on SLES 10 are provided by OpenSSH (<http://www.openssh.org>), a free version of SSH connectivity tools developed by the OpenBSD Project (<http://www.openbsd.org/>).

Linux administrators often use SSH to remotely access a server for management purposes, such as executing shell commands, transferring files, etc. Because many OES 2 Linux services can be managed at a command prompt via an SSH session, it is important to understand how SSH access is controlled in OES 2 Linux.

This section discusses the following topics:

- [“When Is SSH Access Required?” on page 101](#)

- ♦ “How SSH Access for eDirectory Users Works” on page 101
- ♦ “SSH Security Considerations” on page 102

When Is SSH Access Required?

SSH access is required for the following:

- ♦ **SSH administration access for eDirectory users:** For eDirectory users to manage the server through an SSH connection, they must have SSH access as **LUM-enabled users** (eDirectory users configured for access to Linux services).

NOTE: The standard Linux `root` user is a local user, not an eDirectory user. The `root` user always has SSH access as long as the firewall allows it.

- ♦ **Access to NSS Volume Management in NetStorage:** When an OES 2 Linux server has NSS volumes, eDirectory contains an object named *nssvolumes* that provides management access to the volumes through the File Access (NetStorage) iManager plug-in. Using the plug-in to manage NSS volumes, assign trustee rights, salvage and purge files, etc. requires SSH access to the server.

Although eDirectory administrators can create Storage Location Objects to the NSS volumes without SSH access, providing that they know the path to the volume on the POSIX file system and other volume information, having SSH access makes administering NSS volumes in NetStorage much easier.

- ♦ **Access to any NetStorage Storage Location Objects based on SSH:** The NetStorage server provides Web access to directories and files on other servers (or on itself).

Typically, either an NCP or a CIFS connection is used for connecting the NetStorage server with storage targets. However, an SSH connection can also be used, and if it is, the users accessing data through the connection must have SSH access to the data on the target servers.

How SSH Access for eDirectory Users Works

For eDirectory users, the following work together to control SSH access:

- ♦ **Firewall:** As mentioned, the default firewall configuration on an OES 2 Linux server doesn't allow SSH connections with the server. This restricts the `root` user as well. Therefore, the first requirement for SSH access is configuring the firewall to allow SSH services.
- ♦ **Linux User Management (LUM) must allow SSH as a service:** In OES 2 Linux, access to SSH and other Linux services is controlled through Linux User Management (LUM), and each service must be explicitly included in the LUM configuration on each server.
- ♦ **LUM-enabling:** After SSH is included as a LUM-enabled service on a server, at least one group and its users must be enabled for LUM. Only LUM-enabled eDirectory users can have SSH access.
- ♦ **All eDirectory Groups must allow access:** SSH access is inherited from the LUM-enabled groups that a user belongs to, and access is only granted when all of the groups to which a user belongs allow it.
- ♦ **The Samba connection:** Users who are enabled for Samba (CIFS) file services are added by default to an OES-created Samba group that:
 - ♦ Is LUM-enabled.
 - ♦ Doesn't specify SSH as an allowed service.

Therefore, because SSH access requires that all of a user's groups must all allow access, Samba users are denied SSH access unless

- ♦ The user is removed from the Samba group.
- or
- ♦ The Samba group is modified to allow SSH access for all Samba users.

SSH Security Considerations

Remember that SSH access lets users browse and view most directories and files on a Linux server. Even though users might be prevented from modifying settings or effecting other changes, there are serious security and confidentiality issues to consider before granting SSH access to anyone.

11.4.2 Setting Up SSH Access for LUM-enabled eDirectory Users

If you need to grant SSH access to an eDirectory user, complete the instructions in the following sections in order, as they apply to your situation.

- ♦ [“Allowing SSH Access Through the Firewall” on page 102](#)
- ♦ [“Adding SSH as an Allowed Service in LUM” on page 102](#)
- ♦ [“Enabling Users for LUM” on page 103](#)
- ♦ [“Restricting SSH Access to Only Certain LUM-Enabled Users” on page 103](#)
- ♦ [“Providing SSH Access for Samba Users” on page 104](#)

Allowing SSH Access Through the Firewall

- 1 On the OES 2 Linux server you are granting access to, open the YaST Control Center and click *Security and Users > Firewall*.
- 2 In the left navigation frame, click *Allowed Services*.
- 3 In the *Allowed Services* drop-down list, select *SSH*.
- 4 Click *Add > Next > Accept*.

The firewall is now configured to allow SSH connections with the server.

Adding SSH as an Allowed Service in LUM

- 1 If SSH is already an allowed service for Linux User Management on the server, skip to [“Enabling Users for LUM” on page 103](#).
- or
- If SSH is not an allowed service for Linux User Management on the server, continue with [Step 2](#).
- 2 On the OES 2 Linux server, open the YaST Control Center; then, in the *Open Enterprise Server* group, click *OES Install and Configuration*.
- 3 Click *Accept*.
- 4 When the Novell Open Enterprise Server Configuration screen has loaded, click the *Disabled* link under *Linux User Management*.

The option changes to *Enabled* and the configuration settings appear.

- 5 Click *Linux User Management*.
- 6 Type the eDirectory Admin password in the appropriate field, then click *OK > Next*.
- 7 In the list of allowed services, click *sshd*.
- 8 Click *Next > Next > Finish*.

Each LUM-enabled group in eDirectory, except the system-created Samba group, now shows SSH as an allowed service. The Samba group shows the service as not allowed (or literally speaking, *sshd* is not checked).

Enabling Users for LUM

There are numerous ways to enable users for LUM.

For example, in iManager > *Linux User Management* there are options for enabling users (and choosing a Group in the process) or enabling groups (and enabling users in the process). Linux enabling is part of the process required for Samba access. And finally, there are also command line options.

For specific instructions, refer to “[Managing User and Group Objects in eDirectory](#)” in the *OES 2 SPI: Novell Linux User Management Technology Guide*.

After you configure the server’s firewall to allow SSH, add SSH as an allowed service, and LUM-enable the eDirectory users you want to have SSH access, if those same users are not also enabled for Samba on the server, they now have SSH access to the server.

On the other hand, if you have installed Samba on the server, or if you install Samba in the future, the users who are configured for Samba access will have SSH access disabled.

To restore access for users impacted by Samba, see “[Providing SSH Access for Samba Users](#)” on [page 104](#).

Of course, many network administrators limit SSH access to only those who have administrative responsibilities. They don’t want every LUM-enabled user to have SSH access to the server.

If you need to limit SSH access to only certain LUM-enabled users, continue with “[Restricting SSH Access to Only Certain LUM-Enabled Users](#)” on [page 103](#).

Restricting SSH Access to Only Certain LUM-Enabled Users

SSH Access is easily restricted for one or more users by making them members of a LUM-enabled group and then disabling SSH access for that group. All other groups assignments that enable SSH access are then overridden.

- 1 Open iManager in a browser using its access URL:
http://IP_Address/iManager.html
 where *IP_Address* is the IP address of an OES 2 server with iManager 2.7 installed.
- 2 In the *Roles and Tasks* list, click *Groups > Create Group*.
- 3 Type a group name, for example NoSSHGroup, and select a context, such as the container where your other Group and User objects are located. Then click *OK*.
- 4 In the *Roles and Tasks* list, click *Directory Administration > Modify Object*.
- 5 Browse to the group you just created and click *OK*.

- 6 Click the *Linux Profile* tab.
- 7 Select the *Enable Linux Profile* option.
- 8 In the Add UNIX Workstation dialog box, browse to and select the UNIX Workstation objects for the servers you are restricting SSH access to, then click *OK > OK*.
- 9 Click *Apply > OK*.
- 10 In the Roles and Tasks list, click *Modify Object*, browse to the group again, then click *OK*.
- 11 Click the *Other* sub-tab.
- 12 In the *Unvalued Attributes* list, select *uamPosixPAMServiceExcludeList*, then click the left-arrow to move the attribute to the *Valued Attributes* list.
- 13 In the Add Attribute dialog box, click the plus sign (+) next to the empty drop-down list.
- 14 In the *Add item* field, type *sshd*, then click *OK > OK*.
- 15 Click the *Members* tab.
- 16 Browse to and select the User objects that shouldn't have SSH access, then click *OK*.
- 17 Click *Apply > OK*.

Providing SSH Access for Samba Users

There are two options for providing SSH access to users who have been enabled for Samba access:

- ♦ You can remove the user from the *server_name-W-SambaUserGroup*.

IMPORTANT: This presupposes that the user is a member of a different LUM-enabled group that also provides access to the server. If the user was enabled for LUM only as part of a Samba configuration, then removing the user from the Samba group breaks access to Samba and the user does not have SSH access.

- ♦ You can change access for the entire Samba group by moving the *uamPosixPAMServiceExcludeList* attribute from the *Valued Attributes* list to the *Unvalued Attributes* list, using the instructions in [“Restricting SSH Access to Only Certain LUM-Enabled Users” on page 103](#) as a general guide.

NOTE: Although the option to disable SSH access through the *Modify Group* iManager plug-in is much more simple and straightforward, that option is not working as of this writing. Although the plug-in appears to deselect *sshd* as an allowed service, the service is still selected when group information is reloaded. Novell plans to address this issue in the near future.

Network Services

Network services as used in this section, are associated with protocols that provide the following:

- ♦ Data packet transport on the network.
- ♦ Management of IP addresses and DNS names.
- ♦ Time synchronization to make sure that all network devices and eDirectory™ replicas and partitions have the same time.
- ♦ Discovery of network devices and services, such as eDirectory, printers, and so on as required by certain applications, clients, and other services.

This section discusses the following:

- ♦ [Section 12.1, “TCP/IP,” on page 105](#)
- ♦ [Section 12.2, “DNS and DHCP,” on page 106](#)
- ♦ [Section 12.3, “Time Services,” on page 108](#)
- ♦ [Section 12.4, “Discovery Services \(SLP, WinSock, Etc.\),” on page 119](#)
- ♦ [Section 12.5, “SLP,” on page 120](#)

For links to more information and tasks, see the “[Network Protocols](#)” page in the OES 2 online documentation.

12.1 TCP/IP

Network nodes must support a common protocol in order to exchange packets. Transport protocols establish point-to-point connections so that nodes can send messages to each other and have the packets arrive intact and in the correct order. The transport protocol also specifies how nodes are identified with unique network addresses and how packets are routed to the intended receiver.

Open Enterprise Server 2 includes the Novell® TCP/IP stack on NetWare® and standard Linux TCP/IP support on SUSE® Linux Enterprise Server 10. Both comply with the latest RFCs.

12.1.1 Coexistence and Migration Issues

Internetwork Packet Exchange™ (IPX™) was the foundational protocol for NetWare from the 1980s until the release of NetWare 5.0, when support for pure TCP/IP became standard.

Coexistence between IPX and TCP/IP networks is still supported on NetWare, but IPX is not supported on Linux.

Data migration from TCP/IP to IPX is possible. IPX compatibility must be maintained on both the source and destination servers. Applications and services that run only on IPX must be either rewritten or replaced. After all IPX dependencies are resolved, you can safely remove IPX support from your NetWare servers.

For more information on deploying TCP/IP in a NetWare environment, see the *OES 2 SP1: Novell TCP/ IP for NetWare Administration Guide* .

12.2 DNS and DHCP

Domain Name Service (DNS) is the standard naming service in TCP/IP-based networks. It converts IP addresses, such as 192.168.1.1, to human-readable domain names, such as myserver.example.com, and it reverses the conversion process as required.

The Dynamic Host Configuration Protocol (DHCP) assigns IP addresses and configuration parameters to hosts and network devices.

For NetWare, Novell developed directory-integrated DNS/DHCP services that leverage eDirectory to provide centralized configuration and management through a Java* console accessible in iManager.

OES 2 Linux includes a ported version of the NetWare DNS service, and eDirectory integration with ISC DHCP as explained in the sections that follow.

- ♦ [Section 12.2.1, “DNS Differences Between NetWare and OES 2 Linux,” on page 106](#)
- ♦ [Section 12.2.2, “DHCP Differences Between NetWare and OES 2 Linux,” on page 107](#)

12.2.1 DNS Differences Between NetWare and OES 2 Linux

The following are differences between DNS on NetWare and OES 2 Linux:

Table 12-1 DNS: OES 2 NetWare vs. OES 2 Linux

Feature or Command	OES 2 NetWare	OES 2 Linux
Auditing	Yes	No
DNSMaint	Yes	No
Fault Tolerance	Yes	Yes
Filenames and paths:		
♦ Server binary	♦ sys:/system/named.nlm	♦ /opt/novell/named/bin/novell-named
♦ .db, .jnl file	♦ sys:/etc/dns	♦ /etc/opt/novell/named/named.conf
♦ Stat file, info file		♦ /var/opt/novell/log/named/named.run
Console commands:		
♦ Start the server	♦ named	♦ rcnovell-named or novell-named
♦ Stop the server	♦ named stop	♦ rcnovell-named stop
♦ Check Status	♦ named status	♦ rcnovell-named status

Feature or Command	OES 2 NetWare	OES 2 Linux
♦ Unsupported command parameters	♦ N/A	♦ [-dc categories] ♦ [-mstats] ♦ [-nno_of_cpus] ♦ [-qstats]
Journal log size	Specify at the command prompt by using the jsiz argument.	Specify by using the iManager plug-in > <i>max-journal-size</i> field.
Management	iManager Command Line Interface	iManager Command Line Interface Unlike the Netware implementation, command line parameters cannot be passed when loading and unloading.
SNMP Support	Yes	No

12.2.2 DHCP Differences Between NetWare and OES 2 Linux

Table 12-2 DHCP: OES 2 NetWare vs. OES 2 Linux

Feature or Command	OES 2 NetWare	OES 2 Linux
Auditing	Yes	No
Filenames and paths:		
♦ Conf file	♦ N/A	♦ /etc/dhcpd.conf
♦ Leases	♦ Stored in eDirectory	♦ /var/lib/dhcp/db/dhcpd.leases
♦ Log file	♦ sys:/etc/dhcp/dhcpd.log	♦ /var/log/dhcpd.log
♦ Startup log	♦ N/A	♦ /var/log/dhcp-ldap-startup.log This is a dump of DHCP configurations read from eDirectory when the DHCP server starts.
Management	iManager 2.7 (Wizard-based)	iManager 2.7 (Tab-based) Unlike the NetWare implementation, command line parameters cannot be passed when loading and unloading.
Migration	N/A	There is seamless migration support from NetWare.
Schema changes	N/A	There are separate locator and group objects for centralized management and easy rights management.

Feature or Command	OES 2 NetWare	OES 2 Linux
SNMP Support	Yes	No
Subnet naming	Yes	No

12.3 Time Services

The information in this section can help you understand your time services options and set up time synchronization on your OES 2 servers:

- ♦ [Section 12.3.1, “Overview of Time Synchronization,” on page 108](#)
- ♦ [Section 12.3.2, “Planning for Time Synchronization,” on page 112](#)
- ♦ [Section 12.3.3, “Coexistence and Migration of Time Synchronization Services,” on page 115](#)
- ♦ [Section 12.3.4, “Implementing Time Synchronization,” on page 117](#)
- ♦ [Section 12.3.5, “Configuring and Administering Time Synchronization,” on page 118](#)
- ♦ [Section 12.3.6, “Daylight Saving Time,” on page 119](#)

12.3.1 Overview of Time Synchronization

All servers in an eDirectory tree must have their times synchronized to ensure that updates and changes to eDirectory objects occur in the proper order.

eDirectory gets its time from the server operating system (NetWare or Linux) of the OES 2 server where it is installed. It is, therefore, critical that every server in the tree has the same time.

- ♦ [“Understanding Time Synchronization Modules” on page 108](#)
- ♦ [“OES 2 Servers as Time Providers” on page 110](#)
- ♦ [“OES 2 Servers as Time Consumers” on page 111](#)

Understanding Time Synchronization Modules

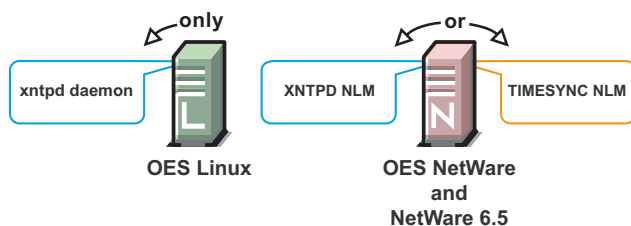
Because your OES eDirectory tree might contain servers running OES 2 Linux, OES 2 NetWare, or previous versions of NetWare, you must understand the differences in the time synchronization modules that each operating system uses and how these modules can interact with each other.

- ♦ [“OES 2 Linux vs. OES 2 NetWare” on page 108](#)
- ♦ [“OES 2 Servers Use the Network Time Protocol \(NTP\) to Communicate” on page 109](#)
- ♦ [“Compatibility with Earlier Versions of NetWare” on page 109](#)

OES 2 Linux vs. OES 2 NetWare

As illustrated in [Figure 12-1](#), OES 2 NetWare (NetWare 6.5) can use either the Network Time Protocol (NTP) or Timesync modules for time synchronization. Both modules can communicate with OES 2 Linux by using NTP. However, when installing virtualized NetWare, Timesync should always be used (see [Section 6.12.3, “Always Use Timesync Rather Than NTP,” on page 71](#)).

OES 2 Linux must use the NTP daemon (xntpd).

Figure 12-1 Time Synchronization for Linux and NetWare

OES 2 Servers Use the Network Time Protocol (NTP) to Communicate

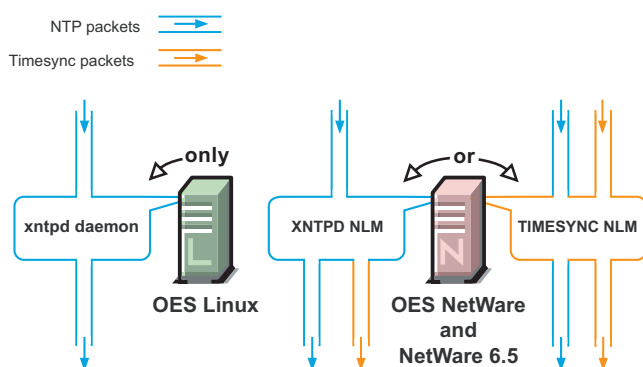
Because OES 2 Linux and NetWare servers must communicate with each other for time synchronization, and because Linux uses only NTP for time synchronization, it follows that both Linux and NetWare must communicate time synchronization information by using NTP time packets.

However, this doesn't limit your options on NetWare.

Figure 12-2 illustrates that OES 2 Linux and NetWare servers can freely interchange time synchronization information because OES 2 NetWare includes the following:

- ♦ A TIMESYNC NLM™ that both consumes and provides NTP time packets in addition to Timesync packets.
- ♦ An XNTPD NLM that can provide Timesync packets in addition to offering standard NTP functionality.

NOTE: Although NetWare includes two time synchronization modules, only one can be loaded at a time.

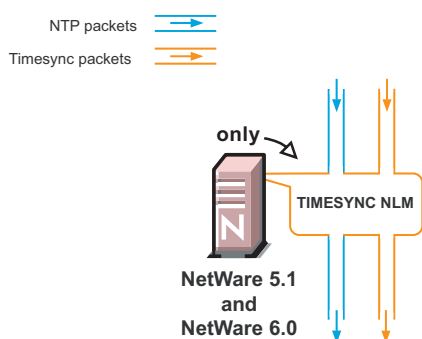
Figure 12-2 NTP Packet Compatibilities with All OES Time Synchronization Modules

Compatibility with Earlier Versions of NetWare

Earlier versions of NetWare (version 4.2 through version 6.0) do not include an NTP time module. Their time synchronization options are, therefore, more limited.

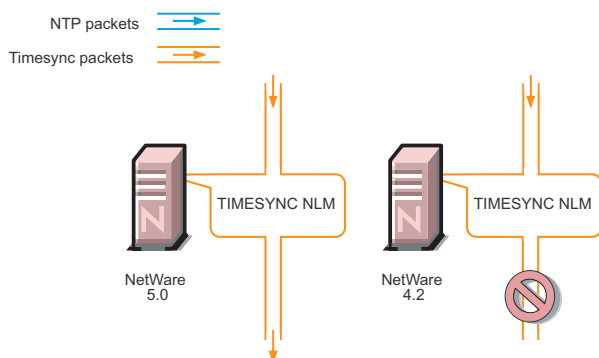
NetWare 5.1 and 6.0 Servers

Figure 12-3 illustrates that although NetWare 5.1 and 6.0 do not include an NTP time module, they can consume and deliver NTP time packets.

Figure 12-3 NTP Compatibility of NetWare 5.1 and 6.0

NetWare 5.0 and 4.2 Servers

Figure 12-4 illustrates that NetWare 4.2 and 5.0 servers can only consume and provide Timesync packets.

Figure 12-4 Synchronizing Time on NetWare 5.0 and 4.2 Servers

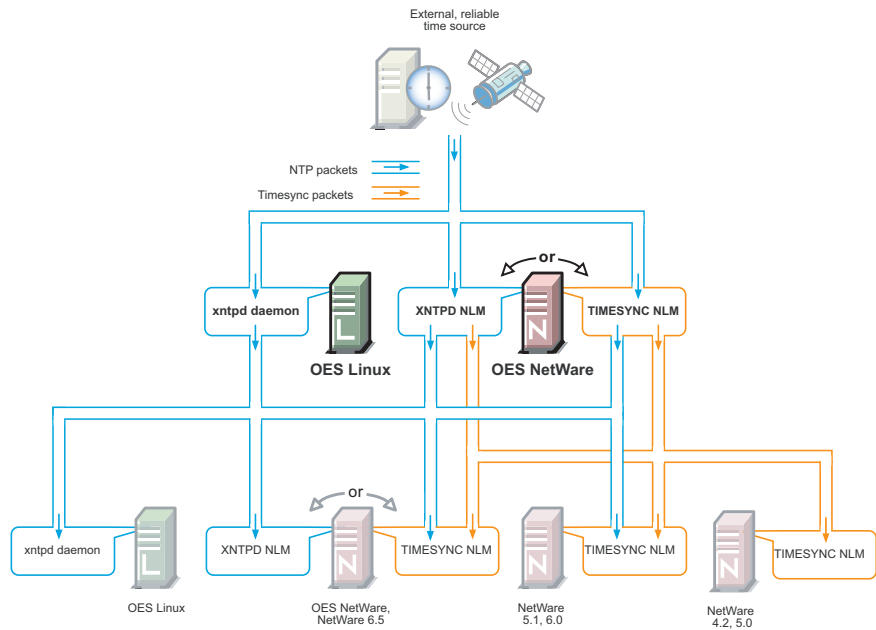
Therefore, if you have NetWare 4.2 or 5.0 servers in your eDirectory tree, and you want to install an OES 2 Linux server, you must have at least one NetWare 5.1 or later server to provide a “bridge” between NTP and Timesync time packets. **Figure 12-5 on page 111** illustrates that these earlier server versions can synchronize through an OES 2 NetWare server.

IMPORTANT: As shown in **Figure 12-4**, we recommend that NetWare 4.2 servers not be used as a time source.

OES 2 Servers as Time Providers

Figure 12-5 shows how OES 2 servers can function as time providers to other OES 2 servers and to NetWare servers, including NetWare 4.2 and later.

Figure 12-5 OES 2 Servers as Time Providers

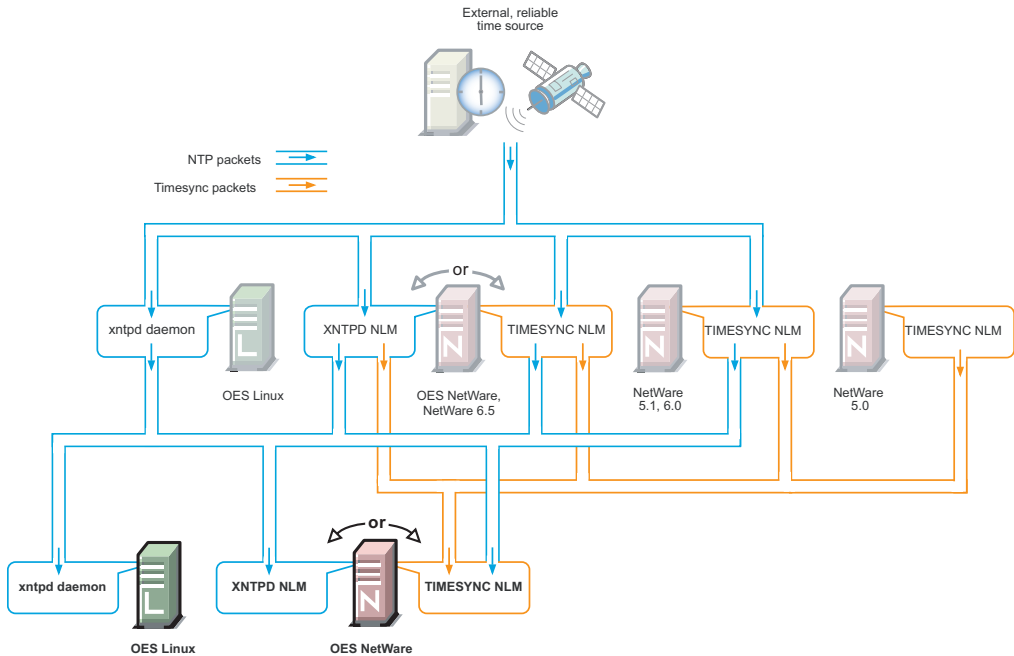


OES 2 Servers as Time Consumers

Figure 12-6 shows the time sources that OES 2 servers can use for synchronizing server time.

IMPORTANT: Notice that NetWare 4.2 is not shown as a valid time source.

Figure 12-6 OES 2 servers as Time Consumers



12.3.2 Planning for Time Synchronization

Use the information in this section to understand the basics of time synchronization planning.

- ♦ “NetWork Size Determines the Level of Planning Required” on page 112
- ♦ “Choosing between Timesync and NTP (NetWare Only)” on page 113
- ♦ “Planning a Time Synchronization Hierarchy before Installing OES” on page 114

For more detailed planning information, refer to the following resources:

- ♦ “How Timesync Works” in the *OES 2 : Novell TimeSync for NetWare Administration Guide*
- ♦ “Network Time Protocol” in the *OES 2: Novell NTP for NetWare Administration Guide*
- ♦ NTP information on the Web (<http://www.cis.udel.edu/~mills/ntp.html>)

NetWork Size Determines the Level of Planning Required

The level of time synchronization planning required for your network is largely dictated by how many servers you have and where they are located, as explained in the following sections.

- ♦ “Time Synchronization for Trees with Fewer Than Thirty Servers” on page 112
- ♦ “Time Synchronization for Trees with More Than Thirty Servers” on page 112
- ♦ “Time Synchronization across Geographical Boundaries” on page 113

Time Synchronization for Trees with Fewer Than Thirty Servers

If your tree will have fewer than thirty servers, the default installation settings for time synchronization should be sufficient for all of the servers except the first server installed in the tree.

You should configure the first server in the tree to obtain time from one or more time sources that are external to the tree. (See **Step 1** in “Planning a Time Synchronization Hierarchy before Installing OES” on page 114.)

All other servers (both Linux and NetWare) automatically point to the first server in the tree for their time synchronization needs.

Time Synchronization for Trees with More Than Thirty Servers

If your tree will have more than thirty servers, you need to plan and configure your servers with time synchronization roles that match your network architecture and time synchronization strategy.

Example roles might include the following:

- ♦ Servers that receive time from external time sources and send packets to other servers further down in the hierarchy
- ♦ Servers that communicate with other servers in peer-to-peer relationships to ensure that they are synchronized

Basic planning steps are summarized in “Planning a Time Synchronization Hierarchy before Installing OES” on page 114.

Refer to the following sources for additional help in planning time server roles:

- ♦ “Configuring Timesync on Servers” in the *OES 2 : Novell TimeSync for NetWare Administration Guide*

- ♦ “**Modes of Time Synchronization**” in the *OES 2: Novell NTP for NetWare Administration Guide*
- ♦ NTP information on the Web (<http://www.cis.udel.edu/~mills/ntp.html>)

Time Synchronization across Geographical Boundaries

If the servers in the tree will reside at multiple geographic sites, you need to plan how to synchronize time for the entire network while minimizing network traffic. For more information, see “**Wide Area Configuration**” in the *OES 2: Novell NTP for NetWare Administration Guide*.

Choosing between Timesync and NTP (NetWare Only)

When you install an OES 2 NetWare server, you can choose between Timesync and NTP for time synchronization.

If you select the Timesync option, you can fully configure each server as you install it to match your time synchronization plan.

If you choose the XNTPD option, you can designate up to three NTP time sources, but fine-tuning your NTP hierarchy requires some manual configuration after the installation is complete. For help, consult the *OES 2: Novell NTP for NetWare Administration Guide*.

About Timesync

Timesync is the Novell legacy time synchronization protocol first delivered with NetWare 4. Over the years it has evolved and is now capable of both consuming and delivering NTP packets and Timesync packets.

Timesync is installed and configured by default to ensure the smooth integration of earlier versions of NetWare.

IMPORTANT: For virtualized NetWare servers, you should always use Timesync and configure it to communicate using NTP as instructed in “**Creating a Response File for an Unattended NetWare Installation**” and “**Setting the Server Time Zone and Time Synchronization Method**” in the *OES 2 SPI: NetWare Installation Guide*.

About NTP

NTP is the emerging choice for many network administrators because:

- ♦ They feel it is easier to manage a single time synchronization protocol.
For example, the same basic configuration file (`ntp.conf`) can be used on both Linux and NetWare.
- ♦ NTP is a cross-platform industry standard available on multiple platforms.
- ♦ The XNTPD NLM that runs on OES 2 NetWare provides Timesync packets for NetWare servers that can’t consume NTP (NetWare 5.0 and 4.2), enabling them to coexist on an NTP time network.

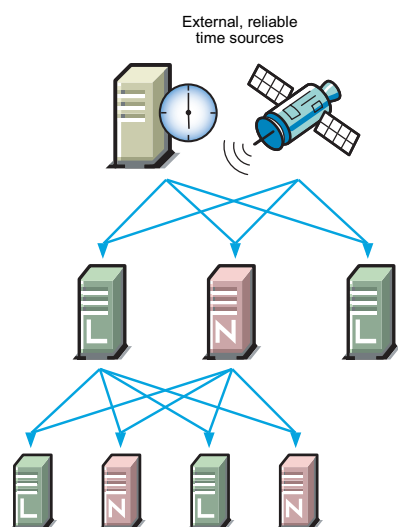
Where to Specify Time Synchronization in the NetWare Install

The dialog box that lets you choose between Timesync and NTP is available as an advanced option in the Time Zone panel during the NetWare installation. Choosing between Timesync and NTP is documented in “[Setting the Server Time Zone and Time Synchronization Method](#)” in the *OES 2 SP1: NetWare Installation Guide*.

Planning a Time Synchronization Hierarchy before Installing OES

The obvious goal for time synchronization is that all the network servers (and workstations, if desired) have the same time. This is best accomplished by planning a time synchronization hierarchy before installing the first OES 2 server, then configuring each server at install time so that you form a hierarchy similar to the one outlined in [Figure 12-7](#).

Figure 12-7 A Basic Time Synchronization Hierarchy



As you plan your hierarchy, do the following:

- 1 Identify at least two authoritative external NTP time sources for the top positions in your hierarchy.
 - ♦ If your network already has an NTP server hierarchy in place, identify the IP address of an appropriate time server. This might be internal to your network, but it should be external to the eDirectory tree and it should ultimately obtain time from a public NTP server.
 - ♦ If your network doesn't currently employ time synchronization, refer to the list of public NTP servers published on the [ntp.org Web site \(http://ntp.isc.org/bin/view/Servers/WebHome\)](http://ntp.isc.org/bin/view/Servers/WebHome) and identify a time server you can use.
- 2 Plan which servers will receive time from the external sources and plan to install these servers first.
- 3 Map the position for each Linux server in your tree, including its time sources and the servers it will provide time for.
- 4 Map the position for each NetWare server in your tree:
 - 4a Include the server's time sources and the servers it will provide time for.

- 4b** Decide whether to use Timesync or NTP for your servers. (See “[Choosing between Timesync and NTP \(NetWare Only\)](#)” on page 113.)
- 4c** If your network currently has only NetWare 4.2 or 5.0 servers, be sure to plan for their time synchronization needs by including at least one newer NetWare server in the tree and configuring the older servers to use the newer server as their time source. (See “[NetWare 5.0 and 4.2 Servers](#)” on page 110.)
- 5** Be sure that each server in the hierarchy is configured to receive time from at least two sources.
- 6** (Conditional) If your network spans geographic locations, plan the connections for time-related traffic on the network and especially across WANs.

For more information, see “[Wide Area Configuration](#)” in the *OES 2: Novell NTP for NetWare Administration Guide*.

For more planning information, see the following documentation:

- ♦ *OES 2 : Novell TimeSync for NetWare Administration Guide*
- ♦ *OES 2: Novell NTP for NetWare Administration Guide*
- ♦ NTP information found on the OES 2 Linux server in /usr/share/doc/packages/xntp and on the Web (<http://www.cis.udel.edu/~mills/ntp.html>)

12.3.3 Coexistence and Migration of Time Synchronization Services

The time synchronization modules in OES have been designed to ensure that new OES 2 servers, running on either NetWare or Linux, can be introduced into an existing network environment without disrupting any of the products and services that are in place.

Both the Linux and NetWare installs automate the time synchronization process where possible, as explained in [Section 12.3.4, “Implementing Time Synchronization,”](#) on page 117.

This section discusses the issues involved in the coexistence and migration of time synchronization in OES in the following sections:

- ♦ “[Coexistence](#)” on page 115
- ♦ “[Migration](#)” on page 116

Coexistence

This section provides information regarding the coexistence of the OES time synchronization modules with existing NetWare or Linux networks, and with previous versions of the TIMESYNC NLM. This information can help you confidently install new OES 2 servers into your current network.

- ♦ “[Compatibility](#)” on page 115
- ♦ “[Coexistence Issues](#)” on page 116

Compatibility

The following table summarizes the compatibility of OES time synchronization modules with other time synchronization modules and eDirectory. These compatibilities are illustrated in [Figure 12-5 on page 111](#) and [Figure 12-6 on page 111](#).

Table 12-3 *Time Synchronization Compatibility*

Module	Compatibility
TIMESYNC NLM (NetWare)	<p>Can consume time from</p> <ul style="list-style-type: none"> ♦ All previous versions of Timesync. However, the NetWare 4.2 TIMESYNC NLM should not be used as a time source. ♦ Any TIMESYNC or NTP daemon. <p>Can provide time to</p> <ul style="list-style-type: none"> ♦ All previous versions of Timesync. ♦ Any TIMESYNC or NTP daemon.
XNTPD NLM (NetWare)	<p>Can consume time from</p> <ul style="list-style-type: none"> ♦ Any NTP daemon. <p>Can provide time to</p> <ul style="list-style-type: none"> ♦ All previous versions of Timesync. ♦ Any NTP daemon.
xntpd daemon (SLES 10)	<p>Can consume time from</p> <ul style="list-style-type: none"> ♦ Any NTP daemon. <p>Can provide time to</p> <ul style="list-style-type: none"> ♦ Any NTP daemon.
eDirectory	eDirectory gets its time synchronization information from the host OS (Linux or NetWare), not from the time synchronization modules.

Coexistence Issues

If you have NetWare servers earlier than version 5.1, you need to install at least one later version NetWare server to bridge between the TIMESYNC NLM on the earlier server and any OES 2 Linux servers you have on your network. This is because the earlier versions of Timesync can't consume or provide NTP time packets and the xntpd daemon on Linux can't provide or consume Timesync packets.

Fortunately, the TIMESYNC NLM in NetWare 5.1 and later can both consume and provide Timesync packets. And the XNTPD NLM can provide Timesync packets when required.

This is explained in [“Compatibility with Earlier Versions of NetWare” on page 109](#).

Migration

Your migration path depends on the platform you are migrating data to.

- ♦ **NetWare to NetWare:** Time synchronization configuration settings are all migrated by the NetWare Migration Wizard (both Timesync and XNTPD modules) because all associated modules and configuration files reside on `sys:system`.

- ♦ **NetWare to Linux:** The OES 2 SP1 Migration Tool can migrate time synchronization services from NetWare to Linux. For more information, see “[Migrating Timesync/NTP from NetWare to NTP on OES 2 SP1 Linux](#)” in the *OES 2 SP1: Migration Tool Administration Guide*.

12.3.4 Implementing Time Synchronization

As you plan to implement your time synchronization hierarchy, you should know how the OES 2 NetWare and OES 2 Linux product installations configure time synchronization on the network. Both installs look at whether you are creating a new tree or installing into an existing tree.

- ♦ “[New Tree](#)” on page 117
- ♦ “[Existing Tree](#)” on page 118

New Tree

By default, both the OES 2 Linux and the OES 2 NetWare installs configure the first server in the tree to use its internal (BIOS) clock as the authoritative time source for the tree.

Because BIOS clocks can fail over time, you should always specify an external, reliable NTP time source for the first server in a tree. For help finding a reliable NTP time source, see the [NTP Server Lists \(http://ntp.isc.org/bin/view/Servers/WebHome\)](http://ntp.isc.org/bin/view/Servers/WebHome) on the Web.

- ♦ “[OES 2 Linux](#)” on page 117
- ♦ “[OES 2 NetWare](#)” on page 117

OES 2 Linux

When you configure your eDirectory installation, the OES 2 Linux install prompts you for the IP address or DNS name of an NTP v3-compatible time server.

If you are installing the first server in a new eDirectory tree, you have two choices:

- ♦ You can enter the IP address or DNS name of an authoritative NTP time source (recommended).
- ♦ You can leave the field displaying Local Time, so the server is configured to use its BIOS clock as the authoritative time source.

IMPORTANT: We do not recommend this second option because BIOS clocks can fail over time, causing serious problems for eDirectory.

OES 2 NetWare

By default, the NetWare install automatically configures the TIMESYNC NLM to use the server’s BIOS clock. As indicated earlier, this default behavior is not recommended for production networks. You should, therefore, manually configure time synchronization (either Timesync or NTP) while installing each NetWare server.

Manual time synchronization configuration is accessed at install time from the Time Zone dialog box by clicking the *Advanced* button as outlined in “[Choosing between Timesync and NTP \(NetWare Only\)](#)” on page 113 and as fully explained in “[Setting the Server Time Zone and Time Synchronization Method](#)” in the *OES 2 SP1: NetWare Installation Guide*.

Existing Tree

When a server joins an existing eDirectory tree, both OES installations do approximately the same thing.

- ♦ “OES 2 Linux” on page 118
- ♦ “OES 2 NetWare” on page 118

OES 2 Linux

If you are installing into an existing tree, the OES 2 Linux install proposes to use the IP address of the eDirectory server (either NetWare or Linux) as the NTP time source. This default should be sufficient unless one of the following is true:

- ♦ The server referenced is a NetWare 5.0 or earlier server, in which case you need to identify and specify the address of another server in the tree that is running either a later version of NetWare or OES 2 Linux.
- ♦ You will have more than 30 servers in your tree, in which case you need to configure the server to fit in to your planned time synchronization hierarchy. For more information, see “[Planning a Time Synchronization Hierarchy before Installing OES](#)” on page 114.

The OES 2 Linux install activates the xntp daemon and configures it to synchronize server time with the specified NTP time source. After the install finishes, you can configure the daemon to work with additional time sources to ensure fault tolerance. For more information, see “[Changing Time Synchronization Settings on a SLES 10 Server](#)” on page 119.

OES 2 NetWare

If you are installing into an existing tree, the OES 2 NetWare install first checks to see whether you manually configured either NTP or Timesync time synchronization sources while setting the server Time Zone (see “[Setting the Server Time Zone and Time Synchronization Method](#)” in the *OES 2 SP1: NetWare Installation Guide*).

If you will have more than 30 servers in your tree, you should have developed a time synchronization plan (see “[Planning a Time Synchronization Hierarchy before Installing OES](#)” on page 114) and used the Time Zone panel to configure your server according to the plan.

If you haven’t manually configured time synchronization sources for the server (for example, if your tree has fewer than 30 servers), the install automatically configures the Timesync NLM to point to the IP address of the server with a master replica of the tree’s [ROOT] partition.

12.3.5 Configuring and Administering Time Synchronization

As your network changes, you will probably need to adjust the time synchronization settings on your servers.

- ♦ “[Changing Time Synchronization Settings on a SLES 10 Server](#)” on page 119
- ♦ “[Changing Time Synchronization Settings on a NetWare Server](#)” on page 119

Changing Time Synchronization Settings on a SLES 10 Server

This method works both in the GUI and at the command prompt and is the most reliable method for ensuring a successful NTP implementation.

- 1 Launch YaST on your SLES 10 server by either navigating to the application on the desktop or typing `yast` at the command prompt.
- 2 Click *Network Services > NTP Client*.
- 3 In the *NTP Client Configuration* dialog box, click *Complex Configuration*.
- 4 Modify the NTP time settings as your needs require.

Changing Time Synchronization Settings on a NetWare Server

Time synchronization settings and their modification possibilities are documented in the following administration guides:

- ♦ Timesync: *OES 2 : Novell TimeSync for NetWare Administration Guide*
- ♦ NTP: *OES 2: Novell NTP for NetWare Administration Guide*

12.3.6 Daylight Saving Time

For information about daylight saving time (DST), see the [DST Master TID on the Novell Support site](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=3094409) (<http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=3094409>)

12.4 Discovery Services (SLP, WinSock, Etc.)

Various discovery mechanisms are usually available on an OES 2 network.

- ♦ DNS/DHCP
- ♦ Directory services
- ♦ Local host configuration files
- ♦ Service Location Protocol (SLP services)
- ♦ WinSock (NetWare only)
- ♦ Universal Description, Discovery, and Integration (UDDI) server

Some systems are designed to leverage only a single discovery technology. Others choose among the various providers. And some use different technologies in combination with each other.

- ♦ [Section 12.4.1, “Novell SLP and OpenSLP,” on page 120](#)
- ♦ [Section 12.4.2, “WinSock and Discovery \(NetWare only\),” on page 120](#)
- ♦ [Section 12.4.3, “UDDI and Discovery,” on page 120](#)
- ♦ [Section 12.4.4, “CIMOM and Discovery,” on page 120](#)

12.4.1 Novell SLP and OpenSLP

NetWare 3 and 4 used the IPX-based Service Advertising Protocol (SAP) as the discovery mechanism. All the servers advertised their services automatically. If a server went offline, the SAP information on the network was dynamically refreshed.

Starting with NetWare 5 and pure TCP/IP, the Service Location Protocol was adopted as the default, though optional, discovery mechanism. SLP was chosen because it was the TCP/IP-based protocol most like SAP in its automatic nature and dynamic refresh capabilities.

For more information, see [Section 12.5, “SLP,” on page 120](#).

12.4.2 WinSock and Discovery (NetWare only)

WinSock collects service information from all available service-discovery sources.

NetWare Loadable Module™ (NLM) programs that leverage WinSock have access to all discovery services on the network automatically. Therefore, if you removed SLP as a source of information (for example) and placed the information into DNS or a local host file, any NLM that leverages WinSock would not know the difference.

NOTE: There is no WinSock equivalent in the Linux environment. BSDSock provides for transport only, not name resolution. Therefore, any NetWare services that leveraged WinSock and are provided on OES 2 Linux use other service-discovery mechanisms.

12.4.3 UDDI and Discovery

UDDI is an open source, platform-independent registry that lets you provide a discovery service on the World Wide Web to easily locate, integrate, and manage businesses and services.

For NetWare 6.5, Novell developed a directory-enabled UDDI server for use with the exteNd™ J2EE™ Application Server. Starting with OES 1 NetWare, the UDDI server component was removed from the list of products that can be installed.

However, the Novell UDDI server has been released as open source software and is available for download on the [Novell Forge Web site \(http://forge.novell.com/modules/xfmod/project/showfiles.php?group_id=1025\)](http://forge.novell.com/modules/xfmod/project/showfiles.php?group_id=1025).

12.4.4 CIMOM and Discovery

The current OpenWBEM implementation of the Common Information Model Object Manager (CIMOM) lists SLP as an optional discovery provider. If SLP is to be used with CIMOM, it must be in compliance with the SLP API specification (RFC 2614). The default discovery vehicle for CIMOM is the statically configured URI. For more information, see the CIMOM specification at the [Desktop Management Task Force \(DMTF\) Web site \(http://www.dmtf.org\)](http://www.dmtf.org).

12.5 SLP

OES 2 includes separate but compatible SLP solutions on its Linux and NetWare platforms:

This section discusses the following topics:

- ♦ [Section 12.5.1, “Why SLP Is Needed,” on page 121](#)
- ♦ [Section 12.5.2, “Comparing Each Platform’s SLP Solution,” on page 121](#)
- ♦ [Section 12.5.3, “Setting Up OpenSLP on OES 2 Networks,” on page 122](#)
- ♦ [Section 12.5.4, “Using Novell SLP on OES 2 Networks,” on page 126](#)

12.5.1 Why SLP Is Needed

OES 2 NetWare: Although many other applications and server types rely on SLP for service discovery, OES 2 services on NetWare are actually integrated with eDirectory, and if eDirectory is configured correctly, the services work without SLP. However, SLP is automatically provided on NetWare for other services that might be installed.

OES 2 Linux: On the other hand, for OES 2 services to work on OES 2 Linux, the server must either:

- ♦ Have an eDirectory replica installed.

This is not automatic after the third server installed in a tree, nor is having more than three to five replicas on servers in the tree recommended.
- ♦ Have eDirectory registered with the OpenSLP service running on the server.

This requires SLP configuration either during the OES 2 Linux installation or manually.

12.5.2 Comparing Each Platform’s SLP Solution

Table 12-4 SLP Solutions

Platform	NetWare	SLES 10 SP1
SLP Solution	Novell SLP	OpenSLP
About the Solution	<p>The Novell version of SLP adapted portions of the SLP standard to provide a more robust service advertising environment.</p> <p>Novell SLP remains the default discovery mechanism for OES 2 NetWare servers. However, all NetWare service components that engage in discovery, including Novell Client™ software, can use alternative mechanisms such as DNS, eDirectory, or local host configuration files.</p>	<p>OpenSLP is an implementation of various IETF specifications, including RFC 2614 (SLP version 2.0). It is the default SLP service installed on SLES 10.</p> <p>In OES 2 Linux, OpenSLP is available for those applications that require it. The default discovery mechanism is actually DNS, but SLP must be present for any applications that require it, especially in those cases where the OES 2 Linux server is the fourth or later server added to a tree and doesn't have an eDirectory replica automatically installed.</p>

Platform	NetWare	SLES 10 SP1
Differences	<p>Novell SLP directory agents (DAs) store service registrations for their SLP scope in eDirectory.</p> <p>As a new service registration is stored in eDirectory, other DAs assigned to the same scope are notified so that they can refresh their caches with the latest service information.</p> <p>Also, when a Novell SLP DA starts up, it immediately populates its cache with the latest service information stored in eDirectory.</p> <hr/> <p>NOTE: Novell SLP DAs do not directly share information with each other as many administrators have assumed. But they do maintain well synchronized caches through eDirectory as described above.</p>	<p>OpenSLP directory agents (DAs) are completely separate and have no way to initially populate or refresh their service information the way Novell SLP DAs do.</p> <p>A DA's cache is empty when it starts up and is populated only as services register themselves.</p>
Compatibility	Novell SLP user agents (UAs) or service agents (SAs) can access both Novell SLP DAs and OpenSLP DAs.	OpenSLP-based user agents or service agents can access both Novell SLP DAs and OpenSLP DAs.
Documentation	“Implementing the Service Location Protocol” in the <i>Novell eDirectory 8.8 Administration Guide</i> .	“Configuring OpenSLP for eDirectory” in the <i>Novell eDirectory 8.8 Administration Guide</i> .

12.5.3 Setting Up OpenSLP on OES 2 Networks

SLP services are always installed as part of both NetWare and SLES 10 SP1 (the underlying OES 2 Linux platform). On NetWare the Novell SLP service is configured to automatically work with eDirectory and other services. On OES 2 Linux, the OpenSLP service must be manually configured to work with eDirectory and other services.

- ♦ [“When Is OpenSLP Required?”](#) on page 122
- ♦ [“Setting Up an OpenSLP DA Server”](#) on page 123
- ♦ [“Configuring OES 2 Linux Servers to Access the OpenSLP DA”](#) on page 124
- ♦ [“Configuring NetWare Servers to Use the OpenSLP Service”](#) on page 125

When Is OpenSLP Required?

You must set up OpenSLP on your OES 2 Linux server if both of the following apply:

- ♦ You plan to install more than three servers into a new tree being created on an OES 2 Linux server.
- ♦ You either don't have an existing Novell SLP service, or you don't want to continue using Novell SLP.

IMPORTANT: If you need to set up OpenSLP for the reasons above, you should do it before you install the fourth OES 2 Linux or any NetWare servers in your tree. Setting up SLP services on every OES 2 Linux server is recommended.

Setting Up an OpenSLP DA Server

If you need OpenSLP and you don't already have an OpenSLP Directory Agent (DA) set up on your network, for simplicity's sake we recommend that you set up the first OES 2 Linux server in your tree as an OpenSLP DA. Although SLP services can be managed without having a Directory Agent, that approach is far less robust, requires multicasting, and for OES 2 Linux it involves disabling the firewall.

After creating the DA, you can then configure all subsequently installed servers to either point to that DA or to other DAs you create later.

- 1 On the OES 2 Linux server that will become the DA, open the `/etc/slp.conf` file in a text editor.

- 2 In `slp.conf`, remove the semicolon [`;`] from the beginning of the following line:

```
;net.slp.isDA = true
```

so that it reads

```
net.slp.isDA = true
```

- 3 Find the following line:

```
;net.slp.useScopes = myScope1, myScope2, myScope3
```

IMPORTANT: The example in the configuration file is misleading because the spaces after each comma are not ignored as one might expect them to be.

Therefore, the scope names created or configured by the statement after the first comma actually have leading spaces in them. For example, the first scope name is "myScope1" but the scope names that follow it all have leading spaces, " myScope2", " myScope3" and so on. This is a problem, especially if one of the later names becomes the first name in a subsequent SLP configuration and the leading space is ignored.

If you use the scopes given in the example, remove the spaces between the entries.

-
- 4 Modify the line by removing the semicolon and typing the name of the scope you want this DA to use to provide service information on the network. For example, you might change the line as follows:

```
net.slp.useScopes = Directory
```

IMPORTANT: Although SLP provides a default scope if no scope is specified, it is always good practice to define one or more scopes by configuring the `net.slp.useScopes` parameter in `slp.conf`.

Scopes group and organize the services on your network into logical categories. For example, the services that the Accounting group needs might be grouped into an Accounting scope.

More information about scope planning is available in "SLP Scopes" in the *Novell eDirectory 8.8 Administration Guide* and on the [OpenSLP Web site \(http://www.openslp.org/\)](http://www.openslp.org/).

When no scope is specified, all services are registered in a scope named Default.

- 5 Configure the firewall on the DA server to allow SLP daemon traffic:
 - 5a In the YaST Control Center, click *Security and Users > Firewall*.
 - 5b In the left navigation frame, click *Allowed Services*.
 - 5c Click the *Services to Allow* drop-down list and select *SLP Daemon*.
 - 5d Click *Add > Next*.
 - 5e Click *Accept*.
- 6 At the command prompt, enter the following command to restart the SLP daemon:


```
rcslpd restart
```
- 7 (Conditional) If you are doing this after installing OES 2 and eDirectory, you must also restart eDirectory by entering the following command:


```
rcndsd restart
```
- 8 Continue with the following sections that apply to your situation:
 - ♦ [Configuring OES 2 Linux Servers to Access the OpenSLP DA \(page 124\)](#)
 - ♦ [Configuring NetWare Servers to Use the OpenSLP Service \(page 125\)](#)

Configuring OES 2 Linux Servers to Access the OpenSLP DA

If you created the OpenSLP DA on an OES 2 Linux server installed in your tree, then SLP is properly configured on that server and these instructions do not apply to it.

For all other OES 2 Linux servers installed in your eDirectory tree, you should complete one of the following procedures as it applies to your situation:

- ♦ [“Configuring for DA Access During the OES 2 Linux Installation” on page 124](#)
- ♦ [“Configuring for DA Access Before or After Installing the OES 2 Linux Server” on page 125](#)

Configuring for DA Access During the OES 2 Linux Installation

As you install OES 2 Linux by using the instructions in the “[Novell eDirectory Services](#)” section of the *OES 2 SP1: Linux Installation Guide*, do the following:

- 1 When you reach the SLP section of the installation, select *Configure SLP to Use an Existing Directory Agent*.
 The first option, *Do not configure SLP*, causes problems with eDirectory and other services if this is the fourth or later server installed in the tree. The second option, *Use Multicast*, requires that you disable the firewall on the server. Disabling the firewall is always discouraged.
- 2 In the *Service Location Protocol Scopes* field, specify the scope you defined in [Step 4 on page 123](#). You can also list additional scopes, separated by commas (no spaces).
 For example, you might type `Directory` in the field if that is the scope name you assigned to the DA you created.
- 3 In the *Configured SLP Directory Agent* field, type the IP address of the DA server you defined in [“Setting Up an OpenSLP DA Server” on page 123](#). You can also list additional DA addresses, separated by commas.
- 4 Return to the “[Novell eDirectory Services](#)” instructions in the *OES 2 SP1: Linux Installation Guide*.

Configuring for DA Access Before or After Installing the OES 2 Linux Server

Whether you configure DA access before installing OES 2 Linux on a SLES 10 SP1 server or after a simultaneous install of SLES 10 SP1 and OES 2, the manual DA configuration process is the same.

1 Open `/etc/slp.conf` in a text editor.

2 Find the following line:

```
;net.slp.useScopes = myScope1, myScope2, myScope3
```

IMPORTANT: The example in the configuration file is misleading because the spaces after each comma are not ignored as one might expect them to be.

Therefore, the scope names created or configured by the statement after the first comma actually have leading spaces in them. For example, the first scope name is “myScope1” but the scope names that follow it all have leading spaces, “ myScope2”, “ myScope3” and so on. This is a problem, especially if one of the later names becomes the first name in a subsequent SLP configuration and the leading space is ignored.

If you use the scopes given in the example for some reason, remove the spaces between the entries.

3 Modify the line by removing the semicolon and typing the name or names of the scopes you want this server to have access to. Be sure to include the scope you defined in [Step 4 on page 123](#).

For example, you might change the line as follows:

```
net.slp.useScopes = Directory
```

4 Find the following line:

```
;net.slp.DAAddresses = myDa1,myDa2,myDa3
```

5 Modify the line by removing the semicolon and typing the actual IP address of the OpenSLP DA you defined in [“Setting Up an OpenSLP DA Server” on page 123](#).

```
net.slp.DAAddresses = IP_Address
```

6 Save the file and close it.

7 At the Linux command prompt, enter the following to restart the SLP daemon and reset its configuration:

```
rcslpd restart
```

Configuring NetWare Servers to Use the OpenSLP Service

IMPORTANT: NetWare uses Novell SLP by default and will configure a server for that service if possible.

Complete one of the following as it applies to your situation:

- ♦ [“Configuring for DA Access During the NetWare Server Installation” on page 125](#)
- ♦ [“Configuring for DA Access After Installing the NetWare Server” on page 126](#)

Configuring for DA Access During the NetWare Server Installation

1 In the dialog box where you set up IP addresses for network boards, click *Advanced*.

2 Click the *SLP* tab.

- 3 Specify the IP address of the OES 2 Linux DA servers—up to three.
- 4 Type the list of scopes covered by the configured DAs that you want the NetWare server to have access to.

IMPORTANT: We recommend you do not configure the server to use multicast because that necessitates disabling firewalls, which is never recommended.

- 5 Click OK.

Configuring for DA Access After Installing the NetWare Server

- 1 Using a text editor, edit the `SYS:ETC/slp.cfg` file on the NetWare server and add the following line for each DA server you want the NetWare server to have access to:

```
DA IPV4, IP_Address1
DA IPV4, IP_Address2
```

where *IP_AddressX* is the IP address of an OES 2 Linux DA server.

- 2 Save the file and close it.
- 3 At the NetWare console prompt, specify the scopes you want the NetWare server to have access to, write the SLP cache to the registry, and restart the SLP service:

```
set slp scope list = scope1,scope2,...
flush cdb
set slp reset = on
```

- 4 Verify that SLP is functioning correctly by entering the following command:

```
display slp services
```

12.5.4 Using Novell SLP on OES 2 Networks

If you have a NetWare tree, you automatically have Novell SLP on your network and you can continue to use it as the SLP service for both OES 2 platforms.

This section discusses the following:

- ♦ “NetWare Is Configured with Novell SLP By Default” on page 126
- ♦ “Configuring OES 2 Linux Servers to Access the Novell SLP DA” on page 127
- ♦ “Checking the Status of Novell SLP Services” on page 128

NetWare Is Configured with Novell SLP By Default

When you install NetWare, if you don’t specify an alternate SLP configuration, the server is automatically configured to use Novell SLP in a way that is sufficient for most networks. Information about Novell SLP and customization instructions is available in “[Implementing the Service Location Protocol](#)” in the *Novell eDirectory 8.8 Administration Guide*.

Configuring OES 2 Linux Servers to Access the Novell SLP DA

For each of the OES 2 Linux servers installed in your eDirectory tree, you should complete one of the following procedures as it applies to your situation:

- ♦ “Configuring for DA Access During the OES 2 Linux Installation” on page 127
- ♦ “Configuring for DA Access Before or After Installing the OES 2 Linux Server” on page 127

Configuring for DA Access During the OES 2 Linux Installation

As you install OES 2 Linux, in the “**Novell eDirectory Services**” section of the *OES 2 SP1: Linux Installation Guide*, do the following:

- 1 When you reach the SLP section of the installation, select *Configure SLP to Use an Existing Directory Agent*.
The first option, *Do not configure SLP*, causes problems with eDirectory and other services if this is the fourth or later server installed in the tree. The second option, *Use Multicast*, requires that you disable the firewall on the server. Disabling the firewall is always discouraged.
- 2 In the *Service Location Protocol Scopes* field, specify one or more appropriate scopes that are defined on your network.
If you aren’t sure about the exact scope names, you can view the SLP configuration of a NetWare server on the same network segment. Log into Novell Remote Manager on the server and click *Manage Applications > SLP*.
You can list multiple scopes, separated by commas (no spaces).
For example, you might type `Directory` in the field.
- 3 In the *Configured SLP Directory Agent* field, type the IP address of an appropriate DA server.
You can use Novell Remote Manager on a NetWare server if you aren’t sure which address to use.
You can also list additional DA addresses, separated by commas.
- 4 Return to the “**Novell eDirectory Services**” instructions in the *OES 2 SP1: Linux Installation Guide*.

Configuring for DA Access Before or After Installing the OES 2 Linux Server

Whether you configure DA access before installing OES 2 Linux on a SLES 10 SP1 server or after a simultaneous install of SLES 10 SP1 and OES 2, the manual DA configuration process is the same.

- 1 Open `/etc/slp.conf` in a text editor.
- 2 Find the following line:

```
;net.slp.useScopes = myScope1, myScope2, myScope3
```

IMPORTANT: The example in the configuration file is misleading because the spaces after each comma are not ignored as one might expect them to be.

Therefore, the scope names created or configured by the statement after the first comma actually have leading spaces in them. For example, the first scope name is “myScope1” but the scope names that follow it all have leading spaces, “ myScope2”, “ myScope3” and so on. This is a problem, especially if one of the later names becomes the first name in a subsequent SLP configuration and the leading space is ignored.

If you use the scope names given in the example, remove the spaces between the entries.

- 3 Modify the line by removing the semicolon and typing the name or names of the scopes you want this server to have access to.

If you aren't sure about the exact scope names, you can view the SLP configuration of a NetWare server on the same network segment. Log into Novell Remote Manager on the server and click *Manage Applications > SLP*.

You can list multiple scopes, separated by commas (no spaces).

For example, you might change the line as follows:

```
net.slp.useScopes = Directory
```

- 4 Find the following line:

```
;net.slp.DAAddresses = myDa1,myDa2,myDa3
```

- 5 Modify the line by removing the semicolon and typing the actual IP address of the Novell SLP DA (using Novell Remote Manager if necessary).

```
net.slp.DAAddresses = IP_Address
```

- 6 Save the file and close it.

- 7 At the Linux command prompt, enter the following to restart the SLP daemon and reset its configuration:

```
rcslpd restart
```

- 8 Enter the following commands to verify that the DA and scopes you configured are recognized.

```
slptool findsrvs service:
```

The DA server should be listed.

```
slptool findscopes
```

The scopes should be listed.

- 9 If you did this after installing OES 2 Linux, enter the following name to verify that the tree is found:

```
slptool findsrvs service:ndap.novell
```

Checking the Status of Novell SLP Services

There are several ways to check the status of Novell SLP services.

- ♦ If you know the IP addresses of the DAs, check the `SYS:\etc\slp.cfg` file on non-DA servers to see if the DA IP addresses are listed.
- ♦ If you know the scope names, check for the proper scope name configuration by using the `SET SLP SCOPE LIST` command.
- ♦ Use the `DISPLAY SLP SERVICES` command to list all of the services that are registered in all of the scopes that the server is configured to use.
- ♦ Use iManager to open the scope container object to see all of the registered services.
- ♦ If you are registering different services in different scopes, look in the `SYS:\etc\slp.cfg` file for `REGISTER TYPE` lines.
- ♦ At the DOS prompt on a Windows workstation with Client32™ installed, use the `SLPINF0 / ALL` command.

Storage and File Systems

Hosting shared data storage is one of the primary functions of network servers. Whether data volumes are directly attached to the server in RAID configurations or externally accessible in Storage Area Network (SAN) or Network Attached Storage (NAS) configurations, users need to be able to access their data on a continual basis.

Use this section to understand the file storage solutions available in Open Enterprise Server 2 and then to plan a storage solution that meets your file system management needs.

The “[Storage and File Systems](#)” section in the OES 2 online documentation provides overview, planning, implementation, and configuration links.

This section provides the following information about the process of planning and implementing storage services in OES:

- ♦ [Section 13.1, “Overview of OES 2 Storage,” on page 129](#)
- ♦ [Section 13.2, “Planning OES File Storage,” on page 134](#)
- ♦ [Section 13.3, “Coexistence and Migration of Storage Services,” on page 141](#)
- ♦ [Section 13.4, “Initial Setup Is Required for NetWare,” on page 143](#)
- ♦ [Section 13.5, “Configuring and Maintaining Storage,” on page 143](#)

Other storage-related topics in this guide:

- ♦ [Chapter 16, “Access Control and Authentication,” on page 173](#)
- ♦ [Section 16.2, “Authentication Services,” on page 186](#)
- ♦ [Appendix D, “Backup Services,” on page 255](#)
- ♦ [Chapter 17, “File Services,” on page 191](#)

13.1 Overview of OES 2 Storage

This section presents the following overview information for the file systems included in OES:

- ♦ [Section 13.1.1, “Databases,” on page 129](#)
- ♦ [Section 13.1.2, “iSCSI,” on page 130](#)
- ♦ [Section 13.1.3, “File System Support in OES,” on page 130](#)
- ♦ [Section 13.1.4, “Storage Basics by Platform,” on page 132](#)
- ♦ [Section 13.1.5, “Storage Options,” on page 132](#)
- ♦ [Section 13.1.6, “NetWare Core Protocol Support \(Novell Client Support\) on Linux,” on page 134](#)

13.1.1 Databases

See the topics in “[databases](#)” in the OES online documentation.

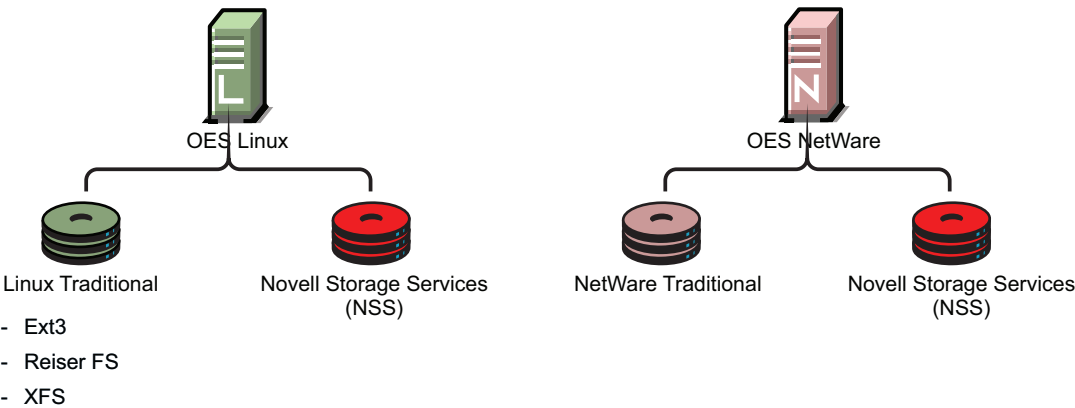
13.1.2 iSCSI

See the topics in “[iSCSI for NetWare](#)” in the OES online documentation.

13.1.3 File System Support in OES

As shown in [Figure 13-1](#), both OES 2 server platforms support Novell® Storage Services™ as well as their traditional file systems.

Figure 13-1 File System Choices on OES 2 Servers



[Table 13-1](#) summarizes OES file system types and provides links to more information.

Table 13-1 File Systems Available on OES 2 Servers

File System Type	Summary	Link for More Information
Linux POSIX File Systems	<p>SLES 10 includes a number of different file systems, the most common of which are Ext3 and ReiserFS.</p> <p>OES 2 services are supported on Ext3, ReiserFS, and XFS.</p>	<p>For an overview of the supported file systems in OES 2, see “File Systems Overview” in the <i>OES 2 SP1: File Systems Management Guide</i>.</p>
NetWare® Traditional File System	<p>Although it is considered a legacy file system on NetWare servers, the NetWare Traditional file system is still robust. It supports the NetWare file service access model.</p>	<p>For more information, see the <i>OES 2 SP1: NetWare Traditional File System Administration Guide</i>.</p>

File System Type	Summary	Link for More Information
Novell Storage Services (NSS)	<p>NSS lets you manage your shared file storage for any size organization.</p> <p>On NetWare, NSS features include visibility, a trustee access control model, multiple simultaneous name space support, native Unicode, user and directory quotas, rich file attributes, multiple data stream support, event file lists, and a file salvage subsystem.</p> <p>Most of these features are also supported on NSS on Linux. For a feature comparison, see “Comparison of NSS on NetWare and NSS on Linux” in the <i>OES 2 SP1: NSS File System Administration Guide</i>.</p>	<p>For an overview of NSS, see “Overview of NSS” in the <i>OES 2 SP1: NSS File System Administration Guide</i>.</p>

Novell Storage Services (NSS)

The following sections summarize key points regarding NSS:

- ♦ “[Understanding NSS Nomenclature](#)” on page 131
- ♦ “[Comparing NSS with Other File Systems](#)” on page 131
- ♦ “[NSS and Storage Devices](#)” on page 132

Understanding NSS Nomenclature

NSS uses a specific nomenclature to describe key media objects. These terms appear in both the NSS documentation and in NSS error messages.

For more information, see “[NSS Nomenclature](#)” in the *OES 2 SP1: NSS File System Administration Guide*.

Comparing NSS with Other File Systems

Because OES 2 supports a variety of file systems, you might want to compare their features and benefits as outlined in the following sections of the *OES 2 SP1: NSS File System Administration Guide*:

- ♦ **NSS Linux vs. NSS NetWare:** “[Comparison of NSS on NetWare and NSS on Linux](#)”
- ♦ **NSS Linux vs. Linux POSIX:** “[Comparison of NSS on Linux and NCP Volumes on Linux POSIX File Systems](#)”
- ♦ **NSS Netware vs. NetWare Traditional:** “[Comparison of NSS on NetWare and the NetWare Traditional File System](#)”

NSS and Storage Devices

NSS supports both physical devices (such as hard disks) and virtual devices (such as software RAIDs and iSCSI devices).

For more information on the various devices that NSS supports, see “[Managing Devices](#)” in the *OES 2 SPI: NSS File System Administration Guide*.

13.1.4 Storage Basics by Platform

The following sections summarize storage basics for Linux and NetWare.

- ♦ “[Linux and File Systems](#)” on page 132
- ♦ “[NetWare Directories](#)” on page 132
- ♦ “[NetWare Storage Devices](#)” on page 132

Linux and File Systems

For a high-level overview of the file system on Linux, including the root (/) directory, mount points, standard folders, and case sensitivity, see “[Understanding Directory Structures in Linux POSIX File Systems](#)” in the *OES 2 SPI: File Systems Management Guide*.

NetWare Directories

NetWare uses volumes and directories (or folders) to organize data. NetWare file systems support directory paths, fake root directories, Directory Map objects, and drive mappings.

For more information, see “[Understanding Directory Structures for the NSS and NetWare Traditional File Systems](#)” in the *OES 2 SPI: File Systems Management Guide*.

NetWare Storage Devices

NetWare lets you use many different kinds of storage devices, including server disks, single storage devices, arrays of storage devices, and virtual storage devices.

To understand how NetWare connects with and uses storage devices, see “[Overview of Server Disks and Storage Devices for NetWare](#)” in the *OES 2 SPI: NetWare Server Disks and Storage Devices*.

13.1.5 Storage Options

The following sections summarize OES storage options.

- ♦ “[Dynamic Storage Technology](#)” on page 132
- ♦ “[Direct-Attached Storage Options \(NSS and Traditional\)](#)” on page 133
- ♦ “[Advanced Storage Options \(NSS Only\)](#)” on page 133

Dynamic Storage Technology

Dynamic Storage Technology for OES 2 Linux lets you present the files and subdirectories on two separate NSS volumes as though they were on a single, unified NSS volume called a shadow volume.

NCP™ client users and Samba/CIFS users who access the primary volume see the files and subdirectories from both volumes as if they were all on one volume. All the actions they take—renaming, deleting, moving, etc.—are synchronized by Dynamic Storage Technology across the two volumes.

Unlike the NCP client, backup tools see the volumes separately and can therefore apply one backup policy to the primary and a different backup policy to the secondary volume.

You can use Dynamic Storage Technology to substantially reduce storage costs by placing your less frequently accessed files on less expensive storage media. You can even employ a “move on demand” migration strategy by defining new, more expensive SAN or RAID storage that is initially empty as the primary volume, and then configuring Dynamic Storage Technology so that data is migrated to this primary storage only when it is accessed.

In addition, Dynamic Storage Technology doesn’t suffer the performance penalty that HSM solutions do.

For more information about Dynamic Storage Technology, see the *OES 2 SP1: Dynamic Storage Technology Administration Guide*.

Direct-Attached Storage Options (NSS and Traditional)

As shown in [Figure 13-1 on page 130](#), you can install traditional volumes and Novell Storage System (NSS) volumes on both OES platforms. These devices can be installed within the server or attached directly to the server through an external SCSI bus.

For more information, see “[Direct Attached Storage Solutions](#)” in the *OES 2 SP1: Storage and File Services Overview*.

Advanced Storage Options (NSS Only)

NSS volumes support the following advanced storage solutions, as documented in the *OES 2 SP1: Storage and File Services Overview*.

- ◆ **Network Attached Storage Solutions**

A dedicated data server or appliance that provides centralized storage access for users and application servers through the existing network infrastructure and by using traditional LAN protocols such as Ethernet and TCP/IP. When Gigabit Ethernet is used, access speeds are similar to direct attached storage device speeds.

The disadvantage is that data requests and data compete for network bandwidth.

- ◆ **Storage Area Network Solutions**

A separate, dedicated data network consisting of servers and storage media that are connected through high-speed interconnects, such as Fibre Channel.

- ◆ **Novell iSCSI**

You can create a SAN using Novell iSCSI, which uses Novell eDirectory™ to manage iSCSI resources, including granting trustee rights and user file access. For information, see *OES 2 SP 1: iSCSI 1.1.3 for NetWare Administration Guide*.

- ◆ **Fault-Tolerant and High-Availability Architectures**

Use one or more of the following technologies:

- ♦ **Multiple Path I/O:** NSS helps prevent failure in the connection between the CPU and the storage device by automatically identifying multiple paths between each NetWare server and its storage devices.

For more information, see “[Managing Multipath I/O to Devices \(NetWare\)](#)” in the *OES 2 SP1: NSS File System Administration Guide*.

- ♦ **Software RAIDs:** NSS supports software RAIDs to improve storage availability and performance by enhancing data fault tolerance and I/O performance.

For more information, see “[Managing NSS Software RAID Devices](#)” in the *OES 2 SP1: NSS File System Administration Guide*.

- ♦ **Server Clusters:** You can configure up to 32 NetWare servers or Linux servers into a high-availability cluster where resources and services are dynamically allocated to any server in the cluster and automatically switched to another server if the hosting server fails.

By manually switching services, IT organizations can maintain and upgrade servers during production hours and eliminate scheduled downtime.

For more information, see the *OES 2 SP1: Novell Cluster Services 1.8.5 for NetWare Administration Guide* and the *OES 2 SP1: Novell Cluster Services 1.8.6 for Linux Administration Guide*.

13.1.6 NetWare Core Protocol Support (Novell Client Support) on Linux

Many organizations rely on Novell Client™ software and the NetWare Core Protocol™ (NCP) for highly secure access to file storage services.

Novell Storage Services (NSS) volumes are NCP volumes by nature, but you can also define Linux POSIX volumes as NCP volumes. The main difference in access control between NSS volumes and Linux POSIX volumes that are defined as NCP volumes is that NSS extended file and directory attributes are not available on Linux POSIX volumes.

The NCP server for OES 2 Linux lets you attach to Linux POSIX volumes that are defined as NCP volumes using Novell Client software. For more information, see [Section 17.6, “NCP Implementation and Maintenance,”](#) on page 214.

13.2 Planning OES File Storage

The following sections can help you plan for storage on your OES network:

- ♦ [Section 13.2.1, “Directory Structures,”](#) on page 135
- ♦ [Section 13.2.2, “File Service Support Considerations,”](#) on page 135
- ♦ [Section 13.2.3, “General Requirements for Data Storage,”](#) on page 135
- ♦ [Section 13.2.4, “OES 2 Linux Storage Planning Considerations,”](#) on page 135
- ♦ [Section 13.2.5, “NSS Planning Considerations,”](#) on page 140

13.2.1 Directory Structures

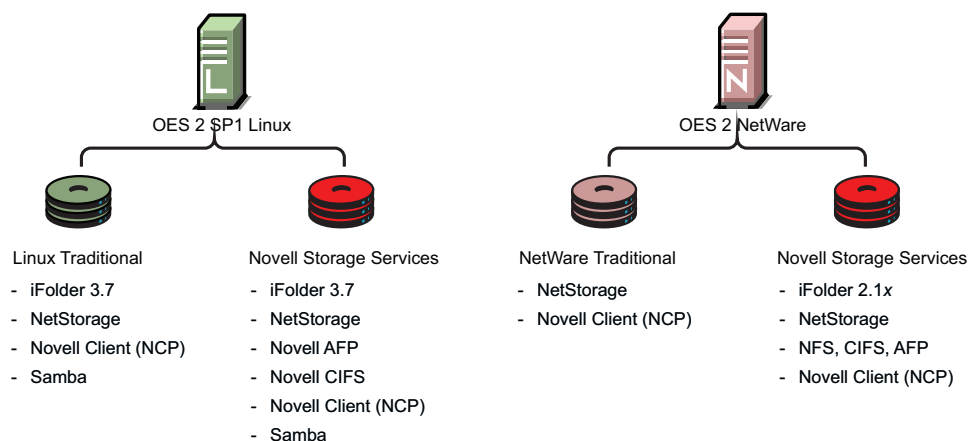
Linux: To plan the directory structures you need on OES 2 Linux, see “[Understanding Directory Structures in Linux POSIX File Systems](#)” in the *OES 2 SP1: File Systems Management Guide*.

Netware: To plan the directory structures you need on OES 2 NetWare, see “[Planning Directory Structures for NetWare Servers](#)” in the *OES 2 SP1: File Systems Management Guide*.

13.2.2 File Service Support Considerations

Figure 13-2 shows which file services can access which volume types.

Figure 13-2 File Services Supported on Volume Types



13.2.3 General Requirements for Data Storage

Finding the right storage solution requires you to identify your data storage requirements. You might want to compare your list of requirements against those described in “[Storage Solutions](#)” in the *OES 2 SP1: Storage and File Services Overview*.

13.2.4 OES 2 Linux Storage Planning Considerations

Not all data is the same. Not all workloads are the same. Not all file systems are the same. Matching your data and workloads to the available file systems and their capabilities lets you build efficient, scalable, and cost-effective solutions. This section discusses issues to consider when planning your file systems on OES 2 Linux servers, and includes the following topics:

- “[The Workgroup Environment](#)” on page 136
- “[File System Support](#)” on page 136
- “[File Access Protocol Support](#)” on page 138
- “[OES 2 Linux Workloads](#)” on page 139

The Workgroup Environment

When selecting a file system, it is important to understand the environment in which it operates. For OES 2 Linux, the primary target environment is the workgroup, which requires the following:

- ♦ A shared file system for Linux, Macintosh, and Windows desktops. Think of this as a NAS (network-attached storage) for desktops.
- ♦ A rich, flexible permissions model to maintain security while providing for the management of many different users with different permissions throughout the file system. The permissions must be granular, allow for delegation of permission management, and ease the administrative burden in an environment where change is constant.
- ♦ A robust enterprise-wide identity management system tied into authentication and file system permissions is a must.
- ♦ The capabilities for correcting end user mistakes that are made daily (accidental overwrites, deletes, etc.).
- ♦ Integration with collaboration tools.
- ♦ Data encryption on an individual user or group basis for compliance and security.
- ♦ Departmental Web servers and databases.
- ♦ SAN support to provide flexible storage management.
- ♦ Backup support for both desktop and server data, with rich tools for monitoring the health of the backup system and quickly locating and repairing problems with data protection.
- ♦ Regulatory compliance. Regulatory requirements are now pushing new models of protecting and storing employee-generated data that is in LAN systems. It is important to apply correct regulatory requirements only on those users to which they must be applied, and then to produce audits showing compliance.
- ♦ Highly available collaboration (e-mail) services, with rich tools to monitor, audit, and trend resource usage.

File System Support

OES 2 Linux offers support for four file systems: Novell Storage Services (NSS), Ext3, ReiserFS, and XFS. Following is an explanation of each file system and the pros and cons of using them in the workloads supported by OES 2.

- ♦ “Novell Storage Services (NSS)” on page 136
- ♦ “Ext2” on page 137
- ♦ “Ext3” on page 137
- ♦ “ReiserFS” on page 137
- ♦ “XFS” on page 138

Novell Storage Services (NSS)

- ♦ Supported only through EVMS; not currently supported through LVM.
- ♦ Best for shared LAN file serving; excellent scalability in the number of files
- ♦ Journalled
- ♦ Novell Trustee Model and NSS directory and file attributes (such as Rename Inhibit) provide access control that is much richer than POSIX

The Novell Storage Services file system is used in NetWare 5.0 and above, and most recently is open sourced and included in the SUSE[®] Linux Enterprise Server (SLES) 9 SP1 Linux distribution and later (used in the Novell Open Enterprise Server Linux product).

The NSS file system is unique in many ways, especially in its ability to manage and support shared file services from simultaneous different file access protocols. It is designed to manage access control (using a unique model, called the Novell Trustee Model, that scales to hundreds of thousands of different users accessing the same storage securely) in enterprise file sharing environments.

NSS and its predecessor NWFS are the only file systems that can restrict the visibility of the directory tree based on the user ID accessing the file system. NSS and NWFS have built-in ACL (access control list) rights inheritance. NSS includes mature and robust features tailored for the file-sharing environment of the largest enterprises. The file system also scales to millions of files in a single directory. NSS also supports multiple data streams and rich metadata; its features are a superset of existing file systems on the market for data stream, metadata, name space, and attribute support.

Ext2

- ♦ Legacy file system
- ♦ Not journaled
- ♦ POSIX access control

Ext2 does not maintain a journal, so it is generally not desirable to use it for any server that needs high availability, with one important exception. If the server is running as a Xen VM guest, you should format the `/boot` partition with Ext2 as explained in “[Paravirtual Mode and Journaling File Systems](http://www.novell.com/documentation/sles10/xen_admin/data/sec_xen_filesystem.html)” (http://www.novell.com/documentation/sles10/xen_admin/data/sec_xen_filesystem.html) in the *Virtualization with Xen* (http://www.novell.com/documentation/sles10/xen_admin/data/bookinfo.html) guide.

Ext3

- ♦ Most popular Linux file system; limited scalability in size and number of files
- ♦ Journaled
- ♦ POSIX extended access control

The Ext3 file system is a journaled file system that has the widest use in Linux today. It is regarded by many in the Linux user community as the default Linux file system. It is quite robust and quick, although it does not scale well to large volumes or a great number of files.

A scalability feature has been added called H-trees, which significantly improved Ext3's scalability. However, it is still not as scalable as some of the other file systems. With H-trees, it scales similarly to NTFS. Without H-trees, Ext3 does not handle more than about 5,000 files in a directory.

ReiserFS

- ♦ Best performance and scalability when the number of files is great and/or files are small
- ♦ Journaled
- ♦ POSIX extended access control

The Reiser file system is the default file system in SUSE Linux distributions. ReiserFS was designed to remove the scalability and performance limitations that exist in Ext2 and Ext3 file systems.

Reiser scales and performs extremely well on Linux, outscaling Ext3 with H-trees. In addition, Reiser was designed to use disk space very efficiently. As a result, it is the best file system on Linux where there are a great number of small files in the file system. Because collaboration (e-mail) and many Web servings applications have many small files, Reiser is best suited for these types of workloads.

XFS

- ♦ Best for extremely large file systems, large files, and lots of files
- ♦ Journaled (an asymmetric parallel cluster file system version is also available)
- ♦ POSIX extended access controls

The XFS file system is open source and is included in major Linux distributions. It originated from SGI (Irix) and was designed specifically for large files and large volume scalability.

Video and multimedia files are best handled by this file system. Scaling to petabyte volumes, it also handles very large amounts of data. It is one of the few file systems on Linux that supports HSM data migration.

File Access Protocol Support

OES 2 Linux offers support for a variety of file access protocols.

- ♦ **AFP:** The Apple Filing Protocol (AFP) is a network protocol that offers file services for Mac OS X and the original Mac OS.
- ♦ **CIFS (Novell CIFS and Samba):** The Common Internet File Services (CIFS) protocol is the protocol for Windows networking and file services.
Novell CIFS is a ported version of the CIFS file service traditionally available only on NetWare but now available for OES 2 Linux starting with SP1.
Samba is an open source software version of CIFS based on extensive use and analysis of the wire protocol of Microsoft Windows machines.
- ♦ **FTP:** The File Transfer Protocol (FTP) is one of the most common and widely used simple protocols in the Internet. Virtually all platforms and devices support FTP at some level, but it is a very simple protocol, only allowing for uploading and downloading of files.
- ♦ **HTTP:** The Hypertext Transfer Protocol (HTTP) is the dominant protocol on the World Wide Web today, and is the one “spoken” by Web browser clients and Web servers. It is like FTP in being designed strictly for transfers of HTML (Hypertext Markup Language) and additional markup languages that have been invented, such as XML (Extensible Markup Language).
- ♦ **NCP:** The NetWare Core Protocol (NCP) is the client server protocol developed by Novell for supporting DOS, Windows, OS/2*, Macintosh, UNIX* (UnixWare*), and Linux for shared file services.

The NCP Server on Linux includes emulation for the Novell Trustee Model and inheritance plus visibility when it runs on traditional POSIX file systems such as Ext3 and Reiser. When it runs on NSS on Linux, these capabilities are synchronized with the NSS File system and its extended directory and file attributes, such as Rename Inhibit.

OES 2 Linux Workloads

Each file system has its strengths and weaknesses depending on the workload the file system supports. This section gives some guidelines for picking and building the right file system for a given workload. In determining which file system to use for a particular workload, consider your environment and the following explanation of each workload to determine which file system best meets your workload environment.

Table 13-2 *File System Support per Workload*

Workload Type	NSS File System	Ext3 File System	Reiser File System	XFS File System
File serving – Application server	Supported	Supported	Recommended	Recommended
File serving – end user files	Recommended	Supported	Supported	Supported
Network printing (iPrint)	Recommended	Recommended	Recommended	Recommended
iFolder	Recommended	Supported	Recommended	Recommended
Collaboration (GroupWise®)	Recommended	Supported	Recommended	Recommended
Cluster services	Supported	Supported	Supported	Supported
Dynamic Storage Technology	Supported	Not Supported	Not Supported	Not Supported

The following sections provide a brief summary of considerations for each workload listed in [Table 13-2](#).

File Serving (NAS)

Generally there are two types of NAS use cases: Serving files to application servers in a tiered service oriented architecture (SOA), and serving files to end user desktops and workstations. The former has minimal access control requirements. The latter has quite heavy access control requirements.

Typically for serving files to application servers (traditional NAS), you would choose a file system that is scalable and fast. Reiser and XFS would be good choices in this environment. For file serving to end user workstations, the access control and security management capabilities of the NSS file systems with CIFS and NCP file access protocols are important.

The NSS model does better than the other file systems for very large numbers of users. It allows for security between users and also allows for very fine granular sharing between given users and groups. NSS includes a visibility feature implemented in the file system that prevents unauthorized users from even seeing subdirectory structures they don't have rights to access.

Network Printing (iPrint)

iPrint is file system agnostic. There is no noticeable difference in performance or reliability on any of the file systems.

iFolder

Novell iFolder does not depend on a particular file system. Based on the client workload, the file system should be chosen at the server side. Because it mostly serves user data, a file system that can scale with a large number of files is the best suited in most deployments, making Reiser and NSS the best bets. Novell iFolder maintains its own ACL, so having an NSS file system that supports a rich ACL might be redundant.

GroupWise

GroupWise deals with many little files. Because only the application process is accessing the file system, the added overhead of the rich ACL and file attributes found in NSS is redundant. The necessary characteristics are a file system whose performance remains relatively constant regardless of the number of files that are in the volume, and that performs well with small files. Best bets would be ReiserFS, XFS, and NSS. Ext3 does not handle large systems well (where you have more than 10,000 files in the system).

Novell Cluster Services

Although Novell Cluster Services™ does not depend on a particular file system, you must use the same file systems from node to node. For example, if you are using NSS on one node, you need to use NSS on the failover node as well.

Dynamic Storage Technology

Dynamic Storage Technology does not depend on a particular file system in principle; however, it is currently supported only on NSS volumes.

Novell plans to add support for additional file systems in the future. When that happens, it will be important to remember that file systems cannot be mixed between volumes and shadow volumes. For example, if you choose to shadow an NSS volume, the secondary volume must also be NSS.

13.2.5 NSS Planning Considerations

Consider the following when planning for NSS:

- ♦ “Device Size Limit” on page 140
- ♦ “Other NSS Planning Topics” on page 140

Device Size Limit

NSS recognizes logical or physical devices up to 2 terabytes (TB) in size. If you have a storage disk larger than 2 TB, use the storage device’s management utility to carve the disk into smaller logical devices to use with the NSS file system.

This is especially important to remember when planning for NSS volumes on Linux because the size limit for Linux POSIX volumes is 8 TB.

Other NSS Planning Topics

To plan for NSS volumes—including prerequisites, security considerations, and moving volumes between Linux and NetWare—see “Planning NSS Storage Solutions” in the *OES 2 SP1: NSS File System Administration Guide*.

13.3 Coexistence and Migration of Storage Services

The following sections summarize the coexistence and migration issues related to storage services.

- ♦ [Section 13.3.1, “MySQL,” on page 141](#)
- ♦ [Section 13.3.2, “OES 2 Linux Options,” on page 141](#)
- ♦ [Section 13.3.3, “OES 2 NetWare Options,” on page 142](#)

13.3.1 MySQL

OES 2 includes the open source MySQL database server on both the NetWare and Linux platforms. When combined with a Web application and a Web server, MySQL is a very reliable and scalable database for use in hosting e-commerce and business-to-business Web applications.

NOTE: The more powerful PostgreSQL* database server comes with SUSE Linux Enterprise Server 10. It has also been ported to the NetWare platform and is available separately as open source software.

13.3.2 OES 2 Linux Options

OES 2 Linux provides support for Novell Storage Services (NSS) as well as Linux POSIX file systems.

- ♦ [“NSS Volumes” on page 141](#)
- ♦ [“Linux POSIX File Systems” on page 142](#)

NSS Volumes

NSS volumes are cross-compatible between NetWare and Linux.

To use NSS on OES 2 Linux, you must have a disk available to be managed by Enterprise Volume Management System (EVMS). The boot partition (such as `/boot` for Grub) and system partition (such as for the swap and system volumes) are managed by Logical Volume Manager 2 (LVM2). Any disk managed by LVM2 cannot be managed by EVMS, which makes the disks where the boot partition and system partition reside unavailable to NSS.

If you have a single-disk server that you want to install OES 2 for Linux on and create an NSS volume, see [“Installing Linux with EVMS as the Volume Manager of the System Device”](#) in the *OES 2 SP1: Linux Installation Guide*.

On OES 2 Linux, you can use NSS volumes only as data volumes. Configure NSS pools and volumes in iManager or NSSMU after the server installation completes successfully.

Starting with OES 1 SP1 NetWare and OES 2 Linux, a new metadata structure provides enhanced support for hard links. After you install or upgrade your operating system, you must upgrade the media format in order to use the new metadata structure; some restrictions apply. For more information, see [“Upgrading the NSS Media Format”](#) in the *OES 2 SP1: NSS File System Administration Guide*.

For additional information about coexistence and migration of NSS volumes, as well as access control issues for NSS on Linux, see “[Cross-Platform Issues for NSS](#)” in the *OES 2 SP1: NSS File System Administration Guide*.

Linux POSIX File Systems

You can install NCP Server for Linux to provide NetWare Core Protocol access to Linux POSIX file systems. This allows users running the Novell Client software to map drives to the Linux file system data, with access controls being enforced by NCP.

For more information on using NCP Server for Linux in OES, see the *OES 2 SP1: NCP Server for Linux Administration Guide*.

Users can access data storage on OES 2 NetWare and OES 2 Linux servers through a number of methods. For more information, see “[Overview of File Services](#)” on page 191.

13.3.3 OES 2 NetWare Options

OES 2 NetWare supports both the NetWare Traditional file system and Novell Storage Services (NSS).

- ♦ “[NetWare Traditional File System](#)” on page 142
- ♦ “[NSS Volumes](#)” on page 142

NetWare Traditional File System

After upgrading an older NetWare server to OES 2 NetWare, it is possible for a NetWare Traditional file system volume to still reside on that server. You can continue to use Traditional volumes with OES 2 NetWare, or you can upgrade them to NSS.

For information on converting Traditional volumes to NSS, see “[Upgrading NetWare 5.1 NSS Volumes and NetWare Traditional Volumes to NSS Volumes](#)” in the *OES 2 SP1: NSS File System Administration Guide*.

If you want to migrate data from a Traditional volume to an NSS volume on OES 2 Linux, use the Novell Server Consolidation Utility 4.0 or later. You must first install NFS name space support on the Traditional volume.

For more information on migrating data from NetWare to Linux, see “[Understand NetWare-to-Linux Data Migration Issues](#)” in the *Novell Server Consolidation and Migration Toolkit Administration Guide*.

You can upgrade both NetWare Traditional volumes and Legacy NSS volumes to OES 2.

For more information, see “[Upgrading Legacy NSS and NetWare Traditional Volumes](#)” in the *OES 2 SP1: NSS File System Administration Guide*.

NSS Volumes

NSS volumes are cross-compatible between NetWare and Linux servers. You can mount an NSS data volume on either kernel—Linux or NetWare—and move it between them as long as they both support the same media format. In a clustered SAN, volumes that were originally created on a NetWare server can fail over between kernels, allowing for full data and file system feature preservation when migrating data to Linux.

Supporting NSS volumes in a mixed environment and migrating data between OES platforms presents a number of possibilities for your storage solutions. However, to ensure success you must fully understand the proper methods and limitations involved.

For additional information about coexistence and migration of NSS volumes, as well as access control issues for NSS on Linux, see “[Migrating NSS Devices from NetWare to OES 2 Linux](#)” in the *OES 2 SP1: NSS File System Administration Guide*.

13.4 Initial Setup Is Required for NetWare

During installation, NetWare creates an NSS system pool (`sys`) and volume (`sys:`) on your server’s primary hard drive. You must create other NSS pools and volumes before you can use your system effectively. For information, see the *OES 2 SP1: NSS File System Administration Guide*.

13.5 Configuring and Maintaining Storage

- [Section 13.5.1, “Managing Directories and Files,”](#) on page 143
- [Section 13.5.2, “Managing NSS,”](#) on page 143
- [Section 13.5.3, “Optimizing Storage Performance,”](#) on page 145
- [Section 13.5.4, “Disk Management on NetWare,”](#) on page 145

13.5.1 Managing Directories and Files

To learn about managing directories and files for the OES 2 server type, see the following sections in the *OES 2 SP1: File Systems Management Guide*.

- **Linux:** “[Understanding Directory Structures in Linux POSIX File Systems](#)”
- **NetWare:** “[Managing Folders and Files on NSS and NetWare Traditional Volumes](#)”

13.5.2 Managing NSS

Use the links in [Table 13-3](#) to find information on the many management tasks associated with NSS volumes.

Table 13-3 *NSS Management*

Category/Feature	Description	Link
Archive and Version Services	Use Archive and Version Services with NSS volumes to save interval-based copies of files that can be conveniently restored by administrators and users.	OES 2 SP1: Novell Archive and Version Services 2.1 for Linux Administration Guide OES 2: Novell Archive and Version Services 2.1 for NetWare Administration Guide
Compression	Conserve disk space and increase the amount of data a volume can store.	“Managing Compression on NSS Volumes” in the <i>OES 2 SP1: NSS File System Administration Guide</i>

Category/Feature	Description	Link
Console Commands	Manage NSS volumes at an OES 2 NetWare server console, or an OES 2 Linux terminal console via the NSS Console (<code>nsscon</code>) utility.	“NSS Commands” and “NSS Utilities” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Distributed File Services (DFS)	Use DFS junctions to transparently redirect data requests, split volumes while maintaining transparent access, and quickly move volume data to another volume.	OES 2 SP1: Novell Distributed File Services Administration Guide
Encryption	Create and manage encrypted NSS volumes that make data inaccessible to software that circumvents normal access control.	“Managing Encrypted NSS Volumes” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
EVMS	Use EVMS, which is required for NSS, to manage volumes on Linux, including the system (root [/]) volume if NSS is installed on the same disk.	“Using EVMS to Manage Devices with NSS Volumes (Linux)” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Hard Links	Create multiple names for a single file in the same or multiple directories in an NSS volume.	“Managing Hard Links” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Monitoring	Monitor NSS file systems.	“Monitoring the Status of the NSS File System and Services” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Multipath Support (NetWare)	Manage the dynamic, multiple, redundant connection paths NSS creates between a NetWare server and its external storage devices.	“Managing Multipath I/O to Devices (NetWare)” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Partitions	Manage partitions on NSS volumes.	“Managing Partitions” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Pools	Create and manage NSS pools.	“Managing NSS Pools” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Quotas	Set space restrictions for users and directories to control storage usage.	“Managing Space Quotas for Volumes, Directories, and Users” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Salvage subsystem	Use the salvage subsystem to make deleted files and directories available for undelete or purge actions.	“Salvaging and Purging Deleted Volumes, Directories, and Files” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Tools	Learn about the various tools available to manage NSS volumes, the tool capabilities, and how to use them.	“Management Tools for NSS” in the <i>OES 2 SP1: NSS File System Administration Guide</i>

Category/Feature	Description	Link
Troubleshooting	Troubleshoot NSS on OES 2 Linux and OES 2 NetWare.	“Troubleshooting the NSS File System” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
File System Trustees and Attributes	Control user access to data by setting trustees, trustee rights, and inherited rights filters for files. Control file behavior by setting file and folder attributes.	“Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Volumes	Create and manage NSS volumes in NSS pools.	“Managing NSS Volumes” in the <i>OES 2 SP1: NSS File System Administration Guide</i>

13.5.3 Optimizing Storage Performance

- ♦ **NSS on Linux:** [“Tuning NSS Performance on Linux” in the *OES 2 SP1: NSS File System Administration Guide*](#)
- ♦ **NSS on NetWare:** [“Tuning NSS Performance on NetWare” in the *OES 2 SP1: NSS File System Administration Guide*](#)

13.5.4 Disk Management on NetWare

Disk management is obviously central to providing storage services. To plan how you will add, allocate, maintain, and remove disks accessed by OES 2 NetWare servers, see [OES 2 SP1: NetWare Server Disks and Storage Devices](#).

eDirectory, LDAP, and Domain Services for Windows

This section discusses the following topics:

- ♦ [Section 14.1, “Overview of Directory Services,” on page 147](#)
- ♦ [Section 14.2, “eDirectory,” on page 148](#)
- ♦ [Section 14.3, “LDAP \(eDirectory\),” on page 149](#)
- ♦ [Section 14.4, “Domain Services for Windows,” on page 150](#)

14.1 Overview of Directory Services

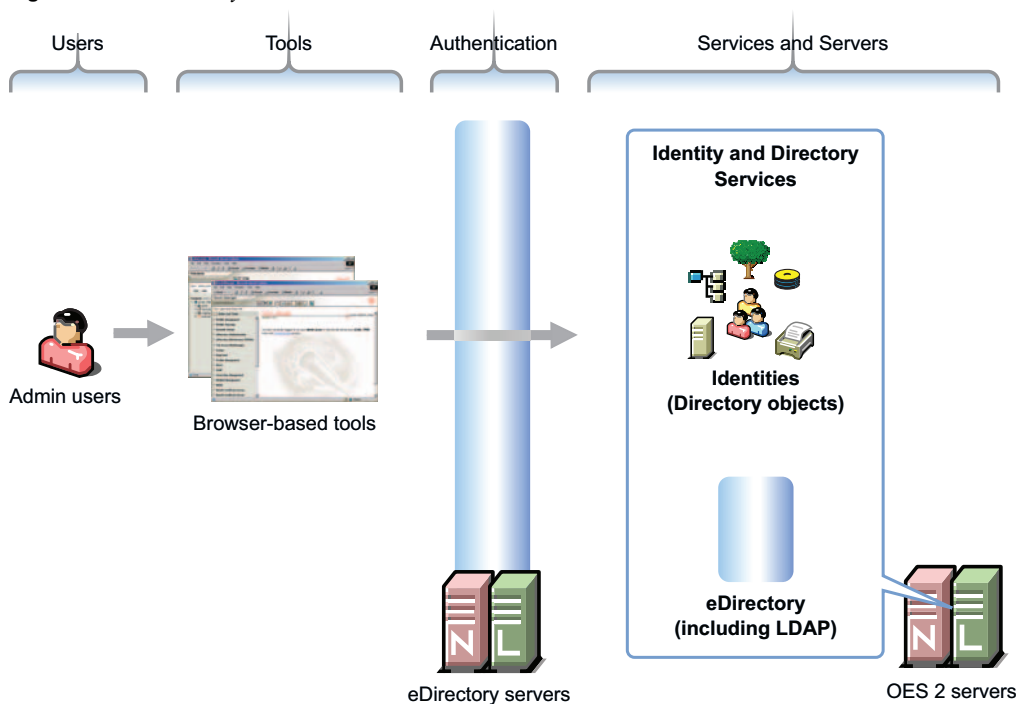
Storing and managing network identities in directory services is a fundamental expectation for networking.

In the simplest terms, Novell® eDirectory™ is a tree structure containing a list of objects (or identities) that represent network resources, such as the following:

- ♦ Network users
- ♦ Servers
- ♦ Printers
- ♦ Applications

eDirectory is designed to provide easy, powerful, and flexible management of network resources (including eDirectory itself) in ways that no other directory service can match. You can administer eDirectory through the same browser-based tools on both OES platforms.

For more information, see [Chapter 14, “eDirectory, LDAP, and Domain Services for Windows,” on page 147](#).

Figure 14-1 eDirectory Overview

14.2 eDirectory

Novell eDirectory is the central, key component of Novell Open Enterprise Server (OES) and provides the following:

- ♦ Centralized identity management
- ♦ The underlying infrastructure for managing your network servers and the services they provide
- ♦ Access security both within the firewall and from the Web

This section discusses the following tasks:

- ♦ [Section 14.2.1, “Installing and Managing eDirectory on OES,” on page 148](#)
- ♦ [Section 14.2.2, “Planning Your eDirectory Tree,” on page 149](#)
- ♦ [Section 14.2.3, “eDirectory Coexistence and Migration,” on page 149](#)

14.2.1 Installing and Managing eDirectory on OES

The tools you can use to install and manage eDirectory on OES are outlined in the following sections.

- ♦ [“OES Installation Programs” on page 148](#)
- ♦ [“iManager” on page 149](#)

OES Installation Programs

OES requires that eDirectory be installed by using the NetWare® Install or the YaST-based install for OES Linux.

IMPORTANT: Other utilities, such as ndsconfig and ndsmanage, are not supported for installing or removing eDirectory on OES servers.

iManager

iManager is the OES eDirectory management tool and is used for all eDirectory management and most OES component management tasks, including the following:

- ♦ Creating eDirectory objects, including User and Group objects
- ♦ Managing eDirectory objects
- ♦ Configuring and managing OES service component controls in eDirectory
- ♦ Accessing other OES component management tools

For information on using iManager, see the *Novell iManager 2.7.2 Administration Guide*.

14.2.2 Planning Your eDirectory Tree

If you don't have eDirectory installed on your network, it is critical that you and your organization take time to plan and design your eDirectory tree prior to installing OES.

The *OES2 SP2: Lab Guide for Linux and Virtualized NetWare* provides an introduction to eDirectory planning that you might find useful for getting started with eDirectory.

For detailed information on getting started using eDirectory, see “**Designing Your Novell eDirectory Network**” in the *Novell eDirectory 8.8 Installation Guide*.

To learn what's new in eDirectory 8.8, see the *Novell eDirectory 8.8 Whats New Guide*.

14.2.3 eDirectory Coexistence and Migration

Novell Directory Services® (NDS®) was introduced with NetWare 4.0. The successor to NDS, Novell eDirectory, is also available for Microsoft Windows, Red Hat*, and SUSE® versions of Linux, as well as various flavors of UNIX (Solaris*, AIX*, and HP-UX*).

As eDirectory has evolved, backward compatibility issues have arisen. For example, moving from NetWare 4.x to 5.x involved not only upgrading NDS, but also moving from IPX™ to TCP/IP. This transition brought significant changes to the core schema and security-related components. Novell has consistently provided the migration tools and support required to migrate to new eDirectory versions.

OES 2 Linux includes eDirectory 8.8. For those upgrading an existing OES 1 SP2 NetWare (NetWare 6.5 SP6) server, eDirectory 8.7.3 is still available. New NetWare installations require eDirectory version 8.8.

For complete coexistence and migration information and instructions, see “**Migrating to eDirectory 8.8 SP4**” in the *Novell eDirectory 8.8 Installation Guide*.

14.3 LDAP (eDirectory)

This section contains information about LDAP support in OES.

- ♦ **Section 14.3.1, “Overview of eDirectory LDAP Services,” on page 150**

- [Section 14.3.2, “Planning eDirectory LDAP Services,” on page 150](#)
- [Section 14.3.3, “Migration of eDirectory LDAP Services,” on page 150](#)
- [Section 14.3.4, “eDirectory LDAP Implementation Suggestions,” on page 150](#)

14.3.1 Overview of eDirectory LDAP Services

Lightweight Directory Access Protocol (LDAP) Services for Novell eDirectory is a server application that lets LDAP clients access information stored in eDirectory.

Most OES 2 services leverage the LDAP server for eDirectory for authentication, as illustrated in the service overviews in this guide.

14.3.2 Planning eDirectory LDAP Services

LDAP for eDirectory provides LDAP authentication for the objects stored in eDirectory. As you plan your eDirectory tree, be sure you understand the information in [“Understanding LDAP Services for Novell eDirectory”](#) in the *Novell eDirectory 8.8 Administration Guide*.

14.3.3 Migration of eDirectory LDAP Services

If you have users in an OpenLDAP database and you want to migrate them to eDirectory, you can use the Novell Import Conversion Export (ICE) utility. For more information, see [“Novell eDirectory Management Utilities”](#) in the *Novell eDirectory 8.8 Administration Guide*.

14.3.4 eDirectory LDAP Implementation Suggestions

For help with setting up and using LDAP for eDirectory, refer to [“Configuring LDAP Services for Novell eDirectory”](#) in the *Novell eDirectory 8.8 Administration Guide*.

14.4 Domain Services for Windows

Novell Domain Services for Windows (DSfW) allows eDirectory users on Windows workstations to access storage on both OES servers and Windows servers through native Windows and Active Directory authentication and file service protocols.

DSfW enables companies with Active Directory and Novell eDirectory deployments to achieve better coexistence between the two platforms.

- Users can work in a pure Windows desktop environment and still take advantage of some OES back-end services and technology, without the need for a Novell Client™ or even a matching local user account on the Windows workstation.
- Network administrators can use Microsoft Management Console (MMC) to administer users and groups within the DSfW domain, including their access rights to Samba-enabled storage on OES servers.

This section discusses the following:

- [Section 14.4.1, “Graphical Overview of DSfW,” on page 151](#)
- [Section 14.4.2, “Planning Your DSfW Implementation,” on page 154](#)
- [Section 14.4.3, “Implementing DSfW on Your Network,” on page 154](#)

14.4.1 Graphical Overview of DSfW

- ♦ “File Access” on page 151
- ♦ “User Management” on page 152
- ♦ “Storage Management” on page 153

File Access

Figure 14-2 DSfW File Access Overview

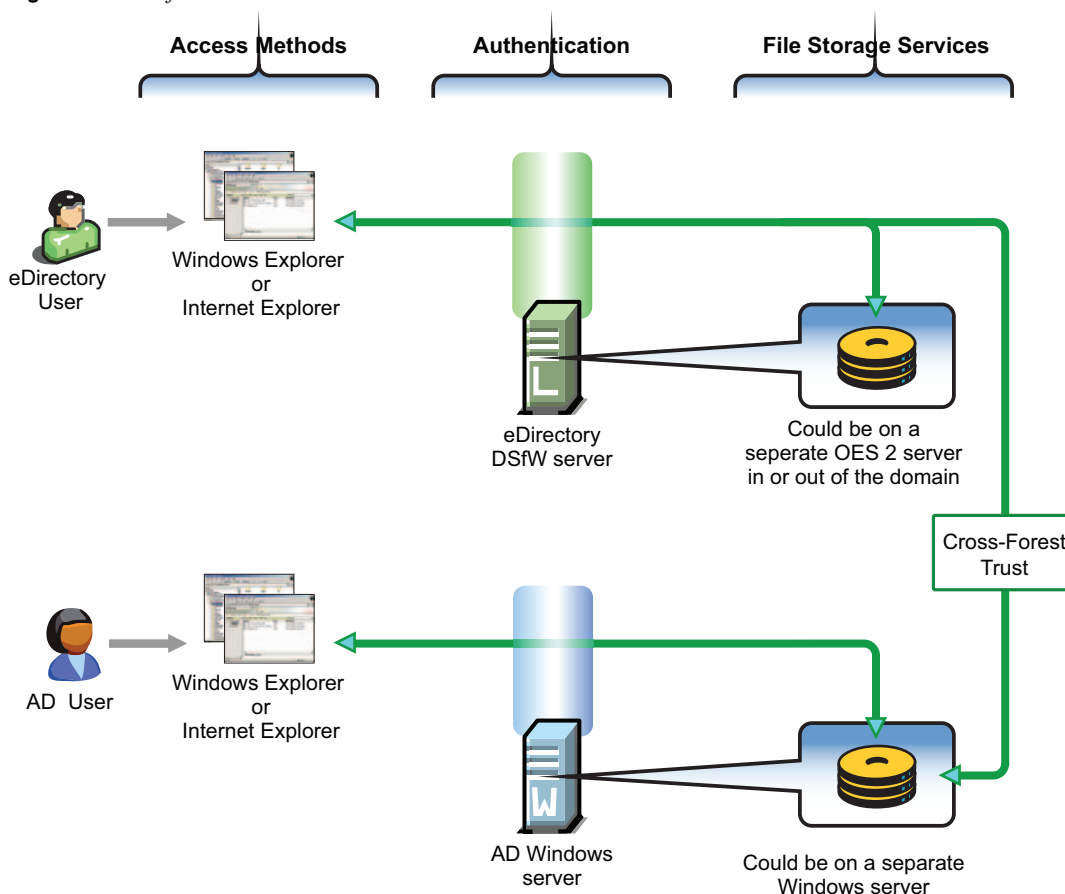


Table 14-1 *DSfW File Access*

Access Methods	Authentication	File Storage Services
eDirectory and Active Directory users on Windows workstations can access files through Windows Explorer (CIFS) or Internet Explorer (WebDAV Web Folders). No Novell Client can be on the machine.	For eDirectory users, file service access is controlled by authentication through the eDirectory server using common Windows authentication protocols, including Kerberos*, NTLM, and SSL/TLS.	On OES 2 servers, file storage services are provided by Samba to NSS or traditional Linux file systems.
Unlike Windows workgroup or Novell Samba, the user doesn't need to have a matching username and password on the local workstation.	For AD users, file service access is controlled by authentication through the AD server.	For eDirectory users, access to storage on Windows servers is available through a cross-forest trust. Access rights are granted by the AD administrator following the establishment of the cross-forest trust.
Although not shown, Novell Client users can also access files through a normal NCP™ connection.		

User Management

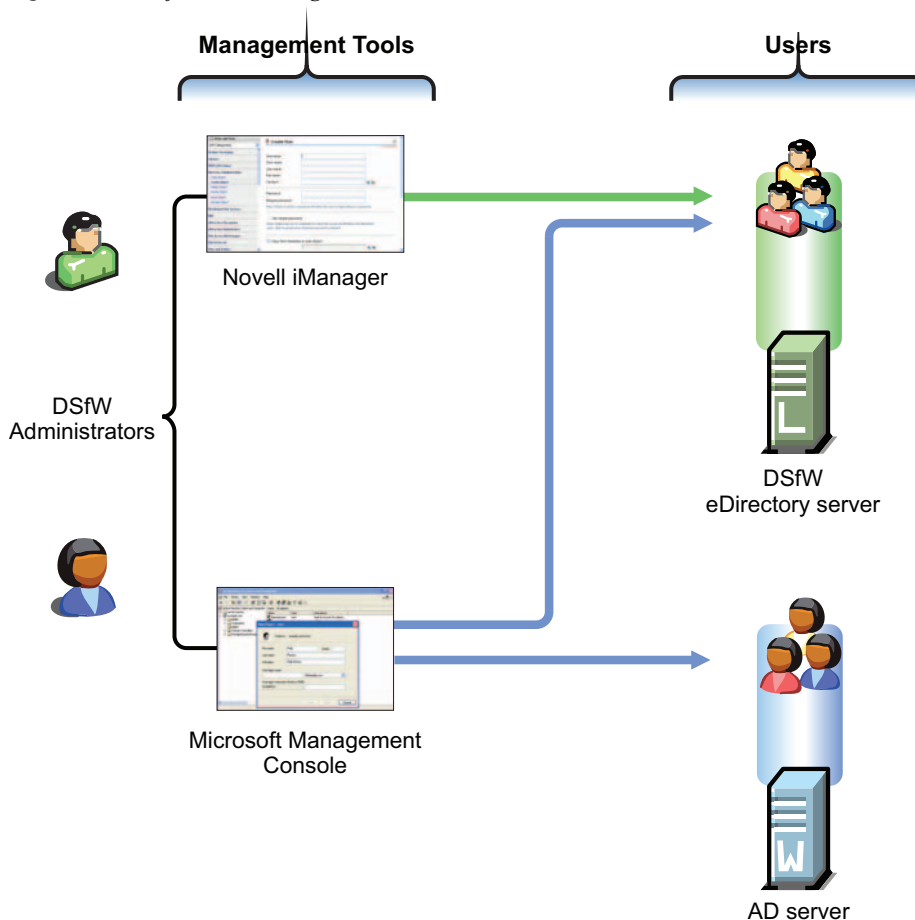
Figure 14-3 *DSfW User Management Overview*

Table 14-2 *DSfW User Management*

Management Tools	Users
iManager manages DSfW users like other eDirectory users.	DSfW users must have the Default Domain Password policy assigned and a valid Universal Password.
MMC manages both AD users and DSfW users as though they were AD users.	DSfW users are automatically enabled for Samba and LUM.

Storage Management

Figure 14-4 *DSfW Storage Management Overview*

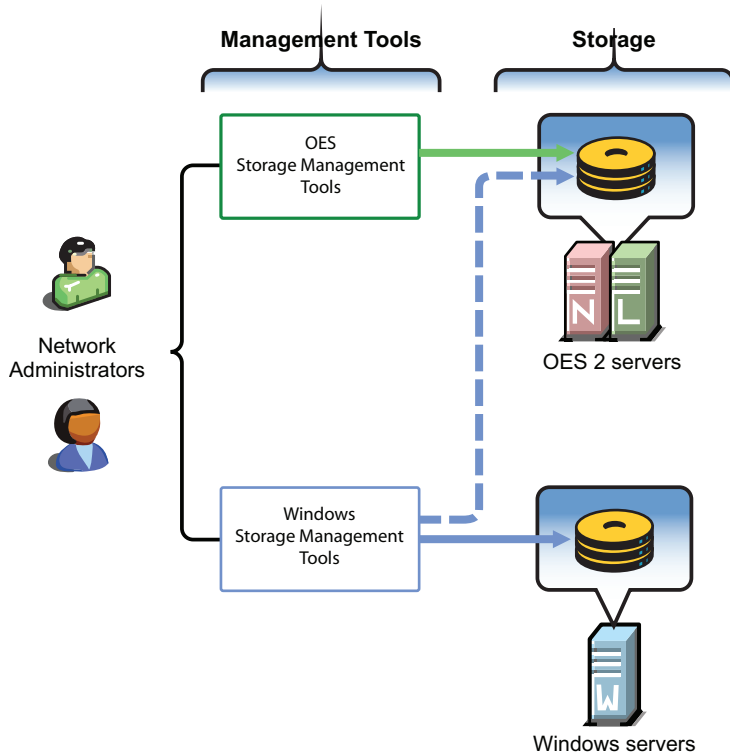


Table 14-3 *DSfW Storage Management*

Management Tools	Storage
Network administrators use native OES and Windows storage management tools to create and manage storage devices on OES and Windows servers, respectively.	Storage devices on OES 2 servers can be either NSS or traditional Linux volumes. Samba management standards apply to both volume types.
Windows management tools can also manage share access rights and POSIX file system rights on DSfW storage devices after the shares are created. They cannot create the shares or perform other device management tasks.	

14.4.2 Planning Your DSfW Implementation

For planning information, see the *OES 2 SP1: Domain Services for Windows Administration Guide*.

14.4.3 Implementing DSfW on Your Network

This section highlights some of the potential caveats to consider when installing DSfW. For complete information, see the *OES 2 SP1: Domain Services for Windows Administration Guide*, especially the “**Troubleshooting DSfW**” section.

- ♦ “Universal Password in a Name-Mapped Scenario” on page 154
- ♦ “DSfW Must Be Installed at the Root of an eDirectory Partition” on page 154
- ♦ “Hierarchical Placement of Users in the eDirectory Tree” on page 155
- ♦ “OES 2 Service Limitations” on page 155
- ♦ “Domain and Container Names Must Match” on page 155
- ♦ “Install DSfW on a New OES 2 Linux Server When Possible” on page 155
- ♦ “DNS Configuration” on page 155

Universal Password in a Name-Mapped Scenario

If you install DSfW into an existing tree and your users don’t currently have a Universal Password policy assigned, they won’t be able to log in without the Novell Client until the Universal Password has been set.

Therefore, you should consider implementing Universal Password and giving users an opportunity to log into the network before installing DSfW. Logging in after a password policy is in place creates a Universal Password for users so that their transition to DSfW is seamless.

DSfW Must Be Installed at the Root of an eDirectory Partition

You must install DSfW in the root container or an eDirectory partition, either one that currently exists or one that you create for DSfW. In both cases, the first DSfW server installed in the partition becomes the master of the partition.

Hierarchical Placement of Users in the eDirectory Tree

DSfW users must reside in the same eDirectory partition where DSfW is installed, either in the same container or in a container below it in the hierarchy. Therefore, DSfW should be installed high enough in the eDirectory tree that it encompasses all of the users that you want to enable for DSfW access.

OES 2 Service Limitations

Only designated OES 2 services can be installed on a DSfW server. For more information, see “[Unsupported Service Combinations](#)” in the *OES 2 SPI: Domain Services for Windows Administration Guide*.

Domain and Container Names Must Match

When you install DSfW, the Domain name you specify must match the name of the container you are installing into. For more information, see “[Installing the First DSfW Server in a New eDirectory Tree](#)” in the *OES 2 SPI: Domain Services for Windows Administration Guide*.

Install DSfW on a New OES 2 Linux Server When Possible

Because of the service limitations mentioned in [OES 2 Service Limitations](#), Novell strongly recommends that you install DSfW on a new server.

DNS Configuration

As you set up DNS, observe the following guidelines:

- ♦ **First DSfW Server (FRD):** This should point to itself as the primary DNS server, and to the network DNS server as the secondary DNS server (if applicable).
- ♦ **Subsequent DSfW Servers:** These must point to the FRD as their primary DNS server and optionally to the network DNS server as their secondary DNS server.
- ♦ **DSfW Workstations:** These must be able to resolve the FRD of the DSfW forest. For example, you might configure workstations to point to the FRD as their primary DNS server and to the network DNS server secondarily. Or if the network DNS server is configured to forward requests to the DSfW server, then workstations could point to it as their primary DNS server.

Users and Groups

Networks exist to serve users and groups of users. Open Enterprise Server 2 provides strong user and group management through eDirectory™ and its associated technologies.

- ♦ [Section 15.1, “Creating Users and Groups,” on page 157](#)
- ♦ [Section 15.2, “Linux User Management: Access to Linux for eDirectory Users,” on page 157](#)
- ♦ [Section 15.3, “Identity Management Services,” on page 166](#)
- ♦ [Section 15.4, “Using the Identity Manager 3.5 Bundle Edition,” on page 167](#)

15.1 Creating Users and Groups

All OES 2 services require that you create User objects to represent the users on your system. The Linux User Management (LUM) and Samba components on OES 2 Linux also require that you create a LUM-enabled Group object that you can assign the users to.

In addition to these basic objects, it is usually helpful to organize your tree structure by using Organizational Unit objects to represent the structure of your organization and to serve as container objects to help manage the users, groups, servers, printers, and other organization resources you manage through eDirectory.

The *Lab Guide for OES 2 Linux* provides basic instructions for creating container objects as well as Group and User objects in eDirectory.

For more information about Samba, see [Creating eDirectory Users for Samba](#) in the *OES2 SPI: Samba Administration Guide*.

For detailed information on understanding, creating, and managing the various objects your organization might require, see the *Novell eDirectory 8.8 Administration Guide*.

15.2 Linux User Management: Access to Linux for eDirectory Users

Users and groups on NetWare® servers are created in and managed through eDirectory; users and groups on Linux servers are usually created locally and managed according to the POSIX (Portable Operating System Interface) standard.

Because Open Enterprise Server provides services running on both Linux and NetWare, Novell® has developed a technology that lets eDirectory users also function as “local” POSIX users on Linux servers. This technology is called Linux User Management or LUM.

The following sections outline the basic principles involved in Novell LUM and cover the following topics:

- ♦ [Section 15.2.1, “Overview,” on page 158](#)
- ♦ [Section 15.2.2, “Planning,” on page 163](#)
- ♦ [Section 15.2.3, “Coexistence and Migration,” on page 164](#)
- ♦ [Section 15.2.4, “LUM Implementation Suggestions,” on page 164](#)

15.2.1 Overview

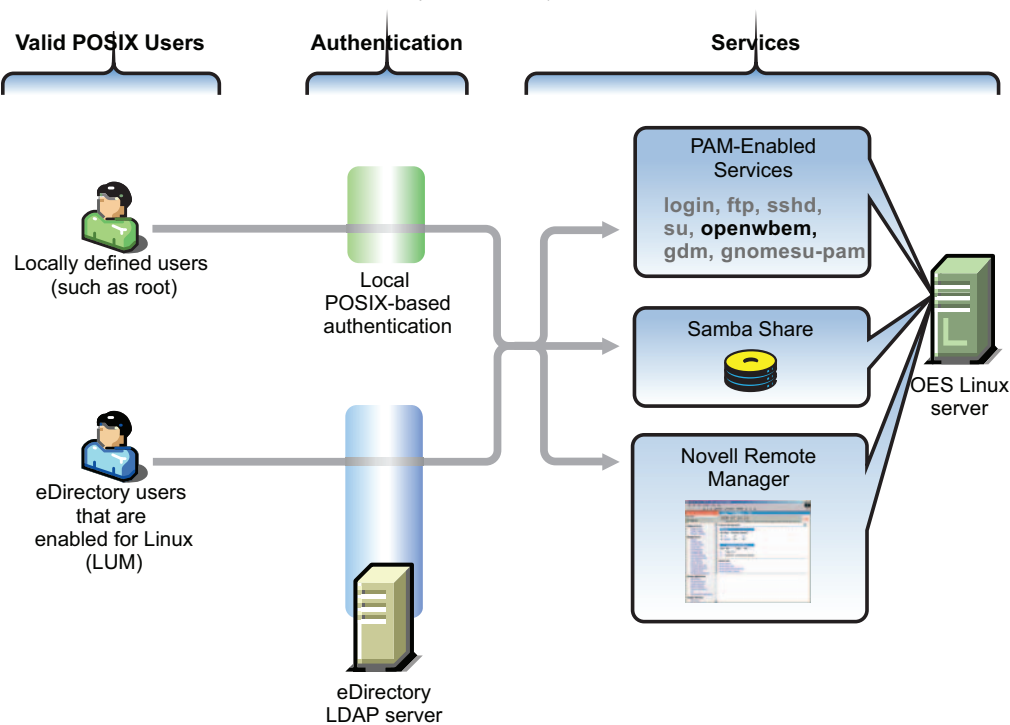
The topics in this section are designed to help you understand when LUM-enabled access is required so that your network services are accessible and work as expected. For more information about Linux User Management, see “Overview” in the *OES 2 SP1: Novell Linux User Management Technology Guide*.

- “A Graphical Preview of Linux User Management” on page 158
- “Linux Requires POSIX Users” on page 159
- “Linux Users Can Be Local or Remote” on page 159
- “The root User Is Never LUM-Enabled” on page 159
- “About Service Access on OES 2 Linux” on page 160
- “Services in OES 2 Linux That Require LUM-Enabled Access” on page 160
- “Services That Do Not Require LUM-Enabled Access But Have Some LUM Requirements” on page 162
- “Services That Do Not Require LUM-enabled Access” on page 162
- “LUM-Enabling Does Not Provide Global Access to ALL OES 2 Linux Servers” on page 163

A Graphical Preview of Linux User Management

Figure 15-1 illustrates how Linux User Management controls access to the OES 2 server.

Figure 15-1 LUM Provides POSIX Access for eDirectory Users



The following table explains the information presented in Figure 15-1.

Table 15-1 *Linux User Management*

Valid POSIX Users	Authentication	eDirectory Authenticated Services
Some services on OES 2 Linux servers must be accessed by POSIX users.	When the system receives an action request, it can authenticate both local POSIX users and users who have been enabled for Linux access.	Users can potentially access PAM-enabled services, Samba shares, and Novell Remote Manager as either local or eDirectory users.
eDirectory users can function as POSIX users if they are enabled for Linux access (LUM).		By default, only the <code>openwbem</code> command (required for server management) is enabled for eDirectory access.

Linux Requires POSIX Users

Linux requires that all users be defined by standard POSIX attributes, such as username, user ID (UID), primary group ID (GID), password, and other similar attributes.

Linux Users Can Be Local or Remote

Users that access a Linux server can be created in two ways:

- ♦ **Locally (on the server):** Local users are managed at a command prompt (using commands such as `useradd`) or in YaST. (See the `useradd(8)` man page and the YaST online help for more information.) These local users are stored in the `/etc/passwd` file. (See the `passwd(5)` man page for more information.)

IMPORTANT: As a general rule on OES 2 Linux servers, the only local user account that should exist is `root`. All other user accounts should be created in eDirectory and then be enabled for Linux access (LUM). You should never create duplicate local and eDirectory user accounts.

For more information, see [Section 6.1, “Avoiding POSIX and eDirectory Duplications,” on page 63](#).

-
- ♦ **Remotely (off the server):** Remote users can be managed by other systems, such as LDAP-compliant directory services. Remote user access is enabled through the Pluggable Authentication Module (PAM) architecture on Linux.

The Linux POSIX-compliant interfaces can authenticate both kinds of users, independent of where they are stored and how they are managed.

The root User Is Never LUM-Enabled

The OES 2 user management tools prevent you from creating an eDirectory user named `root`, thus replacing the `root` user on an OES 2 Linux server. If `root` were to be a LUM user and eDirectory became unavailable for some reason, there would be no root access to the system.

Even if eDirectory is not available, you can still log into the server through Novell Remote Manager and perform other system management tasks as the `root` user.

About Service Access on OES 2 Linux

Novell Linux User Management (LUM) lets you use eDirectory to centrally manage remote users for access to one or more OES 2 Linux servers.

In other words, LUM lets eDirectory users function as local (POSIX) users on an OES 2 Linux server. Access is enabled by leveraging the Linux Pluggable Authentication Module (PAM) architecture. PAM makes it possible for eDirectory users to authenticate with the OES 2 Linux server through LDAP.

In OES, the terms *LUM-enabling* and *Linux-enabling* are both used to describe the process that adds standard Linux (POSIX) attributes and values to eDirectory users and groups, thus enabling them to function as POSIX users and groups on the server.

You can use iManager to enable eDirectory users for Linux. For instructions, see [“About Enabling eDirectory Users for Linux Access” on page 164](#).

Services in OES 2 Linux That Require LUM-Enabled Access

Some services on an OES 2 Linux server require that eDirectory users be LUM-enabled:

- ♦ **Novell Samba (CIFS) Shares on the Server:** Windows workgroup users who need access to Samba shares defined on the server must be LUM-enabled eDirectory users who are configured to access the server. This is because Samba requires POSIX identification for access.

By extension, NetStorage users who need access to Samba (CIFS) Storage Location objects that point to the server must also be LUM-enabled eDirectory users with access to the server.

NOTE: Although Samba users must be enabled for LUM, Samba is not a PAM-enabled service. Logging in to the OES 2 Linux server through Samba does not create a home directory.

- ♦ **Core Linux Utilities Enabled for LUM:** These are the core utilities and other shell commands that you can specify during the OES install to be enabled for authentication through eDirectory LDAP. In Linux, these are known as PAM-enabled utilities.

IMPORTANT: Before you accept the default PAM-enabled service settings, be sure you understand the security implications explained in [Section 21.2.2, “User Restrictions: Some OES 2 Linux Limitations,” on page 234](#).

The core utilities available for LUM-enablement are summarized in [Table 15-2](#).

Table 15-2 PAM-enabled Services Controlled by LUM

Command	Where Executed	Task
ftp	Another host	Transfer files to and from the OES 2 server which, in this case, is a remote host.
login	<ul style="list-style-type: none"> ♦ OES 2 server ♦ SSH session with OES 2 server 	Log in to the OES 2 server, either directly or in an SSH session with the server.
openwbem	Local host	Required for iPrint, NSS, SMS, Novell Remote Manager, and iManager.

Command	Where Executed	Task
gdm	<ul style="list-style-type: none"> ♦ Local host ♦ Remote host 	Run and manage the X servers using XDMCP.
gnomesu-pam	Local host	Required for GNOME applications that need superuser access.
sshd	Another host	Establish a secure encrypted connection with the OES 2 server which, in this case, is a remote host.
su	<ul style="list-style-type: none"> ♦ OES 2 server ♦ SSH session with OES 2 server 	<p>Temporarily become another user.</p> <p>This is most often used to temporarily become the <code>root</code> user, who is not a LUM user and is, therefore, not affected by LUM.</p>

NOTE: Logging in to the OES 2 Linux server through a PAM-enabled service for the first time causes the creation of a home directory on the server.

- ♦ **Novell Remote Manager on Linux:** You can access Novell Remote Manager as the following:
 - ♦ The `root` user with rights to see everything on the Linux server.
 - ♦ A local Linux user with access governed by POSIX access rights. (Having local users in addition to `root` is not recommended on OES 2 servers.)
 - ♦ A LUM-enabled eDirectory user, such as the Admin user created during the install.
- ♦ **Novell Storage Management Services (SMS) on Linux:** You can access SMS utilities as
 - ♦ The `root` user with rights to see everything on the Linux server.
 - ♦ A local Linux user with access governed by POSIX access rights. (Having local users in addition to `root` is not recommended on OES 2 servers.)
 - ♦ A LUM-enabled eDirectory user, such as the Admin user created during the install.

Services That Do Not Require LUM-Enabled Access But Have Some LUM Requirements

Some services do not require eDirectory users to be LUM-enabled for service access:

- ♦ **NetStorage:** NetStorage users don't generally need to be LUM-enabled. However, salvaging and purging files through NetStorage on an NSS volume can only be done by users who are enabled for Linux.

IMPORTANT: Files that are uploaded by non-LUM users via NetStorage are owned, from a POSIX perspective, by the `root` user. The assumption is that such users are accessing their data on NSS or NCP™ volumes by using an NCP storage location object. In both cases, the Novell Trustee Model applies and POSIX ownership is irrelevant.

If non-LUM NetStorage users are later enabled for Samba access (which includes LUM-enabling) and begin using Samba as a file service, their NetStorage uploaded files are not accessible through Samba until you change POSIX file ownership. Although the Novell implementation of Samba leverages eDirectory for authentication, Samba file and directory access is always controlled by POSIX. The Novell Trustee Model doesn't apply to Samba.

Both Novell trustee assignments and POSIX file ownership are tracked correctly after users are LUM-enabled.

Although NetStorage doesn't require LUM-enabled access, the service itself runs as a POSIX-compliant system User (initially a local user on the OES 2 Linux server) who functions on behalf of the end users that are accessing the service.

If NetStorage must access NSS volumes, this local system user must be moved to eDirectory and LUM-enabled because only eDirectory users can access NSS volumes. The OES 2 installation program configures this correctly by default.

For more information, see [Appendix I, "System User and Group Management in OES 2 SP1," on page 267](#).

- ♦ **NSS:** eDirectory users that access NSS volumes directly through NCP (the Novell Client™) are not required to be LUM-enabled.

The exception is that if the Salvage feature is used, information on who deleted a file is not tracked unless the user is LUM-enabled. If a non-enabled user deletes a file, Salvage reports that the file was deleted by the server.

Additionally, if any other file access protocol, such as Samba/CIFS, is used to access NSS through the virtual file system layer that makes NSS appear to be a POSIX-compliant file system, then the users must be LUM-enabled.

Services That Do Not Require LUM-enabled Access

The following end user services do not require LUM-enabled access:

- ♦ iFolder 3.7
- ♦ iPrint
- ♦ NCP Client to an NCP Volume
- ♦ NCP Client to an NSS Volume (except deleter tracking for Salvage operations as noted in ["Services That Do Not Require LUM-Enabled Access But Have Some LUM Requirements" on page 162](#))

- ♦ Novell AFP
- ♦ Novell CIFS
- ♦ QuickFinder™

LUM-Enabling Does Not Provide Global Access to ALL OES 2 Linux Servers

As you plan to LUM-enable users for access to the services that require it, keep in mind that each OES 2 Linux server being accessed must be associated with a LUM-enabled group that the accessing users belong to.

In other words, it is not sufficient to LUM-enable users for access to a single OES 2 Linux server if they need access to multiple servers. An association between the LUM-enabled groups that the users belong to and the eDirectory UNIX Workstation object associated with the server must be formed by using iManager for each server the users need access to. This can be accomplished for multiple servers by using the process described in [“Enabling Users to Access Multiple OES 2 Linux Servers” on page 164](#).

For more information on LUM, see the *OES 2 SP1: Novell Linux User Management Technology Guide*.

15.2.2 Planning

The following sections summarize LUM planning considerations.

- ♦ [“eDirectory Admin User Is Automatically Enabled for Linux Access” on page 163](#)
- ♦ [“Planning Which Users to Enable for Access” on page 163](#)
- ♦ [“Be Aware of System-Created Users and Groups” on page 163](#)

eDirectory Admin User Is Automatically Enabled for Linux Access

When you install Linux User Management on an OES 2 Linux server, the Admin User object that installs LUM is automatically enabled for eDirectory LDAP authentication to the server.

Planning Which Users to Enable for Access

You need to identify the eDirectory users (and groups) who need access to services on OES 2 Linux servers that require LUM-enabled users.

This can be easily determined by doing the following:

1. Review the information in [“Services in OES 2 Linux That Require LUM-Enabled Access” on page 160](#).
2. Identify the servers that will run the services mentioned.
3. On your planning sheets, note the users and groups that you need to enable and the servers you need to enable them to access.

Be Aware of System-Created Users and Groups

You should also be aware of the system-created users and groups that are LUM-enabled when NSS is installed. For more information, see [Appendix I, “System User and Group Management in OES 2 SP1,” on page 267](#).

15.2.3 Coexistence and Migration

For coexistence and migration information, see “[Understanding the Need for Linux Enabling Users](#)” in the *Novell Server Consolidation and Migration Toolkit Administration Guide*.

15.2.4 LUM Implementation Suggestions

The following sections summarize LUM implementation considerations.

- ♦ “[About Enabling eDirectory Users for Linux Access](#)” on page 164
- ♦ ““[UNIX Workstation](#)” and “[Linux Workstation](#)” Are the Same Thing” on page 164
- ♦ “[Enabling Users to Access Multiple OES 2 Linux Servers](#)” on page 164
- ♦ “[Enabling eDirectory Groups for Linux Access](#)” on page 165
- ♦ “[Enabling eDirectory Users for Linux Access](#)” on page 165

About Enabling eDirectory Users for Linux Access

You can enable eDirectory users for Linux User Management by using either iManager 2.7 or the `nambulkadd` command.

- ♦ **iManager:** You can enable existing eDirectory users for Linux access by using the Linux User Management tasks in iManager.

You can enable multiple users in the same operation as long as they can be assigned to the same primary LUM-enabled group. The enabling process lets you associate the group with one or more OES 2 Linux servers or Linux workstations. For more information, see “[Enabling Users to Access Multiple OES 2 Linux Servers](#)” on page 164.

Samba users are also enabled for Linux access as part of the Samba-enabling process.

- ♦ **nambulkadd:** If you have eDirectory users and groups that need to be enabled for Linux access, you can use the `nambulkadd` command to modify multiple objects simultaneously. For more information, see the *OES 2 SP1: Novell Linux User Management Technology Guide*.

“UNIX Workstation” and “Linux Workstation” Are the Same Thing

When you use iManager to manage OES 2 Linux access, you might notice some inconsistencies in naming.

When OES 2 Linux servers are created, a “UNIX Workstation - *server_name*” object is created in eDirectory, where *server_name* is the DNS name of the OES 2 Linux server. In some places the iManager help refers to these server objects as “Linux Workstation” objects.

Both “UNIX Workstation” and “Linux Workstation” refer to the same eDirectory objects.

Enabling Users to Access Multiple OES 2 Linux Servers

IMPORTANT: Users gain server access through their LUM-enabled group assignment rather than through a direct assignment to the UNIX Workstation objects themselves.

You can enable users for access to multiple OES 2 Linux servers by associating the LUM-enabled groups to which the users belong with the UNIX Workstation objects you want users to have access to.

Enabling eDirectory Groups for Linux Access

There are two methods for enabling eDirectory groups for Linux access:

- ♦ “Using iManager” on page 165
- ♦ “Using LUM Utilities at the Command Prompt” on page 165

Using iManager

The following steps assume that the eDirectory Group objects already exist and that any User objects you want to enable for Linux also exist and have been assigned to the groups.

- 1 Log in to iManager as the eDirectory Admin user or equivalent.
- 2 Click *Linux User Management > Enable Groups for Linux*.
- 3 Browse to and select one or more Group objects, then click *OK*.
- 4 If you want all users assigned to the group to be enabled for Linux, make sure the *Linux-Enable All Users in These Groups* option is selected.
- 5 Click *Next* twice.
- 6 Browse to and select one or more UNIX Workstation (OES 2 Linux server) objects, then click *OK*.
- 7 Click *Next*, click *Finish*, then click *OK*.

Using LUM Utilities at the Command Prompt

Novell Linux User Management includes utilities for creating new LUM-enabled groups, and for enabling existing eDirectory groups for Linux access.

- ♦ The `nambulkadd` utility lets you use a text editor to create a list of groups you want enabled for Linux access. For more information, see “`nambulkadd`” in the *OES 2 SP1: Novell Linux User Management Technology Guide*.

IMPORTANT: Be sure to include a blank line at the end of each text file. Otherwise, the last line of the file won’t be processed properly.

- ♦ The `namgroupadd` utility lets you create a new LUM-enabled group or enable an existing eDirectory group for Linux access. For more information, see “`namgroupadd`” in the *OES 2 SP1: Novell Linux User Management Technology Guide*.

Enabling eDirectory Users for Linux Access

There are two methods for enabling eDirectory users for Linux access:

- ♦ “Using iManager” on page 166
- ♦ “Using LUM Utilities at the Command Prompt” on page 166

Using iManager

The following steps assume that the eDirectory User objects already exist.

- 1 Log in to iManager as the eDirectory Admin user or equivalent.
- 2 Click *Linux User Management > Enable Users for Linux*.
- 3 Browse to and select one or more User objects, then click *OK*.
- 4 Click *Next*.
- 5 As indicated, you can do the following:
 - ♦ Select and enable an existing eDirectory group for Linux.
 - ♦ Select an eDirectory group that is already enabled for Linux.
 - ♦ Specify the name and context of a new eDirectory group to create and enable for Linux.

Select the option that matches your requirements.
- 6 Click *Next*.
- 7 Browse to and select one or more UNIX Workstation (OES 2 Linux server) objects, then click *OK*.
- 8 Click *Next*, click *Finish*, then click *OK*.

Using LUM Utilities at the Command Prompt

Novell Linux User Management includes utilities for creating new LUM-enabled users, and for enabling existing eDirectory users for Linux access.

- ♦ The `nambulkadd` utility lets you use a text editor to create a list of users you want enabled for Linux access. For more information, see “`nambulkadd`” in the [OES 2 SP1: Novell Linux User Management Technology Guide](#).

IMPORTANT: Be sure to include a blank line at the end of each text file. Otherwise, the last line of the file won’t be processed properly.

- ♦ The `namuseradd` utility lets you create a single LUM-enabled user or enable an existing eDirectory user for Linux access. For more information, see “`namuseradd`” in the [OES 2 SP1: Novell Linux User Management Technology Guide](#).

15.3 Identity Management Services

Providing network users with a network identity is a fundamental expectation for networking, but it can also become confusing when users need to track multiple identities to use network services. When you add the traditional POSIX users found on Linux systems to the mix, the picture becomes even more complex.

The identity management services provided by Novell Open Enterprise Server (OES) leverage Novell eDirectory to simplify and customize identity management to fit your needs:

- ♦ If you currently store and manage all your users and groups in eDirectory, you can continue to do so.

- ♦ If you use Novell Client software to provide network file and print services, you can now provide seamless file and print access to OES 2 Linux servers by using the NCP server for Linux and iPrint services. For more information, see [Section 17.6, “NCP Implementation and Maintenance,” on page 214](#) and [Chapter 18, “Print Services,” on page 221](#).
- ♦ If you want eDirectory users to have access to OES 2 Linux services that require POSIX authentication, you can enable the users for Linux access. For more information, see [Section 15.2, “Linux User Management: Access to Linux for eDirectory Users,” on page 157](#).
- ♦ If you need to store and manage users in multiple directories, you can greatly strengthen your organization’s security and dramatically decrease your identity management costs by deploying Novell Identity Manager. For more information, see [Section 15.4, “Using the Identity Manager 3.5 Bundle Edition,” on page 167](#).

15.4 Using the Identity Manager 3.5 Bundle Edition

Novell Identity Manager is a data-sharing solution that leverages the Identity Vault to synchronize, transform, and distribute information across applications, databases, and directories.

The Identity Manager Bundle Edition provides licensed synchronization of information (including passwords) held in NT Domains, Active Directory Domains, and eDirectory systems. When data from one system changes, Identity Manager detects and propagates these changes to other connected systems based on the business policies you define.

In this document:

- ♦ [Section 15.4.1, “What Am I Entitled to Use?,” on page 167](#)
- ♦ [Section 15.4.2, “System Requirements,” on page 168](#)
- ♦ [Section 15.4.3, “Installation Considerations,” on page 168](#)
- ♦ [Section 15.4.4, “Getting Started,” on page 168](#)
- ♦ [Section 15.4.5, “Activating the Bundle Edition,” on page 168](#)
- ♦ [Section 15.4.6, “Frequently Asked Questions about Activation,” on page 169](#)

15.4.1 What Am I Entitled to Use?

The Bundle Edition allows you to use the Identity Manager engine and the following Identity Manager drivers:

- ♦ Identity Manager Driver for eDirectory
- ♦ Identity Manager Driver for Active Directory
- ♦ Identity Manager Driver for NT

Other Identity Manager Integration Modules (drivers) are included in the software distribution. You can install and use these additional Integration Modules for 90 days, at which time you must purchase Novell Identity Manager and the Integration Modules you want to use.

The User Application and the service drivers (Loopback, Manual Task, and Entitlements) are not included as part of the license agreement for the Bundle Edition. In order to use these Identity Manager components, you must purchase Identity Manager.

15.4.2 System Requirements

For the latest Identity Manager system requirements, see the *Identity Manager Installation Guide* (<http://www.novell.com/documentation/idm35/install/data/front.html>).

The Bundle Edition does not include Solaris or AIX support. If you want to run the Metadirectory engine or Integration Modules on these platforms, you must purchase Identity Manager.

15.4.3 Installation Considerations

Novell Identity Manager Bundle Edition contains components that can be installed within your environment on multiple systems and platforms. Depending on your system configuration, you might need to run the installation program several times to install Identity Manager components on the appropriate systems.

In order for the product to be activated, you must install Open Enterprise Server before installing the Identity Manager Bundle Edition. For more information on activation issues, see “**Activating the Bundle Edition**” on page 168.

15.4.4 Getting Started

The following sections from the *Novell Identity Manager Administration Guide* will help you plan, install, and configure your Identity Manager Bundle Edition:

- ♦ “Overview” (<http://www.novell.com/documentation/idm35/install/data/alxkrnf.html>)
- ♦ “Planning Your Implementation” (<http://www.novell.com/documentation/idm35/install/data/anhomxn.html>)
- ♦ “Installing Identity Manager” (<http://www.novell.com/documentation/idm35/install/data/a7c9ie0.html>)
- ♦ “Installing Active Directory, NT, and eDirectory Drivers” (<http://www.novell.com/documentation/idm35drivers/index.html>)
- ♦ “Setting Up a Connected System” (<http://www.novell.com/documentation/idm35/admin/data/bs35odr.html>)
- ♦ “Password Synchronization across Connected Systems” (<http://www.novell.com/documentation/idm35/admin/data/an4bz0u.html>)
- ♦ “Logging and Reporting” (http://www.novell.com/documentation/idm35/idm_log/data/bookinfo.html)

For information about customizing your implementation:

- ♦ *Policy Builder and Driver Customization Guide* (<http://www.novell.com/documentation/idm35/policy/data/bookinfo.html>)

15.4.5 Activating the Bundle Edition

If you choose to purchase additional Identity Manager Integration Modules, you need to install the activation credential for those Integration Modules and also the credential for Novell Identity Manager. See *Activating Identity Manager Products Using a Credential* (<http://www.novell.com/documentation/idm35/install/data/brph5hb.html>) for more information on activating other Identity Manager products.

In order to use the Bundle Edition, you must obtain and install an activation credential. Use the following instructions to complete the Bundle Edition activation tasks.

- 1 Browse to the [Identity Manager Bundle Edition Registration \(http://download.novell.com/delivery/reg/idm_bundled.jsp\)](http://download.novell.com/delivery/reg/idm_bundled.jsp) Web site.
- 2 Enter your OES activation code, then click *Submit*.
- 3 Do one of the following:
 - ♦ Save the Product Activation Credential file.
 - or
 - ♦ Open the Product Activation Credential file, then copy the contents of the Product Activation Credential to your clipboard. Carefully copy the contents, and make sure that no extra lines or spaces are included. You should begin copying from the first dash (-) of the credential (----BEGIN PRODUCT ACTIVATION CREDENTIAL) through the last dash (-) of the credential (END PRODUCT ACTIVATION CREDENTIAL-----).
- 4 Open iManager.
- 5 Choose *Identity Manager > Identity Manager Overview*.
- 6 Select the driver set or browse to a driver set, then click *Next*.
- 7 On the Identity Manager Overview page, locate the driver set, click the red *Activation required* by link, then click *Install Activation*.
- 8 Select the driver set where you want to activate an Identity Manager component.
- 9 Do one of the following:
 - ♦ Specify where you saved the Identity Manager Activation Credential, then click *Next*.
 - or
 - ♦ Paste the contents of the Identity Manager Activation Credential into the text area, then click *Next*.
- 10 Click *Finish*.

15.4.6 Frequently Asked Questions about Activation

- ♦ “Do I need to Install Identity Manager on a specific server?” on page 170
- ♦ “I installed the Bundle Edition on Linux or NetWare, but it’s not activated. Why is this?” on page 170
- ♦ “Can I run Identity Manager on a Windows Server?” on page 170
- ♦ “Can I run Identity Manager on a Solaris or AIX Server?” on page 170
- ♦ “My drivers stopped working. What happened?” on page 170
- ♦ “I purchased an additional Integration Module. Why doesn't it work?” on page 170
- ♦ “If I purchase a license for Novell Identity Manager and a license for an additional Integration Module, do I need to re-install the software?” on page 170
- ♦ “How do I know what’s activated?” on page 171

Do I need to Install Identity Manager on a specific server?

Yes. As a Bundle Edition user, you must install Identity Manager on the server where you installed Open Enterprise Server. In order for activation to work properly, you must install Identity Manager on Linux or NetWare, and create a driver set on that server.

I installed the Bundle Edition on Linux or NetWare, but it's not activated. Why is this?

You must install the Bundle Edition on the server where OES exists. If you install it on a non-OES server, the Bundle Edition cannot activate.

Can I run Identity Manager on a Windows Server?

Not with the Bundle Edition. However, you can still synchronize data held on a Windows server by using the Identity Manager Remote Loader service. The Remote Loader enables synchronization between the Metadirectory Engine (on your Linux or NetWare server) and a remote driver (on the Windows server.) See [Setting Up a Connected System \(http://www.novell.com/documentation/idm35/admin/data/bs35odr.html\)](http://www.novell.com/documentation/idm35/admin/data/bs35odr.html) for more information.

In order to run Identity Manager on a Windows server, you need to purchase Novell Identity Manager.

Can I run Identity Manager on a Solaris or AIX Server?

Not with the Bundle Edition. However, you can still synchronize data held on these platforms by using the Identity Manager Remote Loader service. The Remote Loader enables synchronization between the Metadirectory Engine and a remote driver (on the Solaris or AIX server.) See [Setting Up a Connected System \(http://www.novell.com/documentation/idm35/admin/data/bs35odr.html\)](http://www.novell.com/documentation/idm35/admin/data/bs35odr.html) for more information.

In order to run Identity Manager on Solaris or AIX, you need to purchase Novell Identity Manager.

My drivers stopped working. What happened?

You might have installed the Bundle Edition on a non-OES server. The Bundle Edition must be installed on your Linux or NetWare server where OES exists. If Identity Manager is installed on a non-OES platform, activation cannot work. After 90 days, your drivers will stop running if you haven't purchased Novell Identity Manager.

I purchased an additional Integration Module. Why doesn't it work?

With your OES purchase, you are entitled to use the Bundle Edition products. If you want to add new Integration Modules, you also need to purchase Novell Identity Manager. The Integration Module cannot activate until you purchase Novell Identity Manager.

If I purchase a license for Novell Identity Manager and a license for an additional Integration Module, do I need to re-install the software?

No, you just need to install the activation credentials associated with your purchase.

How do I know what's activated?

For information about how to view currently activated products, see [“Viewing Product Activations”](http://www.novell.com/documentation/idm35/install/data/agfhtax.html) (<http://www.novell.com/documentation/idm35/install/data/agfhtax.html>).

Access Control and Authentication

Access Control and Authentication are the keys to:

- ♦ Providing services for users.
- ♦ Ensuring that the network is secure.

This section discusses the following:

- ♦ [Section 16.1, “Controlling Access to Services,” on page 173](#)
- ♦ [Section 16.2, “Authentication Services,” on page 186](#)

16.1 Controlling Access to Services

OES 2 supports a number of options for service access, including

- ♦ Web browsers.
- ♦ File managers and applications on Linux, Macintosh, and Windows workstations.
- ♦ Novell Client™ software.
- ♦ Personal digital assistants (PDAs) and other electronic devices that are enabled for Web access.

You control which of these options can be used through the services you offer and the ways your configure those services.

This section can help you understand access control at a high level so that you can plan, implement, and control access to services. More detail about the items discussed is contained in individual service guides.

The topics that follow are:

- ♦ [Section 16.1.1, “Overview of Access Control,” on page 173](#)
- ♦ [Section 16.1.2, “Planning for Service Access,” on page 180](#)
- ♦ [Section 16.1.3, “Coexistence and Migration of Access Services,” on page 183](#)
- ♦ [Section 16.1.4, “Access Implementation Suggestions,” on page 184](#)
- ♦ [Section 16.1.5, “Configuring and Administering Access to Services,” on page 184](#)

16.1.1 Overview of Access Control

The following sections present overviews of methods for accessing Open Enterprise Server 2 services.

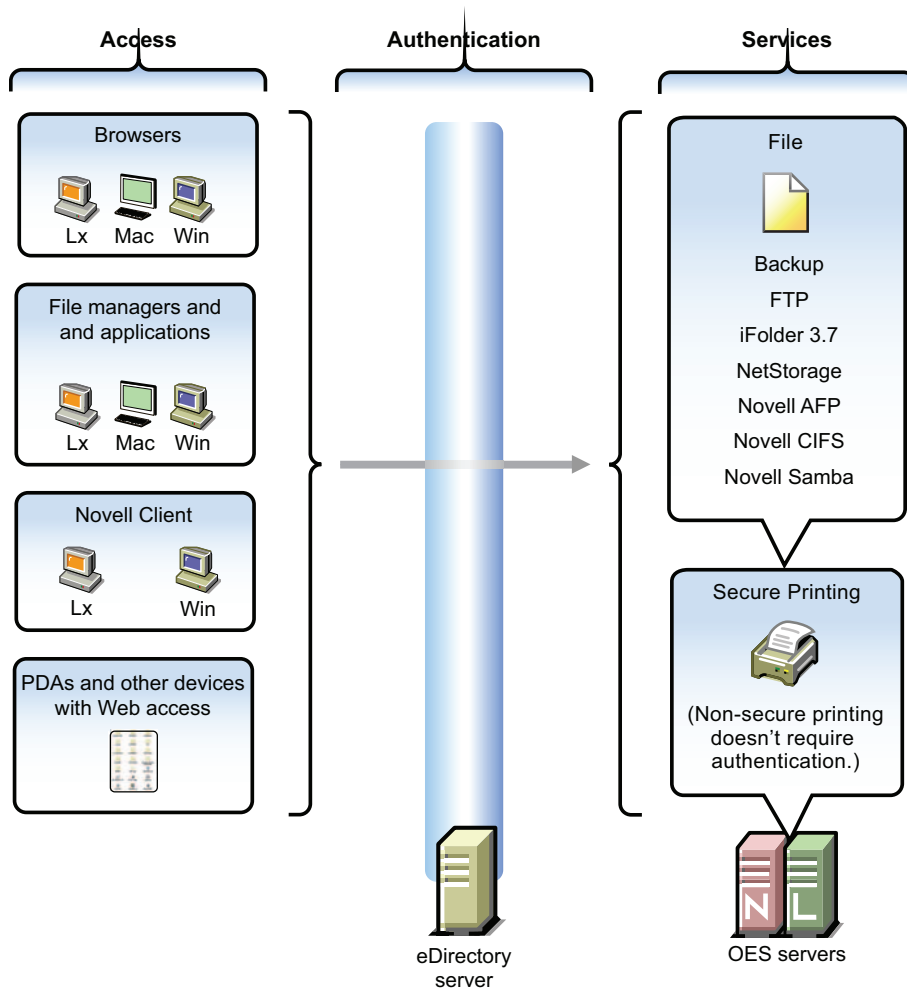
- ♦ [“Access to OES 2 Services” on page 174](#)
- ♦ [“Access Control Options in OES 2” on page 175](#)
- ♦ [“The Traditional Novell Access Control Model” on page 176](#)
- ♦ [“NSS Access Control on OES Linux” on page 178](#)

- ♦ “Novell Client (NCP File Services) Access” on page 179
- ♦ “eDirectory User Access to OES 2 Linux Servers” on page 180

Access to OES 2 Services

Figure 16-1 illustrates the access methods supported by OES 2 services. Novell® eDirectory™ provides authentication to each service.

Figure 16-1 Access Interfaces and the Services They Can Access



The interfaces available for each service are largely determined by the protocols supported by the service.

- ♦ Browsers and personal digital assistants require support for the HTTP protocol.
- ♦ Each workstation type has file access protocols associated with it. Linux uses NFS as its native protocol for file services access, Macintosh workstations communicate using AFP or CIFS, and Windows workstations use the CIFS protocol for file services.
- ♦ Novell Client software for both Windows and Linux uses the NetWare® Core Protocol™ (NCP™) to provide the file services for which Novell is well known.

Understanding the protocol support for OES 2 services can help you begin to plan your OES implementation. For more information, see “[Matching Protocols and Services to Check Access Requirements](#)” on page 182.

Access Control Options in OES 2

Because OES 2 offers both traditional Novell access control and POSIX access control, you have a variety of approaches available to you, including combining the two models to serve various aspects of your network services.

Table 16-1 provides links to documentation that discusses OES 2 access control features.

Table 16-1 *General File System Access Control*

Feature	To Understand	See
Access Control Lists (ACLs) on Linux	How ACLs are supported on the most commonly used Linux POSIX file systems and let you assign file and directory permissions to users and groups who do not own the files or directories.	“ Access Control Lists in Linux ” (http://www.novell.com/documentation/sles10/sles_admin/data/cha_acls.html) in the <i>SLES 10 SP2: Installation and Administration Guide</i> (http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html)
Aligning NCP and POSIX access rights	How to approximate the NCP (or NetWare) access control model on POSIX file systems.	“ Section 17.4, “Aligning NCP and POSIX File Access Rights,” on page 210 ”
Directory and file attributes	Directory and file attributes on OES 2 NetWare.	“ Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes ” in the <i>OES 2 SP1: File Systems Management Guide</i>
File system trustee rights	File system trustee rights on NetWare (NSS and traditional volumes), including how NetWare determines effective file system trustee rights.	“ File-System Trustee Rights ” in the <i>OES 2 SP1: File Systems Management Guide</i>
NetWare Connection Manager	How the NetWare Connection Manager tracks active user connections and provides access permission information for NSS and Traditional volumes on NetWare.	“ The Connection Manager for NetWare ” in the <i>OES 2 SP1: File Systems Management Guide</i>
Novell Client and the NetWare Connection Manager	How the Novell Client works with the Connection Manager to ensure that users have correct access rights to the file system.	“ Novell Client ” in the <i>OES 2 SP1: File Systems Management Guide</i>
NetWare trustee rights and directory and file attributes	How to control who can see which files and what they can do with them.	“ Understanding File System Access Control Using Trustees ” in the <i>OES 2 SP1: File Systems Management Guide</i>

Feature	To Understand	See
POSIX file system rights and attributes on Linux	How to configure file system attributes on OES 2 Linux servers.	"Access Control Lists in Linux" (http://www.novell.com/documentation/sles10/sles_admin/data/cha_acls.html) in the <i>SLES 10 SP2: Installation and Administration Guide</i> (http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html)
Rights to install applications on NetWare	The access rights required to install applications on NetWare file systems.	"Security Guidelines" in the <i>OES 2 SP1: File Systems Management Guide</i>
Security Equivalence in eDirectory	The concept of Security Equivalence in eDirectory.	"eDirectory Objects and Security Equivalence" in the <i>OES 2 SP1: File Systems Management Guide</i>

The Traditional Novell Access Control Model

NetWare is known for its rich access control. OES makes these controls available on Linux through NSS volume support. In addition, some of the controls are available on Linux POSIX file systems through NCP volume creation. NCP volumes are limited because Linux POSIX systems offer only a subset of the directory and file attributes that NSS offers.

In the NetWare access control model, eDirectory objects, such as users and groups, are assigned File System Trustee Rights to directories and files on NSS and NCP volumes. These trustee rights determine what the user or group can do with a directory or file, provided that the directory or file attributes allow the action.

This is illustrated in **Figure 16-2**.

Figure 16-2 Directory and File Access under the NetWare Access Control Model

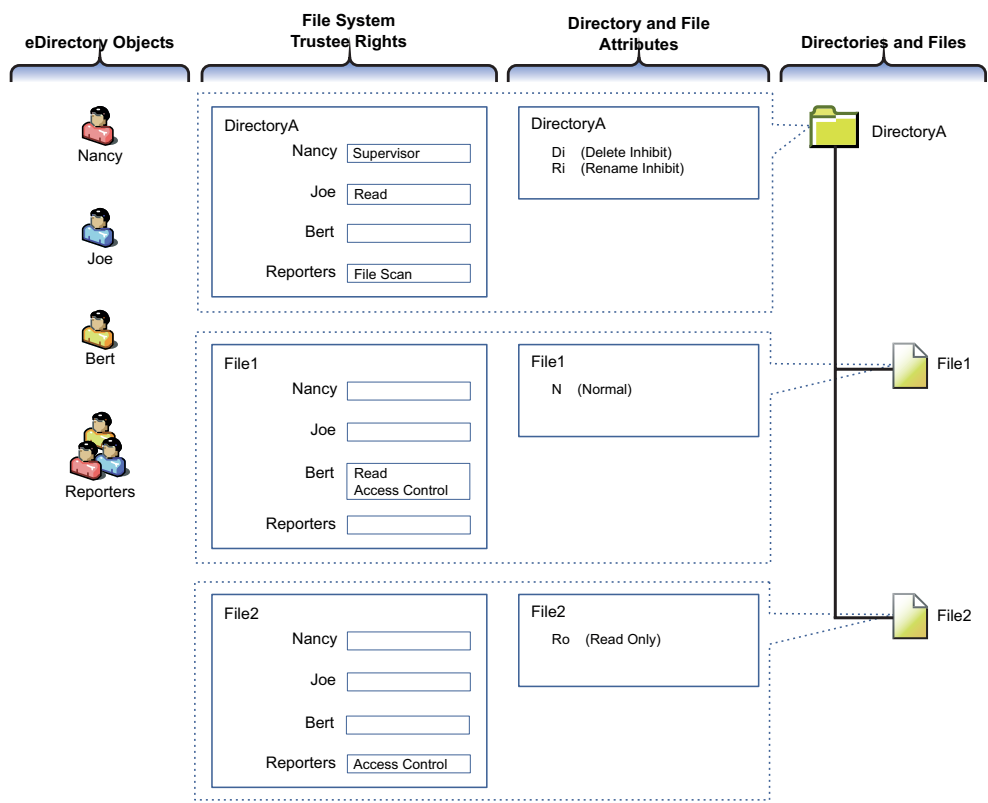


Table 16-2 explains the effective access rights illustrated in Figure 16-2.

Table 16-2 *Access Rights Explanation*

eDirectory Objects	File System Trustee Rights	Directory and File Attributes	Directories and Files
eDirectory objects (in most cases users and groups) gain access to the file system through eDirectory.	<p>File system trustee rights govern access and usage by the eDirectory object specified for the directory or file to which the rights are granted.</p> <p>Trustee rights are overridden by directory and file attributes.</p> <p>For example, even though Nancy has the Supervisor (all) trustee right at the directory (and, therefore, to the files it contains), she cannot delete File2 because it has the Read Only attribute set.</p> <p>Of course, Nancy could modify the file attributes so that File2 could then be deleted.</p>	<p>Each directory and file has attributes associated with it. These attributes apply universally to all trustees regardless of the trustee rights an object might have.</p> <p>For example, a file that has the Read Only attribute is Read Only for all users.</p> <p>Attributes can be set by any trustee that has the Modify trustee right to the directory or file.</p>	<p>The possible actions by the eDirectory users and group shown in this example are as follows:</p> <ul style="list-style-type: none"> ♦ Nancy has the Supervisor trustee right at the directory level, meaning that she can perform any action not blocked by a directory or file attribute. <p>The Di (Delete Inhibit) and Ri (Rename Inhibit) Attributes on Directory A prevent Nancy from deleting or renaming the directory unless she modifies the attributes first. The same principle applies to her ability to modify File2.</p> <ul style="list-style-type: none"> ♦ Because Joe is a member of the Reporters group, he can view file and directory names inside DirectoryA and also see the directory structure up to the root directory. <p>Joe also has rights to open and read any files in DirectoryA and to execute any applications in DirectoryA.</p> <ul style="list-style-type: none"> ♦ Because Bert is a member of the Reporters group, he can view file and directory names inside DirectoryA and also see the directory structure up to the root directory. <p>Bert also has rights to open and read File1 and to execute it if it's an application.</p> <p>And Bert has rights to grant any eDirectory user access to File1.</p> <ul style="list-style-type: none"> ♦ Because all three users are members of the Reporters group, they can grant any eDirectory user access to File2. <p>Of course, for Nancy this is redundant because she has the Supervisor right at the directory level.</p>

NSS Access Control on OES Linux

Table 16-3 provides links to documentation that discusses the various NSS-specific access control features.

Table 16-3 Summary of NSS Access Control Documentation Links

Feature	To Understand	See
Independent Mode vs. NetWare Mode This applies only to Linux servers.	The difference between Independent Mode access and NetWare Mode access.	“Access Control for NSS on Linux” in the <i>OES 2 SP1: File Systems Management Guide</i>
NetWare directory and file attributes on NSS volumes on OES 2 Linux This is only about what is displayed. POSIX permissions are not used for access control to NSS volumes.	How NSS file attributes are reflected in Linux directory and file permissions viewable through POSIX.	“Displaying Key NSS Directory and File Attributes as Linux POSIX Permissions” in the <i>OES 2 SP1: File Systems Management Guide</i>

Novell Client (NCP File Services) Access

If you have not already determined whether to use the Novell Client on your network, we recommend that you consider the following information:

- ♦ [“About the Novell Client” on page 179](#)
- ♦ [“Is the Novell Client Right for Your Network?” on page 179](#)
- ♦ [“Differences between Linux and Windows” on page 180](#)

About the Novell Client

The Novell Client extends the capabilities of Windows and Linux desktops with access to NetWare and OES 2 Linux servers.

After installing Novell Client software, users can enjoy the full range of Novell services, such as

- ♦ Authentication via Novell eDirectory
- ♦ Network browsing and service resolution
- ♦ Secure and reliable file system access
- ♦ Support for industry-standard protocols

The Novell Client supports the traditional Novell protocols (NDAP, NCP, and RSA) and interoperates with open protocols (LDAP, CIFS, and NFS).

Is the Novell Client Right for Your Network?

Although Novell offers services that don’t require Novell Client, (such as NetStorage, Novell iFolder[®] 3.7, and iPrint), many network administrators continue to prefer the Novell Client as the access choice for their network users for the following reasons:

- ♦ They prefer eDirectory authentication to LDAP authentication because they believe it is more secure.
- ♦ They prefer the NetWare Core Protocol (NCP) over the Microsoft CIFS protocol because they believe that CIFS is more vulnerable to the propagation of viruses on the network.

Conversely, other network administrators are equally adamant that their users function better without the added overhead of running an NCP client on each workstation.

We can't determine what is best for your network, but we do provide you with viable choices.

Differences between Linux and Windows

There are some differences between the Linux and Windows clients. These are documented in “[Understanding How the Novell Client for Linux Differs from the Novell Client for Windows 2000/XP](#)” in the *Novell Client 2.0 SP1 for Linux Administration Guide*.

eDirectory User Access to OES 2 Linux Servers

Some services that run on OES 2 Linux servers require that the users accessing them be (or, at least, appear to the Linux system to be) standard Linux users with Linux user credentials, such as a user ID (UID) and primary group ID (GID).

So that eDirectory users can access these services, Novell provides the Linux User Management (LUM) technology. The impact of this on you as the network administrator is that these users and groups must be enabled for eDirectory LDAP authentication to the local server. For more information, see “[Linux User Management: Access to Linux for eDirectory Users](#)” on page 157.

16.1.2 Planning for Service Access

After you understand the access options available to your network users, you can decide which will work best on your network.

Planning tips for network services are contained in the following sections:

- ♦ “[Planning File Service Access](#)” on page 180
- ♦ “[Planning Print Service Access](#)” on page 181
- ♦ “[Matching Protocols and Services to Check Access Requirements](#)” on page 182

Planning File Service Access

As you plan which file services to provide, be aware of the file service/volume and feature support limitations outlined in the following sections.

- ♦ “[Service Access to Volume Type Limitations](#)” on page 180
- ♦ “[Feature Support](#)” on page 181

Service Access to Volume Type Limitations

Supported combinations are outlined in [Table 16-4](#).

Table 16-4 *Service Access to Volume Types*

File Service	Linux POSIX Volumes	NSS Volumes on Linux	NetWare Traditional Volumes	NSS Volumes on NetWare
AFP	No	Yes-Novell AFP	No	Yes-NFAP

File Service	Linux POSIX Volumes	NSS Volumes on Linux	NetWare Traditional Volumes	NSS Volumes on NetWare
CIFS	Yes-Novell CIFS Novell Samba	Yes-Novell CIFS Novell Samba	No	Yes-NFAP
NetStorage	Yes	Yes	Yes	Yes
NetWare Core Protocol (NCP)	Yes	Yes	Yes	Yes
NFS	Yes	Yes-NFSv3	No	Yes-NFAP
Novell iFolder 2.1x	No	No	No	Yes
Novell iFolder 3.7	Yes	Yes	No	No

Details about the file systems supported by each file service are explained in the documentation for each service.

Be aware that file services support different sets of access protocols. A summary of the protocols available for access to the various OES file services is presented in [“Matching Protocols and Services to Check Access Requirements” on page 182](#).

Feature Support

Table 16-5 *Features Supported on Each Volume Type*

Feature	Linux POSIX Volumes	NSS Volumes on Linux	NetWare Traditional Volumes	NSS Volumes on NetWare
Directory quotas	No	Yes	Yes	Yes
Login scripts	Yes (if also defined as an NCP volume)	Yes	Yes	Yes
Mapped drives	Yes (if also defined as an NCP volume)	Yes	Yes	Yes
Novell directory and file attributes	No	Yes	Yes	Yes
Purge/Salvage	No	Yes	Yes	Yes
Trustee rights	Yes (if also defined as an NCP volume)	Yes	Yes	Yes
User space quotas	No	Yes	Yes	Yes

Planning Print Service Access

Novell iPrint has access control features that let you specify the access that each eDirectory User, Group, or container object has to your printing resources.

You can also use iPrint to set up print services that don't require authentication.

NOTE: Access control for printers is supported only on the Windows iPrint Client.

For more information on access control and iPrint, see the following:

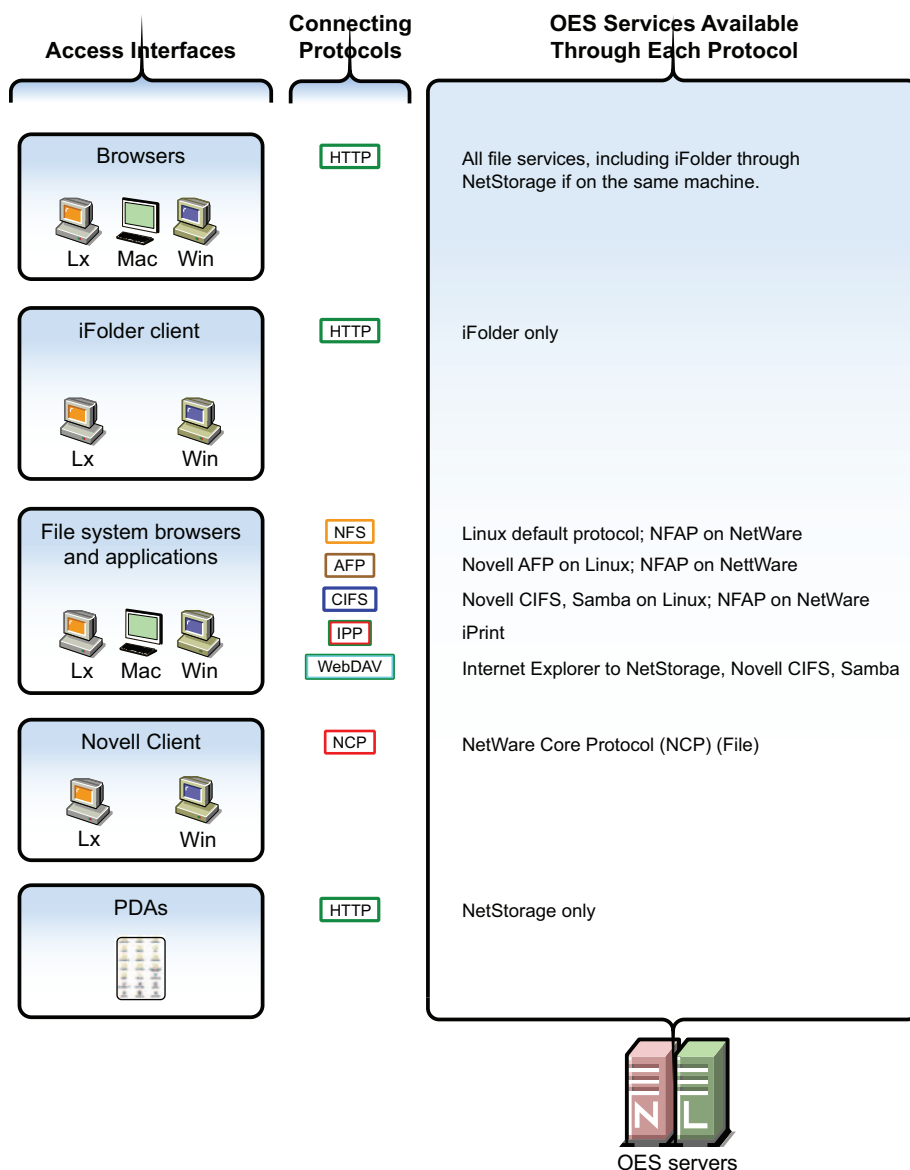
- ♦ “Setting Access Control for Your Print System” in the *OES 2 SP1: iPrint for Linux Administration Guide*
- ♦ “Setting Access Control for Your Print System” in the *OES 2 SP1: iPrint Administration Guide for NetWare*

Matching Protocols and Services to Check Access Requirements

Figure 16-3 illustrates the access interfaces available to users in OES and the services that each interface can connect to. It also shows the protocols that connect access interfaces with network services.

To use this for planning:

1. Review the different access interfaces in the left column.
2. In the middle column, review the protocols each interface supports.
3. In the right column, view the services available to the interfaces via the protocols.

Figure 16-3 Access Interfaces and Services, and the Protocols That Connect Them

16.1.3 Coexistence and Migration of Access Services

Because NetWare Core Protocol (NCP) is now available on Linux, your Novell Client users can attach to OES 2 Linux servers as easily as they have been able to attach to NetWare servers. In fact, they probably won't notice any changes.

NCP Server for Linux enables support for login scripts, mapping drives to OES 2 Linux servers, and other services commonly associated with Novell Client access. This means that Windows users with the Novell Client installed can now be seamlessly transitioned to file services on OES 2 Linux. And with the Novell Client for Linux, Windows users can be moved to SUSE[®] Linux Enterprise Desktop with no disruption in NCP file services.

For more information, see the *OES 2 SP1: NCP Server for Linux Administration Guide*.

16.1.4 Access Implementation Suggestions

After you plan and install OES 2 services, be sure to provide clear access instructions to your network users. For a summary of access methods, see [Appendix E, “Quick Reference to OES 2 User Services,”](#) on page 257.

16.1.5 Configuring and Administering Access to Services

The following sections discuss administering access to services.

- ♦ “Password Management” on page 184
- ♦ “Linux (POSIX) File System Access Rights” on page 184
- ♦ “NSS (and NetWare) File and Directory Trustee Management” on page 185

Password Management

Many network administrators let users administer their own passwords. For more information on password self management, see “[Password Self-Service](#)” in the *Novell Password Management 3.2 Administration Guide*.

Linux (POSIX) File System Access Rights

Access control to Linux POSIX file systems is controlled through POSIX file system access rights or attributes associated with directories and files. In general, the directories and files can be accessed by three POSIX entities:

- ♦ The user who owns the directory or file
- ♦ The group who owns the directory or file
- ♦ All other users defined on the system

These users and the affected group are each assigned (or not assigned) a combination of three attributes for each directory and file:

Table 16-6 *Linux Access Rights*

Attribute	Effect on Directory when Assigned	Effect on File when Assigned
Read	Lets the user or group view the directory's contents.	Lets the user or group open and read the file.
Write	Lets the user or group create or delete files and subdirectories in the directory.	Lets the user or group modify the file.
Execute	Lets the user or group access the directory by using the <code>cd</code> command.	Lets the user or group run the file as a program.

For more information, see “[Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes](#)” in the *OES 2 SP1: File Systems Management Guide*.

NSS (and NetWare) File and Directory Trustee Management

The *OES 2 SP1: File Systems Management Guide* contains a thorough discussion of file and directory trustee management in its “[Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes](#)” section.

The following sections present brief information about managing trustees on NSS volumes.

- ♦ “[Using NetStorage to Change File and Directory Attributes and Trustees](#)” on page 185
- ♦ “[Using the Novell Client to Change File and Directory Attributes and Trustee Rights](#)” on page 185
- ♦ “[Using iManager 2.7 to Change File and Directory Attributes and Trustee Rights](#)” on page 185
- ♦ “[Using the Linux Command Prompt to Change File Attributes](#)” on page 185
- ♦ “[Using the Linux Command Prompt to Change Trustee Rights](#)” on page 185

Using NetStorage to Change File and Directory Attributes and Trustees

You can use the NetStorage Web browser interface to change attributes and trustees for directories and files on NSS volumes, but you can’t change them by using a WebDAV connection to NetStorage.

You cannot change attributes or trustees on NetWare Traditional volumes by using NetStorage.

Using the Novell Client to Change File and Directory Attributes and Trustee Rights

You can use the Novell Client to change NSS file and directory attributes and to grant trustee rights to an NSS volume on an OES 2 Linux server. For more information, see “[NetWare File Security](#)” in the *Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide* and “[Managing File Security](#)” in the *Novell Client 2.0 SP1 for Linux Administration Guide*.

Using iManager 2.7 to Change File and Directory Attributes and Trustee Rights

You can use the iManager 2.7 Files and Folders plug-in to manage directories and files on NCP and NSS volumes. For more information, see the plug-in help.

Using the Linux Command Prompt to Change File Attributes

Use the `attrib` command to change file and directory attributes on an NSS volume.

The `attrib` command is also documented in “[Attributes Utility for Linux](#)” in the *OES 2 SP1: File Systems Management Guide*.

You can also enter the following command at the command prompt:

```
attrib --help
```

Using the Linux Command Prompt to Change Trustee Rights

To grant NSS trustee rights to an NSS volume, enter the following command:

```
rights -f /full/directory/path -r rights_mask trustee full.object.context
```

where `/full/directory/path` is the path to the target directory on the NSS volume, `rights_mask` is the list of NSS rights, and `full.object.context` is the object (User or Group) in its full eDirectory context including the tree name.

For example, you might enter the following:

```
rights -f /data/groupstuff -r rwfc trustee mygroup.testing.example_tree
```

For a complete list of command options, enter `rights` at the command prompt.

The `rights` command is also documented in “[Trustee Rights Utility for Linux](#)” in the *OES 2 SP1: File Systems Management Guide*.

16.2 Authentication Services

This section briefly discusses the following topics:

- ♦ [Section 16.2.1, “Overview of Authentication Services,” on page 186](#)
- ♦ [Section 16.2.2, “Planning for Authentication,” on page 189](#)
- ♦ [Section 16.2.3, “Authentication Coexistence and Migration,” on page 189](#)
- ♦ [Section 16.2.4, “Configuring and Administering Authentication,” on page 189](#)

16.2.1 Overview of Authentication Services

This section provides specific overview information for the following key OES components:

- ♦ [“NetIdentity Agent” on page 186](#)
- ♦ [“Novell Modular Authentication Services \(NMAS\)” on page 187](#)
- ♦ [“Password Support in OES 2” on page 187](#)

For more authentication topics, see “[Access, Authenticate, Log in](#)” in the OES online documentation.

NetIdentity Agent

In OES 2, the NetIdentity Agent works with Novell eDirectory authentication to provide background authentication to Windows Web-based applications that require eDirectory authentication through a secure identity “wallet” on the workstation. Applications access the eDirectory credentials without prompting users for a username and password.

The NetIdentity Agent supports applications running on OES 2 server platforms as follows:

- ♦ **OES 2 Linux:** NetStorage
- ♦ **OES 2 NetWare:** NetStorage and iPrint (if authentication is required)

NetIdentity Agent browser authentication is supported only by Windows Internet Explorer.

The Novell Client provides authentication credentials to NetIdentity, but it does not obtain authentication credentials from NetIdentity because it is not a Web-based application.

NetIdentity Agent requires

- ♦ XTier (NetStorage) on the OES 2 server presented in the URL for the Web-based applications.
- ♦ The NetIdentity agent installed on the workstations.

For more information on using the NetIdentity agent, see the *NetIdentity Administration Guide for NetWare 6.5*.

Novell Modular Authentication Services (NMAS)

Novell Modular Authentication Services (NMAS™) lets you protect information on your network by providing various authentication methods to Novell eDirectory on NetWare, Windows, and UNIX networks.

These login methods are based on three login factors:

- ♦ Password
- ♦ Physical device or token
- ♦ Biometric authentication

For example:

- ♦ You can have users log in through a password, a fingerprint scan, a token, a smart card, a certificate, a proximity card, etc.
- ♦ You can have users log in through a combination of methods to provide a higher level of security.

Some login methods require additional hardware and software. You must have all of the necessary hardware and software for the methods to be used.

NMAS software consists of the following:

- ♦ **NMAS server components:** Installed as part of OES 2.
- ♦ **The NMAS Client:** Required on each Windows workstation that will be authenticating using NMAS.

Support for Third-Party Authentication Methods

Novell Client distributions include a number of NMAS login methods.

Other third-party methods are available for download. For information on the available third-party login methods, see the [NMAS Partner's Web site \(http://www.novell.com/products/nmas/partners_communities.html\)](http://www.novell.com/products/nmas/partners_communities.html). Each method has a `readme.txt` file or a `readme.pdf` file that includes specific installation and configuration instructions.

More Information

For more information on how to use NMAS, see the *Novell Modular Authentication Services 3.3.1 Administration Guide*.

Password Support in OES 2

In the past, administrators have needed to manage multiple passwords (simple password, NDS® passwords, Samba passwords) because of password differences. Administrators have also needed to deal with keeping the passwords synchronized.

In OES you have the choice of retaining your current password maintenance methods or deploying Universal Password to simplify password management. For more information, see the *Novell Password Management 3.2 Administration Guide*.

All Novell products and services are being developed to work with extended character (UTF-8 encoded) passwords. For a current list of products and services that work with extended characters, see [Novell TID 3065822](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3065822&sliceId=1&docTypeID=DT_TID_1_1&dialogID=77556590&stateId=0%200%2077560425) (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3065822&sliceId=1&docTypeID=DT_TID_1_1&dialogID=77556590&stateId=0%200%2077560425).

The password types supported in eDirectory are summarized in [Table 16-7](#).

Table 16-7 *eDirectory Password Types*

Password Type	Description
NDS	The NDS password is stored in a hash form that is nonreversible in eDirectory. Only the NDS system can make use of this password, and it cannot be converted into any other form for use by any other system.
Novell AFP and Novell CIFS	In OES 2, AFP and CIFS users have Universal Password policies assigned by default. The same policy can be used for both services, as shown in “ Creating a UP Policy to Support Both AFP and CIFS ” in the OES2 SP2: Lab Guide for Linux and Virtualized NetWare . More information about password policy planning is available in “ Coordinating Password Policies Among Multiple File Services ” in the OES2 SP1: Readme .
Samba	<p>In OES 2, Samba users have a Universal Password policy assigned by default.</p> <p>OES 2 also supports the Samba hash password if desired. However, you must choose to not deploy Universal Password if you want to use the Samba hash password. Choosing the Samba password requires that users always remember to synchronize it when changing their eDirectory password.</p> <p>For more information, see “Samba Passwords” in the OES2 SP1: Samba Administration Guide.</p>
Simple	<p>The simple password provides a reversible value stored in an attribute on the User object in eDirectory. NMAS securely stores a clear-text value of the password so that it can use it against any type of authentication algorithm. To ensure that this value is secure, NMAS uses either a DES key or a triple DES key (depending on the strength of the Secure Domain Key) to encrypt the data in the NMAS Secret and Configuration Store.</p> <p>The simple password was originally implemented to allow administrators to import users and hashed passwords from other LDAP directories such as Active Directory and iPlanet*.</p> <p>The limitations of the simple password are that no password policy (minimum length, expiration, etc.) is enforced. Also, by default, users do not have rights to change their own simple passwords.</p>

Password Type	Description
Universal	<p>Universal Password (UP) enforces a uniform password policy across multiple authentication systems by creating a password that can be used by all protocols and authentication methods.</p> <p>Universal Password is managed in iManager by the Secure Password Manager (SPM), a component of the NMAS module installed on OES 2 servers. All password restrictions and policies (expiration, minimum length, etc.) are supported.</p> <p>All the existing management tools that run on clients with the UP libraries automatically work with the Universal Password.</p> <p>Universal Password is not automatically enabled unless you install Novell AFP, Novell CIFS, Domain Services for Windows, or Novell Samba on an OES 2 Linux server. You can optionally choose to have the Samba hash password stored separately. This requires, however, that users always synchronize the Samba password when changing their eDirectory password.</p> <p>The Novell Client supports the Universal Password. It also supports the NDS password for older systems in the network. The Novell Client automatically upgrades to use Universal Password when UP is deployed.</p> <p>For more information, see “Deploying Universal Password” in the <i>Novell Password Management 3.2 Administration Guide</i>.</p>

16.2.2 Planning for Authentication

For planning topics, see the “[Access, Authenticate, Log in](#)” in the OES online documentation.

16.2.3 Authentication Coexistence and Migration

For authentication and security coexistence and migration information, see “[Chapter 21, “Security,” on page 231](#) and [Chapter 22, “Certificate Management,” on page 237](#)” in this guide.

16.2.4 Configuring and Administering Authentication

For a list of configuration and administration topics, see “[Access, Authenticate, Log in](#)” in the OES online documentation.

File Services

The file services in Open Enterprise Server 2 let you provide Web-based and network-based file services to your network users.

This section contains the following information:

- ♦ [Section 17.1, “Overview of File Services,” on page 191](#)
- ♦ [Section 17.2, “Planning for File Services,” on page 204](#)
- ♦ [Section 17.3, “Coexistence and Migration of File Services,” on page 208](#)
- ♦ [Section 17.4, “Aligning NCP and POSIX File Access Rights,” on page 210](#)
- ♦ [Section 17.5, “Native File Access Protocols Implementation and Maintenance,” on page 213](#)
- ♦ [Section 17.6, “NCP Implementation and Maintenance,” on page 214](#)
- ♦ [Section 17.7, “NetStorage Implementation and Maintenance,” on page 215](#)
- ♦ [Section 17.8, “Novell AFP Implementation and Maintenance,” on page 218](#)
- ♦ [Section 17.9, “Novell CIFS Implementation and Maintenance,” on page 218](#)
- ♦ [Section 17.10, “Novell iFolder 3.7 Implementation and Maintenance,” on page 219](#)
- ♦ [Section 17.11, “Samba Implementation and Maintenance,” on page 220](#)

NOTE: Novell® iFolder® 2 is available only on NetWare®.

There are no new features in iFolder 2, and most references to it have been removed from the OES 2 documentation. However, the iFolder 2 documentation on the [OES 1 Online Documentation Web site \(http://www.novell.com/documentation/oes/file-services.html#if2\)](http://www.novell.com/documentation/oes/file-services.html#if2) still applies.

17.1 Overview of File Services

The file service components in OES include the following:

- ♦ **FTP Services (page 192):** Lets users securely transfer files to and from OES 2 servers.
- ♦ **Native File Access Protocols (page 192):** Lets Linux, Macintosh, UNIX, and Windows users access and store files on OES 2 NetWare servers through their native file access methods.
- ♦ **NetWare Core Protocol (page 193):** Provides NetWare Core Protocol™ (NCP™) access to NetWare servers and to NCP volumes (including NSS volumes) that you define on OES 2 Linux server partitions.
- ♦ **NetStorage (page 194):** Provides network and Web access to various Linux, NetWare, and Windows file services.

The NetStorage server doesn't actually store files and folders. Rather, it provides access to other file services on OES 2 Linux and NetWare servers that support the native TCP/IP protocol.

- ♦ **Novell AFP (page 199):** Provides native Macintosh access to files stored on an NSS volume on an OES 2 Linux server.

- ♦ **Novell CIFS (page 200)**: Provides native Windows (CIFS and HTTP-WebDAV) access to files stored on an NSS volume on an OES 2 Linux server.
- ♦ **Novell iFolder 3.7 (page 201)**: Provides a Web-based and network-based repository (Novell iFolder server) that stores master copies of locally accessible files on the OES 2 server.
- ♦ **Novell Samba (page 203)**: Provides Windows (CIFS and HTTP-WebDAV) access to files stored on an OES 2 Linux server's file system.

The file service components in OES are generally compatible. However you cannot run Novell Samba on the same OES 2 server as Novell AFP, Novell CIFS, or Domain Services for Windows, which is not reviewed as a file service, but does include an alternative Samba file service.

17.1.1 Using the File Services Overviews

Each graphical overview in the following sections introduces one of the OES file service components. If visual presentations help you grasp basic concepts, continue with the following overviews. If you prefer to skip the overviews, go to **Section 17.2, "Planning for File Services,"** on **page 204**.

17.1.2 FTP Services

OES 2 NetWare has an FTP server that provides for securely transferring files to and from NetWare volumes. You can perform file transfers from any FTP client by using the NetWare FTP Server to log in to eDirectory™. For more information, see the *OES 2 : Novell FTP for NetWare Administration Guide*.

OES 2 Linux offers a level of integration between eDirectory and Pure-FTP that allows users to authenticate to eDirectory for FTP access to the server. You simply select the *Novell FTP Server* pattern in the OES 2 Linux installation and then make sure the users needing access are **LUM-enabled** and have access rights to the areas on the server they need to use. You can also migrate an existing FTP server configuration from a NetWare server to OES 2 Linux.

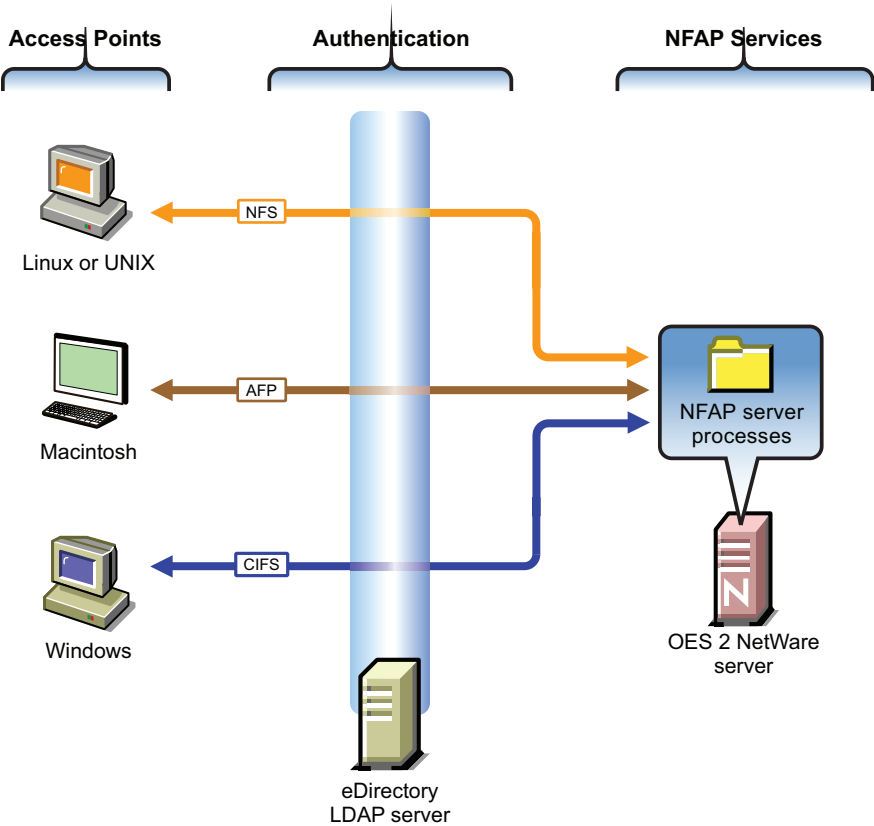
For migration instructions and a brief FAQ, see "Migrating FTP from NetWare to OES 2 SP1 Linux" in the *OES 2 SP1: Migration Tool Administration Guide*.

For documentation on Pure-FTP, visit the [Pure-FTP Web site \(http://pureftpd.sourceforge.net/documentation.shtml\)](http://pureftpd.sourceforge.net/documentation.shtml).

17.1.3 Native File Access Protocols

The Novell Native File Access Protocols (NFAP) product lets users on Macintosh, Windows, and UNIX workstations access and store files on OES 2 NetWare servers without installing any additional software, such as the Novell Client™ (see **Figure 17-1**).

Figure 17-1 Native File Access Protocol Support on NetWare



The following table explains the information illustrated in [Figure 17-1](#).

Table 17-1 NFAP Access

Access Methods	Authentication/File Encryption	NFAP Services
Linux, UNIX, Macintosh, and Windows workstation users can create drive mappings, mount points, etc., to the NetWare server. Then they can access the files as though they were stored on a network server that is native for the respective platforms.	All file service access is controlled by LDAP- based authentication through the eDirectory LDAP server. Although shown separately, eDirectory could be installed on the OES 2 server. After the service is fully configured, users can log in just as they would to access files on other native systems.	Files are stored on NSS volumes on OES 2 NetWare servers. The same files can be accessed by users on different platforms.

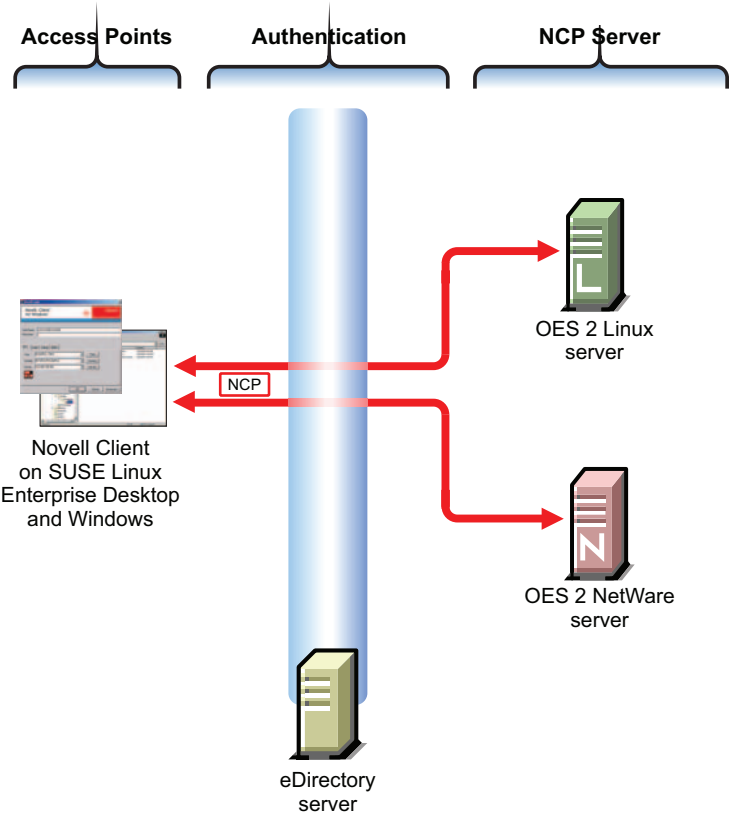
17.1.4 NetWare Core Protocol

NetWare Core Protocol (NCP) is the technology beneath many of the network services for which NetWare is famous.

In OES 2, NCP is also available on Linux. The Novell NCP Server for Linux provides the rich file services that Novell is known for. Windows and Linux users who run Novell Client software can now access data, manage files and folders, map drives, etc., using the same methods as they do on NetWare servers.

Figure 17-2 illustrates the basics of NCP file services. For more information on how NCP can help you manage access to network resources, see “Access Control and Authentication” on page 173.

Figure 17-2 NCP Services for Linux and NetWare



The following table explains the information illustrated in Figure 17-2.

Table 17-2 NCP Access

Access Methods	Authentication	NCP Services
Access is through an NCP client—specifically, the Novell Client.	All file service access is controlled by eDirectory authentication.	Files are stored on NetWare or NCP volumes that the administrator has created. The same core set of NetWare file attributes are available on both Linux and NetWare.

17.1.5 NetStorage

- ♦ “Common Network File Storage Problems” on page 195

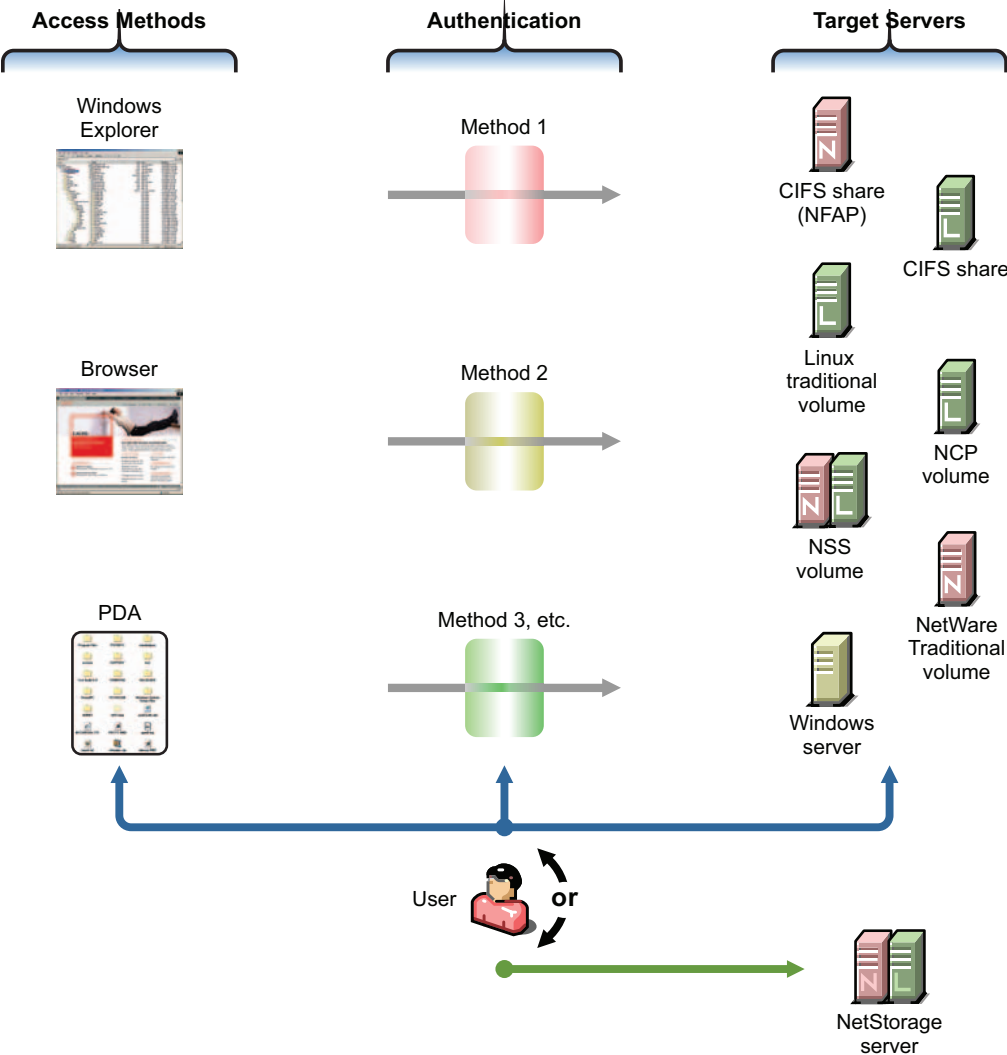
- ♦ “Novell NetStorage on Linux” on page 196
- ♦ “Novell NetStorage on NetWare” on page 197

NetStorage makes network files available anywhere, any time.

Common Network File Storage Problems

Network file access is often confusing and frustrating to users, as illustrated in Figure 17-3.

Figure 17-3 Common Network File Storage Problems



The following table explains the information illustrated in Figure 17-3.

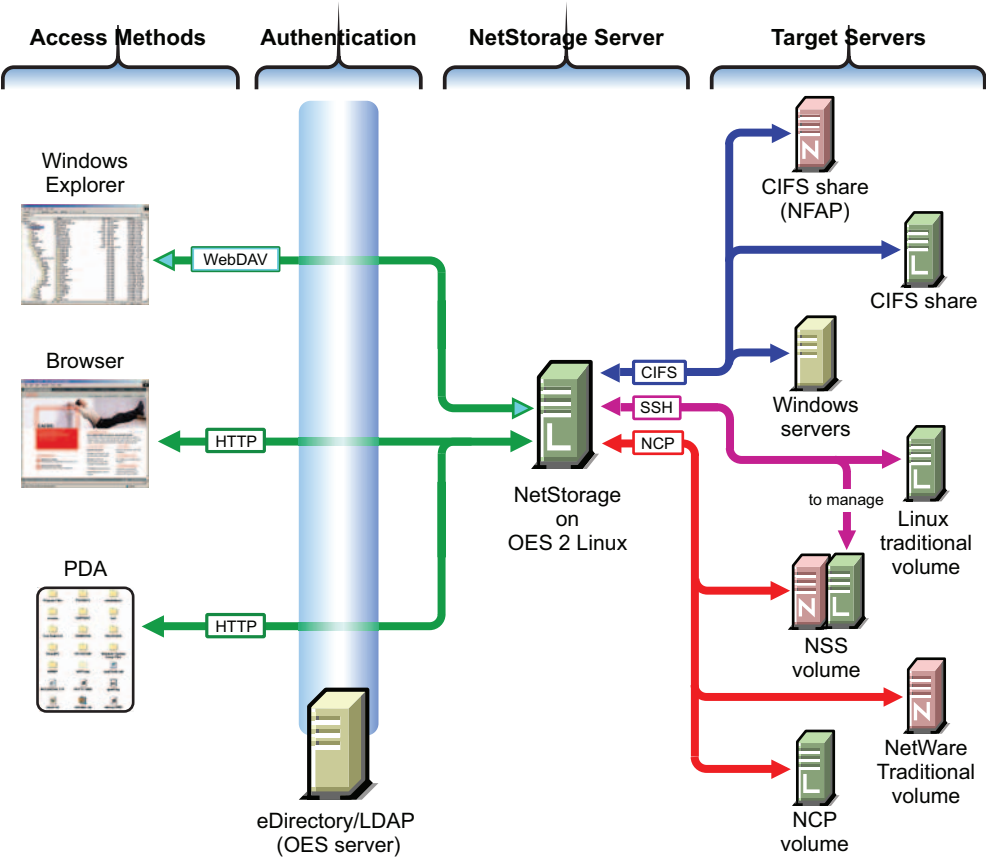
Table 17-3 NetStorage Access Solutions

Access Methods	Authentication	Target File Systems	Solution: NetStorage
Browser or PDA access is critical to those who must travel. However, access method support varies widely among file service providers.	Authentication helps protect information assets, but having diverse authentication methods leads to frustration and lost productivity.	Having diverse file storage services only adds to the complexity and confusion.	Novell NetStorage ties all of these issues together with an easy-to-administer, easy-to-use solution.

Novell NetStorage on Linux

NetStorage on Linux provides local and Web access to files on many systems without requiring the Novell Client (see [Figure 17-4](#)).

Figure 17-4 How NetStorage Works on OES 2 Linux



The following table explains the information illustrated in [Figure 17-4](#).

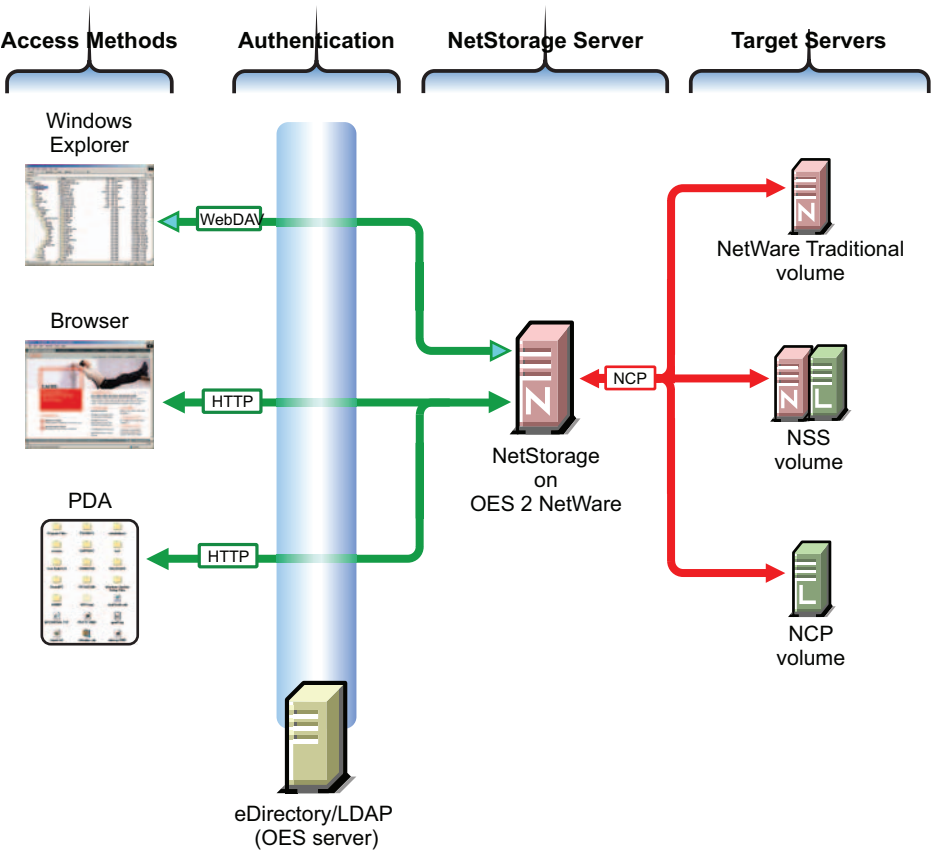
Table 17-4 *NetStorage on Linux*

Access Methods	Authentication	NetStorage Server	Target Servers
<p>Users have read and write access to files from</p> <ul style="list-style-type: none"> ♦ Windows Explorer: Enabled by the HTTP protocol with WebDAV extensions. ♦ Browsers: Users can access files directly by connecting to the NetStorage server. ♦ PDAs: PDA users with network connections can access their files as well. <p>Access is granted through login script drive mapping (NCP server required) or through Storage Location Objects.</p>	<p>File service access is controlled by LDAP-based authentication through the eDirectory LDAP server.</p> <p>Although shown separately, eDirectory could be running on the OES 2 server.</p>	<p>The NetStorage server receives and processes connection requests and provides access to storage on various servers on the network.</p>	<p>NetStorage on Linux can connect eDirectory users to their files and folders stored in the following locations:</p> <ul style="list-style-type: none"> ♦ The same targets as NetWare (see Figure 17-5 on page 198) if the NCP server is running ♦ Windows workgroup shares (CIFS or Samba shares) ♦ Linux POSIX volumes through an SSH connection. <p>Linux volumes can also be made available as NCP volumes.</p> <p>Management of NSS volumes on OES 2 Linux through NetStorage requires SSH access to the server. See “When Is SSH Access Required?” on page 101.</p>

Novell NetStorage on NetWare

NetStorage on NetWare provides local and Web access to files on NetWare and Linux without requiring the Novell Client software (see [Figure 17-5](#)).

Figure 17-5 How NetStorage Works on OES 2 NetWare



The following table explains the information illustrated in Figure 17-5.

Table 17-5 *NetStorage on NetWare*

Access Methods	Authentication	NetStorage Server	Target Servers
<p>Users have read and write access to files from</p> <ul style="list-style-type: none"> ♦ Windows Explorer: Enabled by the HTTP protocol with WebDAV extensions. ♦ Browsers: Users can access files directly by connecting to the NetStorage server. ♦ PDA: PDA users with network connections can access their files as well. <p>Access is granted through login script drive mapping or through Storage Location Objects.</p>	<p>File service access is controlled by LDAP-based authentication through the eDirectory LDAP server.</p> <p>Although shown separately, eDirectory could be running on the OES 2 server.</p>	<p>The NetStorage server receives and processes connection requests and provides access to storage on various servers on the network.</p>	<p>NetStorage on NetWare can connect eDirectory users to their files and folders stored in the following locations:</p> <ul style="list-style-type: none"> ♦ NetWare Traditional volumes where users have access rights ♦ NSS volumes on either NetWare or OES 2 Linux servers where users have access rights ♦ Any administrator-defined NCP volumes created on an OES 2 Linux server

17.1.6 Novell AFP

The Novell AFP service lets users on Macintosh workstations access and store files on OES 2 Linux servers with NSS volumes without installing any additional software, such as the Novell Client™ (see [Figure 17-6](#)).

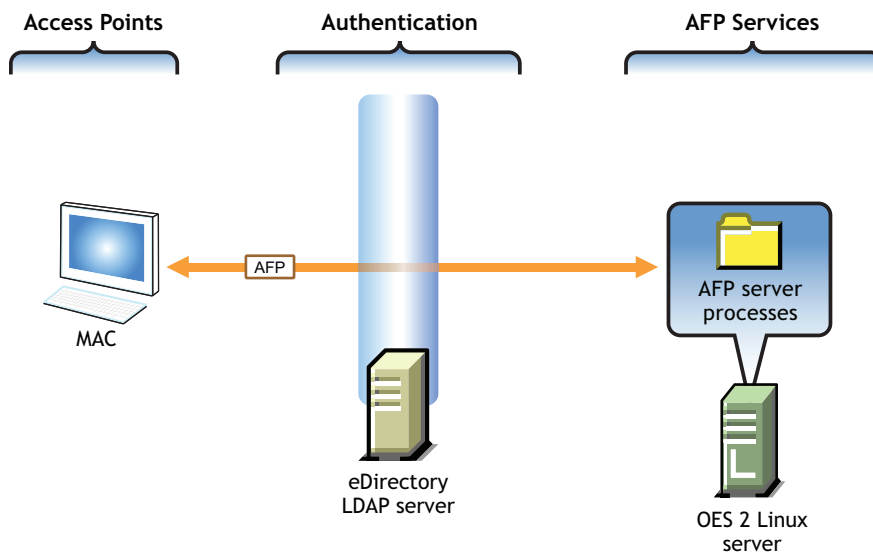
Figure 17-6 *How Novell AFP Works*

Table 17-6 AFP Access

Access Points	Authentication	AFP File Services
eDirectory users on Macintosh workstations have native access to the OES 2 server.	All file service access is controlled by LDAP-based authentication through the eDirectory LDAP server. Although shown separately, eDirectory could be installed on the OES 2 server.	Of course, the same files can also be accessed through other OES file services (such as NetStorage) that connect to Linux volumes.

17.1.7 Novell CIFS

The Novell CIFS service lets users on Windows workstations access and store files on OES 2 Linux servers with NSS volumes without installing any additional software, such as the Novell Client (see [Figure 17-6](#)).

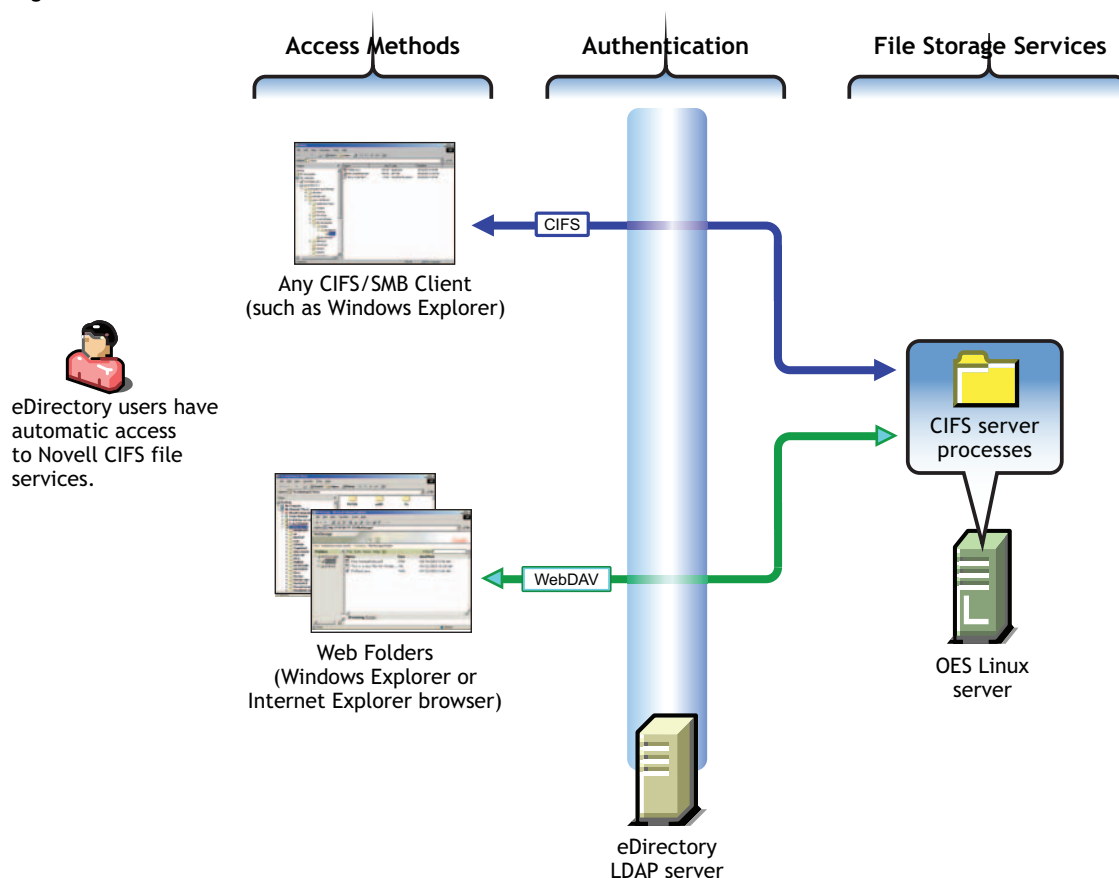
Figure 17-7 How Novell CIFS Works

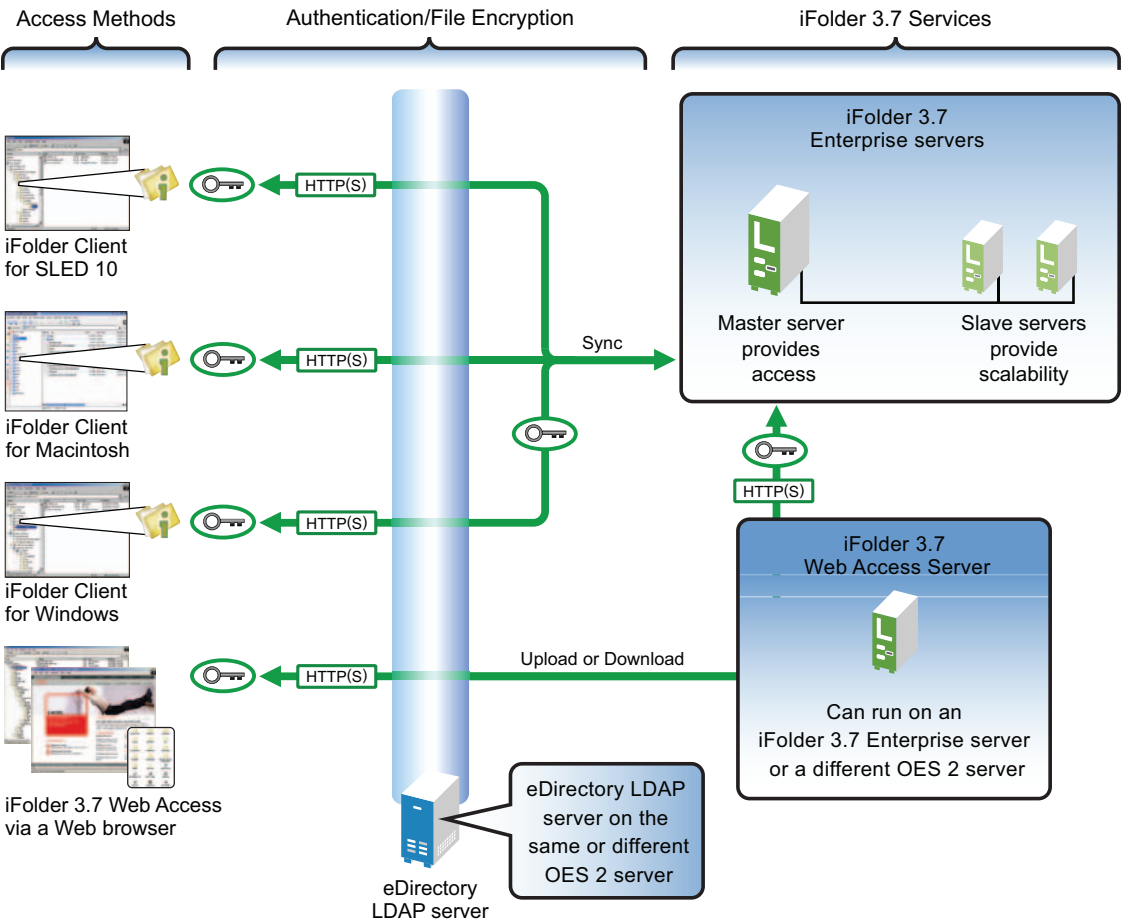
Table 17-7 *CIFS Access*

Access Methods	Authentication	CIFS File Services
<p>eDirectory users on Windows workstations have two native Windows file access options:</p> <ul style="list-style-type: none"> ♦ CIFS Client Access: Windows Explorer users can access and modify files on the OES 2 Linux server just as they would on any workgroup server share. ♦ Web Folder: Users can create Web Folders in Windows Explorer or Internet Explorer. <p>Files on the OES 2 Linux server are accessed and maintained with the HTTP-WebDAV protocol.</p>	<p>All file service access is controlled by LDAP-based authentication through the eDirectory LDAP server.</p> <p>Although shown separately, eDirectory could be installed on the OES 2 server.</p>	<p>Of course, the same files can also be accessed through other OES file services (such as NetStorage) that connect to NSS volumes.</p>

17.1.8 Novell iFolder 3.7

Novell iFolder 3.7 supports multiple iFolders per user, user-controlled sharing, and a centralized network server for file storage and secure distribution (see [Figure 17-8](#)).

Figure 17-8 How Novell iFolder Works



The following table explains the information illustrated in Figure 17-8.

Table 17-8 iFolder Access

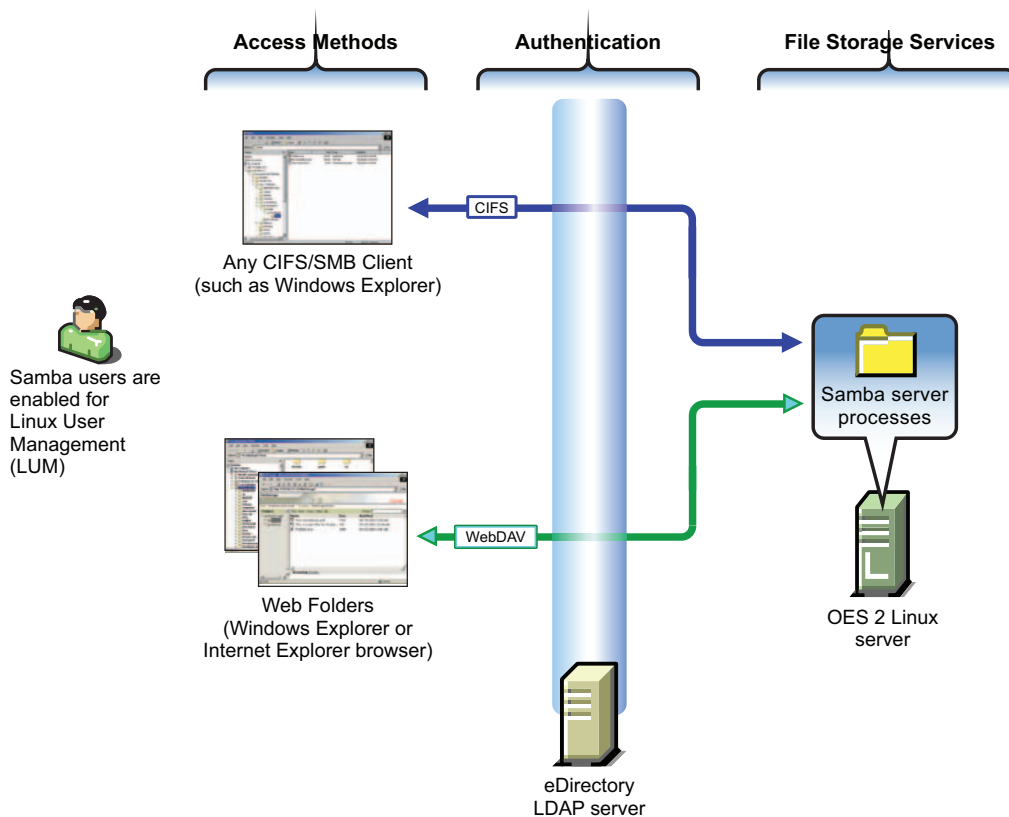
Access Methods	Authentication/File Encryption	Novell iFolder 3.7 Services
Linux and Windows workstation users who have the Novell iFolder Client installed can access and modify their files in one or more workstation folders. Changes are automatically synchronized with the iFolder 3.7 Enterprise servers.	All file service access is controlled by LDAP- based authentication through the eDirectory LDAP server.	Slave servers can be added as needed, providing the ability to dynamically grow iFolder services without disrupting users.
A Macintosh client for iFolder 3.7 is under development and expected to be released with OES 2 SP1.	Although shown separately, eDirectory could be installed on the OES 2 server.	Local and network copies of each file are automatically synchronized by the Novell iFolder Client and Server pieces.
A Web interface lets users access their files from any computer with an active network or Internet connection.	Files can be encrypted for transport using SSL connections (HTTPS).	

Additional overview information is available in “Overview of Novell iFolder 3.7” in the *OES 2 SPI: Novell iFolder 3.7 Administration Guide*.

17.1.9 Novell Samba

Samba on an OES 2 Linux server provides Windows (CIFS and HTTP-WebDAV) access to files stored on the OES 2 server (see Figure 17-9).

Figure 17-9 How Samba on OES Works



The following table explains the information illustrated in Figure 17-9.

Table 17-9 *Samba Access*

Access Methods	Authentication	File Storage Services
<p>eDirectory users on Windows workstations have two native Windows file access options (if their eDirectory accounts have been enabled for LUM and Samba):</p> <ul style="list-style-type: none"> ♦ CIFS Client Access: Windows Explorer users can access and modify files on the Samba server just as they would on any workgroup server share. ♦ Web Folder: Users can create Web Folders in Windows Explorer or Internet Explorer. <p>Files on the OES 2 Linux server running Samba are accessed and maintained with the HTTP-WebDAV protocol.</p>	<p>All file service access is controlled by LDAP-based authentication through the eDirectory LDAP server.</p> <p>Although shown separately, eDirectory could be installed on the OES 2 server.</p>	<p>Of course, the same files can also be accessed through other OES file services (such as NetStorage) that connect to Linux volumes.</p>

Samba is an open source initiative. In addition to Linux support, Samba initiatives provide support for other platforms such as Apple Computer's operating systems. More information is available on the [Web \(http://www.samba.org\)](http://www.samba.org).

17.2 Planning for File Services

Functional overviews of each file service product are included in [Section 17.1, "Overview of File Services,"](#) on page 191.

- ♦ [Section 17.2.1, "Deciding Which Components Match Your Needs,"](#) on page 204
- ♦ [Section 17.2.2, "Comparing Your CIFS File Service Options,"](#) on page 206
- ♦ [Section 17.2.3, "Planning Your File Services,"](#) on page 207

17.2.1 Deciding Which Components Match Your Needs

To decide which file service components to install, you should match service features listed in [Table 17-10](#) to your network's file service requirements.

Table 17-10 *OES File Services Feature Breakdown*

Service	Access Method Features	Back-End Storage Features	Security Features
NCP Server (NetWare Core Protocol)	Novell Client (NCP client)	<ul style="list-style-type: none"> ♦ Any Linux volumes (including NSS) that are defined as NCP volumes ♦ NetWare volumes 	<ul style="list-style-type: none"> ♦ eDirectory Authentication

Service	Access Method Features	Back-End Storage Features	Security Features
NetStorage	<ul style="list-style-type: none"> ♦ Any supported browsers ♦ Personal Digital Assistant (PDA) ♦ Remote (browser-based) ♦ Web Folders (on either an Internet Explorer browser or in Windows Explorer) ♦ Windows Explorer 	<ul style="list-style-type: none"> ♦ Linux POSIX volumes ♦ NetWare volumes ♦ NCP volumes ♦ NSS volumes ♦ Samba (CIFS) servers ♦ Windows (CIFS) servers 	<ul style="list-style-type: none"> ♦ Secure LDAP Authentication
NetWare AFP, CIFS, and NFS support (Native File Access Protocols)	<ul style="list-style-type: none"> ♦ Linux File Managers ♦ Macintosh Finder* ♦ UNIX File Managers ♦ Windows Explorer 	<ul style="list-style-type: none"> ♦ NetWare volumes 	<ul style="list-style-type: none"> ♦ Secure LDAP Authentication
Novell AFP	<ul style="list-style-type: none"> ♦ Macintosh Chooser 	<ul style="list-style-type: none"> ♦ NSS volumes 	<ul style="list-style-type: none"> ♦ Secure LDAP Authentication
Novell CIFS	<ul style="list-style-type: none"> ♦ Any CIFS client ♦ Remote access (Web Folders in the Internet Explorer browser) ♦ Windows Explorer 	<ul style="list-style-type: none"> ♦ NSS volumes 	<ul style="list-style-type: none"> ♦ Secure LDAP Authentication
Novell iFolder 3.7	<ul style="list-style-type: none"> ♦ Linux File Managers ♦ Macintosh Chooser ♦ Offline access with file synchronization (between local and network copies) on reconnect ♦ Web browsers ♦ Windows Explorer 	<ul style="list-style-type: none"> ♦ Novell iFolder 3.7 Enterprise server file repository on OES 2 Linux server 	<ul style="list-style-type: none"> ♦ Files can be encrypted for transport through SSL (HTTPS). ♦ Secure LDAP Authentication
Novell Samba (Linux only)	<ul style="list-style-type: none"> ♦ Any CIFS client ♦ Remote access (Web Folders in the Internet Explorer browser) ♦ Windows Explorer 	<ul style="list-style-type: none"> ♦ Linux POSIX file system on OES 2 server ♦ NSS volumes 	<ul style="list-style-type: none"> ♦ Secure LDAP Authentication

17.2.2 Comparing Your CIFS File Service Options

OES 2 SP1 offers three file services that use the CIFS protocol: Novell CIFS, Novell Samba, and Samba in Domain Services for Windows (DSfW).

Table 17-11 Comparing OES 2 CIFS Solutions

Item	Novell CIFS	Novell Samba	Samba in DSfW
Authentication	A Password policy that allows the CIFS proxy user to retrieve passwords is required.	A Samba-compatible Password policy is required for compatibility with Windows workgroup authentication.	<p>The Domain Services Password policy is required for DSfW users. The domain is set up as a trusted environment.</p> <p>DSfW uses Active Directory authentication methods, such as Kerberos*, to ensure that only authorized users can log in to the domain.</p>
File system support	NSS is the only file system supported for this release.	<p>It is recommended (but not required) that you create Samba shares on NSS data volumes.</p> <p>NSS is fully integrated with eDirectory for easier management, and using an NSS volume allows you to take advantage of the rich data security model in NSS. You can use either iManager or the nssmu utility to create an NSS volume on an OES 2 Linux server. For instructions on how to set up an NSS volume, see <i>"Managing NSS Volumes"</i> in the <i>OES 2 SP1: File Systems Management Guide</i>.</p>	
LUM and Samba enablement	LUM and Samba enablement are not required.	Users must be enabled for LUM and Samba and assigned to a Samba group.	<p>eDirectory users in the domain (eDirectory partition) are automatically Samba users and are enabled to access Samba shares. See <i>"Creating and Provisioning Users"</i> in the <i>OES 2 SP1: Domain Services for Windows Administration Guide</i>.</p> <p>Domain users are set up with the necessary UID and default group (DomainUsers) membership.</p> <p>Every additional eDirectory group created within the domain is automatically Linux-enabled.</p>

Item	Novell CIFS	Novell Samba	Samba in DSfW
Username and password	The same username and password must exist on both the Windows workstation and in eDirectory.	The same username and password must exist on both the Windows workstation and in eDirectory.	eDirectory users in the domain (eDirectory partition) can log into any workstation that has joined the domain. There is no need for a corresponding user object on the workstation.

17.2.3 Planning Your File Services

- 1 For the file services you plan to install, compute the total additional RAM required (above the basic system requirement).
 - ♦ **Native File Access Protocols:** There are no additional RAM requirements.
 - ♦ **NCP:** There are no additional RAM requirements.
 - ♦ **NetStorage:** There are no additional RAM requirements.
 - ♦ **Novell AFP:** There are no additional RAM requirements.
 - ♦ **Novell CIFS:** There are no additional RAM requirements.
 - ♦ **Novell iFolder 3.7:** Suggestions for calculating the additional RAM you need are contained in “**Server Workload Considerations**” in the *OES 2 SP1: Novell iFolder 3.7 Administration Guide*.
 - ♦ **Samba:** There are no additional RAM requirements.
- 2 Record the additional required RAM in your planning notes.
- 3 For the file services you plan to install, compute the total additional disk space required (above the basic system requirement).
 - ♦ **Native File Access Protocols:** Allocate enough disk space to meet your users’ file storage needs. Because all platforms can access the same storage space, you need only consider the total space needed, not the platform-specific requirements.
 - ♦ **NCP:** Allocate enough disk space to meet your users’ file storage needs. On Linux, this space must exist on partitions you have designated as NCP volumes. On NetWare, all volumes are accessible through NCP.
 - ♦ **NetStorage:** There are no disk space requirements because NetStorage provides access only to other file storage services.
 - ♦ **Novell AFP:** Allocate enough disk space for the partition containing the /home directories to meet your users’ file storage needs.
 - ♦ **Novell CIFS:** Allocate enough disk space for the partition containing the /home directories to meet your users’ file storage needs.
 - ♦ **Novell iFolder 3.7:** Suggestions for calculating the additional disk space you need are contained in “**Server Workload Considerations**” in the *OES 2 SP1: Novell iFolder 3.7 Administration Guide*.
 - ♦ **Samba:** Allocate enough disk space for the partition containing the /home directories to meet your users’ file storage needs.
- 4 Record the additional required disk space in your planning notes.

- 5 For the file services you plan to install, refer to the information in the OES 2 installation guides indicated in the following table and note your planning choices on your planning sheet.

File Service Product	Linux Planning References	NetWare Planning References
Native File Access Protocols	N/A	The following sections in the <i>OES 2 SP1: AFP, CIFS, and NFS for NetWare (NFAP) Administration Guide</i> . <ul style="list-style-type: none"> ♦ “Preparing for CIFS and AFP” ♦ “Administrator Workstation Prerequisites” ♦ “Client Computer Prerequisites”
NCP	“Novell NCP Server / Dynamic Storage Technology” in the <i>OES 2 SP1: Linux Installation Guide</i>	Installed by default. No additional planning required.
NetStorage	“Novell NetStorage” in the <i>OES 2 SP1: Linux Installation Guide</i>	“NetStorage Install” in the <i>OES 2 SP1: NetWare Installation Guide</i>
Novell AFP	“Novell AFP for Linux” in the <i>OES 2 SP1: Linux Installation Guide</i>	N/A
Novell CIFS	“Novell CIFS for Linux” in the <i>OES 2 SP1: Linux Installation Guide</i>	N/A
Novell iFolder 3.7	“Novell iFolder” in the <i>OES 2 SP1: Linux Installation Guide</i>	N/A
Samba	“Novell Samba” in the <i>OES 2 SP1: Linux Installation Guide</i>	N/A

17.3 Coexistence and Migration of File Services

Storing shared data on network servers is only half of the picture. The other half is making it possible for users of Windows, Macintosh, and UNIX/Linux workstations to access the data. In some networks, the installation of special software is permitted on the workstations to provide client access. Others require users to be able to access shared data without installing extra software on the workstation.

This section discusses migration of the following services:

- ♦ Section 17.3.1, “Novell Client (NCP),” on page 209
- ♦ Section 17.3.2, “Native File Access Protocols,” on page 209
- ♦ Section 17.3.3, “NetStorage,” on page 209
- ♦ Section 17.3.4, “Novell AFP,” on page 209
- ♦ Section 17.3.5, “Novell CIFS,” on page 210
- ♦ Section 17.3.6, “Novell iFolder 3.7,” on page 210
- ♦ Section 17.3.7, “Samba,” on page 210

17.3.1 Novell Client (NCP)

Novell Client for Windows is the long-standing software solution for providing NCP access to NetWare data from Windows workstations. The Novell Client extends the capabilities of Windows desktops to access the full range of Novell services, such as authentication to eDirectory, network browsing and service resolution, and secure file system access. It supports traditional Novell protocols such as NCP, RSA, and NDAP, and it interoperates with open protocols such as LDAP. For more information on the Novell Client for Windows, see the *Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide*.

The Novell Client for Linux provides these same services for Linux workstations. For more information on the Novell Client for Linux, see the *Novell Client 2.0 SP1 for Linux Administration Guide*.

Because NCP is now available on Linux, Novell Client users can attach to OES 2 Linux servers as easily as they have been able to attach to NetWare servers. The NCP Server for Linux enables support for login script, mapping drives to OES 2 Linux servers, and other services commonly associated with Novell Client access.

For more information on NCP Server for Linux, see the *OES 2 SP1: NCP Server for Linux Administration Guide*.

17.3.2 Native File Access Protocols

On NetWare servers, the Native File Access Protocols (NFAP) service allows users of Windows, Macintosh, and UNIX/Linux workstations to access NetWare server data through their native interfaces. No Novell Client software is required.

With NFAP, Windows workstations can access data through the Common Internet File System (CIFS) protocol. Macintosh workstations can access data through the Apple Filing Protocol (AFP). UNIX/Linux workstations can access data through the Network File System (NFS) protocol.

17.3.3 NetStorage

NetStorage provides Web access to the files and directories on OES 2 servers from browsers and Web-enabled devices such as PDAs.

In OES 2, NetStorage is available for both NetWare and Linux and both are capable of pointing to the file systems on the other. Because NetStorage is a service that facilitates access to file services in various locations but doesn't actually store files, there are no coexistence or migration issues to consider.

For more information about NetStorage, see the *OES 2: NetStorage for NetWare Administration Guide* or the *OES 2 SP1: NetStorage for Linux Administration Guide*.

17.3.4 Novell AFP

Novell AFP provides native AFP protocol access from Macintosh workstations to data on OES 2 Linux servers, offering the same basic AFP connectivity that was previously available only on NetWare. No Novell Client software is required.

For information on migrating AFP services from NetWare to OES 2 Linux, see “*Migrating AFP from NetWare to OES 2 SP1 Linux*” in the *OES 2 SP1: Migration Tool Administration Guide*.

17.3.5 Novell CIFS

Novell CIFS provides native CIFS protocol access from Windows workstations to data on OES 2 Linux servers, offering the same basic CIFS connectivity that was previously available only on NetWare. No Novell Client software is required.

For information on migrating CIFS services from NetWare to OES 2 Linux, see “[Migrating CIFS from NetWare to OES 2 SP1 Linux](#)” in the *OES 2 SP1: Migration Tool Administration Guide*.

17.3.6 Novell iFolder 3.7

iFolder 3.7 supports multiple iFolders per user, user-controlled sharing, and a centralized network of servers to provide scalable file storage and secure distribution. Users can share files in multiple iFolder folders, and share each iFolder folder with a different group of users. Users control who can participate in an iFolder folder and their access rights to the files in it. Users can also participate in iFolder folders that others share with them.

Novell iFolder 3.7 is available only on OES 2 Linux.

For information on migrating from iFolder 2 to iFolder 3.7, see “[Migrating iFolder 2.x](#)” in the *OES 2 SP1: Migration Tool Administration Guide*.

17.3.7 Samba

OES 2 Linux includes Samba software to provide Microsoft CIFS and HTTP-WebDAV access to files on the server. This is especially useful to those who don’t want to use the Novell Client.

There is no migration path from Novell CIFS (NFAP) to Samba.

For more information about Samba in OES 2, see the *OES2 SP1: Samba Administration Guide*.

17.4 Aligning NCP and POSIX File Access Rights

NetWare administrators have certain expectations regarding directory and file security. For example, they expect that home directories are private and that only the directory owners can see directory contents. However, because of the differences in the NetWare Core Protocol (NCP) and POSIX file security models (see [Section 21.2.1, “Comparing the Linux and the NetWare Core Protocol \(NCP\) File Security Models,” on page 233](#)) that is not the case by default on POSIX file systems.

Fortunately, when you install Linux User Management (LUM) in OES 2, there is an option to make home directories private. This option automatically provides the privacy that NetWare administrators are used to seeing. Unfortunately, the option only applies to newly created home directories, so there is more to understand and do if aligning access rights is an issue for you.

Use the information in this section to understand how you can configure POSIX directories to more closely align with the NCP model.

- ♦ [Section 17.4.1, “Managing Access Rights,” on page 211](#)
- ♦ [Section 17.4.2, “Providing a Private Work Directory,” on page 212](#)
- ♦ [Section 17.4.3, “Providing a Group Work Area,” on page 212](#)
- ♦ [Section 17.4.4, “Providing a Public Work Area,” on page 213](#)
- ♦ [Section 17.4.5, “Setting Up Rights Inheritance,” on page 213](#)

17.4.1 Managing Access Rights

NCP directories are, by default, private. When you assign a user or a group as a trustee of a directory or file, those trustees can automatically navigate to the assigned area and exercise whatever access privileges you have assigned at that level and below. You can assign as many trustees with different access privileges as you need.

On the other hand, Linux POSIX directories can be accessed through three sets of permissions defined for each file object on a Linux system. These sets include the read (r), write (w), and execute (x) permissions for each of three types of users: the file owner, the group, and other users. The Linux kernel in OES 2 also supports access control lists (ACLs) to expand this capability. However, ACLs are outside the scope of this discussion. For more information on ACLs, see “[Access Control Lists](http://www.novell.com/documentation/sles10/sles_admin/data/cha_acls.html)” (http://www.novell.com/documentation/sles10/sles_admin/data/cha_acls.html) in the *SLES 10 SP2: Installation and Administration Guide* (http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html).

The Linux `chown` command lets you change the file owner and/or group to a LUM user or a LUM-enabled group. For example, `chown -R user1 /home/user1` changes the owner of the `user1` home directory and all its subdirectories and files to `user1`. For more information, see the `chown` man page on your OES 2 Linux server.

The Linux `chmod` command provides a very simple and fast way of adjusting directory and file access privileges for the three user types: owner, group, and other (all users). In its simplest form, the command uses three numbers, ranging from 0 through 7, to represent the rights for each of the three user types. The first number sets the rights for the owner, the second number sets the rights for the group, and the third number sets the rights for all others. Each number represents a single grouping of rights, as follows:

Number	Setting	Binary Representation
0	- - -	0 0 0
1	- - x	0 0 1
2	- w -	0 1 0
3	- w x	0 1 1
4	r - -	1 0 0
5	r - x	1 0 1
6	r w -	1 1 0
7	r w x	1 1 1

Those familiar with the binary number system find this method an easy way to remember what each number represents.

For example, the command `chmod 777 /home` would grant read, write and execute rights (7) to owner, group, and other for the `/home` directory, while `chmod 700 /home` would grant the three rights to only the directory owner, with group and other having no rights. `chmod 750 /home` would grant `rw` rights to the owner, `r-x` rights to the group, and no rights to other users.

For more information about the `chmod` command, see the `chmod` man page on your OES 2 Linux server.

17.4.2 Providing a Private Work Directory

To make an NCP directory private, you assign a single user as the trustee and make sure that no unexpected users or groups have trustee rights in any of the parent directories.

To provide a private work area on a Linux POSIX volume:

- 1 Make the user is the directory owner. For example, you could use the `chown` command to change the owner (user),

```
chown -R user: /path/user_dir
```

where *user* is the eDirectory user, *path* is the file path to the work directory, and *user_dir* is the work directory name. The `-R` option applies the command recursively to all subdirectories and files.

- 2 Grant only the user read, write, and execute rights (rwx --- ---) to the directory. For example, you could use the `chmod` command as follows,

```
chmod -R 700 /path/user_dir
```

where *path* is the file path to the work directory, and *user_dir* is the work directory name.

- 3 Check each parent directory in the path up to the `root (/)` directory, making sure that all users (referred to as “other users” in Linux) have read and execute rights (r-x) in each directory as shown by the third group of permissions (..... r-x). (Owner and group permissions are represented by dots because their settings are irrelevant.)

The reason for checking directories is that in the parent directories the directory owners are “other” users and they need to be able to see the path down to their own private directories.

Because r-x is the default for most directories on Linux, you probably won’t need to change the permissions.

17.4.3 Providing a Group Work Area

On an NCP volume, you can provide a group work area by assigning users to a group and then granting the group trustee rights to the directory. As an alternative, if users need different levels of access within the work area, you can assign each user as a trustee and grant only the rights needed.

To provide a group work area on a Linux POSIX volume:

- 1 Use the `chown` command to set group ownership for the directory. For example, you could enter

```
chown -R :group /path/group_dir
```

where *group* is the group name, *path* is the file path to the work area, and *group_dir* is the group work directory. The `-R` option applies the action to all subdirectories and files in *group_dir*.

- 2 Grant the group read, write, and execute rights (.. rwx ..). (Owner and other permissions are represented by dots because their settings are irrelevant.)

For example, you could enter

```
chmod -R 770 /path/group_dir
```

where *path* is the file path to the work area, and *group_dir* is the group work directory. The second 7 grants rwx to the group. (The example assumes that the owner of the directory should also retain all rights. Therefore, the first number is also 7.)

- 3 Check each parent directory in the path up to the `root (/)` directory, making sure that the group has read and execute rights (r-x) in each directory as shown by the second group of permissions (. . . r-x . . .).

Use the `chmod` command to adjust this where necessary by specifying the number 5 for the group permission. For more information, see “[Section 17.4.1, “Managing Access Rights,” on page 211.](#)”

17.4.4 Providing a Public Work Area

On an NCP volume, you can provide a public work area by assigning [Public] as a trustee and then granting the required trustee rights to the directory.

For the work area itself, you would set permissions for the owner, group, and all others to read, write, and execute rights (rwx rwx rwx) (`chmod 777`).

All others must also have read and execute rights on the system in each parent directory in the path all the way to the root of the Linux system. This means that you set permissions for all parent directories to rwx --- r-x.

To provide a public work area on a Linux POSIX volume:

- 1 Use the `chown` command to assign all rights (rwx) to other (all users). For example, you could enter

```
chmod -R 707 /path/group_dir
```

where *path* is the file path to the work area, and *group_dir* is the group work directory. The third 7 grants rwx to the group. (The example assumes that the owner of the directory should also retain all rights and that the group setting is irrelevant.)

- 2 Check each parent directory in the path up to the `root (/)` directory, making sure that all users (other) have read and execute rights (r-x) in each directory as shown by the third group of permissions (. rwx). (Owner and group permissions are represented by dots because their settings are irrelevant.)

Use the `chmod` command to adjust this where necessary by specifying the number 5 for the other permission. For more information, see “[Managing Access Rights](#)” at the beginning of this section.

17.4.5 Setting Up Rights Inheritance

The final step in aligning POSIX rights to the NCP model is setting the Inherit POSIX Permissions volume flag in the NCP configuration file so that all files and subdirectories created in these areas inherit the same permissions as their parent directory. For instructions, see “[Configuring Inherit POSIX Permissions for an NCP Volume](#)” in the *OES 2 SPI: NCP Server for Linux Administration Guide*.

17.5 Native File Access Protocols Implementation and Maintenance

After installing a NetWare server, if you want to provide native access to Linux, Macintosh, UNIX, or Windows users, there are tasks to complete for each of the platforms.

The *OES 2 SP1: AFP, CIFS, and NFS for NetWare (NFAP) Administration Guide* contains the following relevant sections:

- ♦ “Working with UNIX Machines”
- ♦ “Working with Macintosh Computers”
- ♦ “Working with Windows Computers”

To ensure a successful NFAP implementation, complete all the instructions in the sections for your chosen platforms.

Because NFAP provides native protocol access to files on NSS volumes on the NetWare server, the service is covered by maintenance tasks that apply to NSS file systems. For information on maintaining file services on NetWare, see the “Storage and File Systems” links in the online documentation.

17.6 NCP Implementation and Maintenance

The implementation information in the following sections can help you get started with NCP on OES 2 servers.

- ♦ Section 17.6.1, “NCP Services on NetWare,” on page 214
- ♦ Section 17.6.2, “Novell NCP Server for Linux,” on page 214
- ♦ Section 17.6.3, “Assigning File Trustee Rights,” on page 215
- ♦ Section 17.6.4, “NCP Maintenance,” on page 215

17.6.1 NCP Services on NetWare

After installing an OES 2 NetWare server, eDirectory users on Windows workstations with the Novell Client installed can access all the directories and files that you have granted them access to.

A common way for granting access is using the menu button (the red N) located in the system tray (taskbar) on most workstations after the Novell Client is installed. More information about managing file access is available in Chapter 16, “Access Control and Authentication,” on page 173.

17.6.2 Novell NCP Server for Linux

If you have installed the NCP Server for Linux, the same eDirectory/Novell Client users can access files on the OES 2 Linux server.

- ♦ “The Default NCP Volume” on page 214
- ♦ “Creating Home and Data Volume Pointers” on page 215

The Default NCP Volume

The NCP Server for Linux enables NCP access to NCP volumes defined on the OES 2 Linux server. When you install the NCP server, the installation creates one NCP volume named `SYS:` that maps to the `/usr/novell/sys` folder on the Linux server.

This NCP volume contains `LOGIN` and `PUBLIC` directories that, in turn, contain a small subset of the files found on a NetWare server in the directories with the same names.

Creating Home and Data Volume Pointers

Initially, there are no NCP home directories or data volumes available to Novell Clients that attach to an OES 2 Linux server.

For existing eDirectory users: If you want users to have NCP home or data directories on the server, you must decide where you want these directories to reside on the server's partitions and then create NCP volumes by using the NCPCON utility at the Linux command prompt.

For example, if you wanted to create an NCP volume (pointer) named `HOME` and mount it to the `/usr` folder on the Linux server, you would enter the following command at the command prompt:

```
ncpcon create volume HOME /usr
```

After issuing this command, when a Novell Client attaches to the OES 2 Linux server, the `HOME:` volume appears along with the `SYS:` volume created by the installation.

For new eDirectory users: If you create an NCP or NSS volume on the server prior to creating users, then you have the option of specifying that volume in iManager as the location of the home directory for the new users.

IMPORTANT: NCP Volume pointers are always created with uppercase names (`HOME:`, `SYS:`, etc.) regardless of the case specified when the volume pointers are created.

17.6.3 Assigning File Trustee Rights

You can use the same methods for assigning file trustee rights on NCP volumes on OES 2 Linux servers that you use when assigning them on NetWare. For example, the Novell Client can be used by anyone with the Access Control right on the volume, or the root user can use the `ncpcon` utility > `rights` command at a command prompt to administer NCP trustee rights. See “[Managing File System Trustees, Trustee Rights, and Attributes on NCP Volumes](#)” in the *OES 2 SPI: NCP Server for Linux Administration Guide*. (The `ncpcon rights` command is related to but not the same as the `rights` utility used to manage trustees on NSS volumes.)

17.6.4 NCP Maintenance

Because NCP provides Novell Client access to files on OES 2 NetWare and OES 2 Linux servers, the service is covered by maintenance tasks that apply to file systems on these servers. For information on maintaining file services, see the “[storage and file systems](#)” section in the online documentation.

17.7 NetStorage Implementation and Maintenance

The following sections are provided only as introductory information. For more information about using NetStorage, see the *OES 2: NetStorage for NetWare Administration Guide*.

- ♦ [Section 17.7.1, “About Automatic Access and Storage Locations,”](#) on page 216
- ♦ [Section 17.7.2, “About SSH Storage Locations,”](#) on page 216
- ♦ [Section 17.7.3, “Novell iFolder 2 Doesn’t Use Storage Locations,”](#) on page 216
- ♦ [Section 17.7.4, “Assigning User and Group Access Rights,”](#) on page 217

- ♦ [Section 17.7.5, “Authenticating to Access Other Target Systems,” on page 217](#)
- ♦ [Section 17.7.6, “NetStorage Authentication Is Not Persistent by Default,” on page 217](#)
- ♦ [Section 17.7.7, “NetStorage Maintenance,” on page 218](#)

17.7.1 About Automatic Access and Storage Locations

The inherent value of NetStorage lies in its ability to connect users with various servers and file systems. Some connections are created automatically depending on the OES platform where NetStorage is installed. Other connections must be created by the network administrator.

Table 17-12 *NetStorage Access Summary*

OES Platform	Automatic Access
Linux	<ul style="list-style-type: none"> ♦ NSS volumes on the same server that use the default mount point (/media/nss) ♦ User Home directories that are specified in eDirectory on NCP or NSS volumes. ♦ Drive mapping locations in login scripts of the user logging in (if the NCP Server for Linux is running on the server)
NetWare	<ul style="list-style-type: none"> ♦ User Home directories ♦ Novell iFolder 2 folders on the same server ♦ Drive mapping locations in login scripts of the user logging in

To provide access to file systems not listed in [Table 17-12](#), you must create Storage Location objects in eDirectory. For instructions on creating Storage Locations, see the following:

- ♦ For Linux: “[Creating a Storage Location Object](#)” in the *OES 2 SP1: NetStorage for Linux Administration Guide*
- ♦ For NetWare: “[Creating a Storage Location Object](#)” in the *OES 2: NetStorage for NetWare Administration Guide*

17.7.2 About SSH Storage Locations

If you plan to use SSH storage locations, be aware that by default any users who are enabled for Samba cannot access data stored at the SSH locations. Additional steps are required to grant simultaneous access to Samba and SSH. For more information, see [Section 11.4, “SSH Services on OES 2 Linux,” on page 100](#).

17.7.3 Novell iFolder 2 Doesn’t Use Storage Locations

Novell iFolder 2 access in NetStorage is controlled through the iFolder Storage Provider task in iManager and does not involve Storage Location objects. For more information about the iManager task, see the context-sensitive help in iManager.

17.7.4 Assigning User and Group Access Rights

Because NetStorage provides access to other file storage systems, the users and groups that access the other systems through NetStorage must be created and granted file and directory access on those systems.

For example:

- ♦ NetWare users must exist in the eDirectory tree where the NetWare server resides and have access rights to the files and directories on the NetWare server.
- ♦ Windows users must exist on the Windows systems and have the required access rights to the files and directories on those systems.
- ♦ If your users will access Samba files on an OES 2 Linux server, they must be enabled for LUM and Samba access on the OES 2 Linux server. For more information, see [“Services in OES 2 Linux That Require LUM-Enabled Access” on page 160](#).

IMPORTANT: The usernames and passwords used to authenticate to the NetStorage (OES) server through eDirectory must match the usernames and passwords defined on the target systems.

17.7.5 Authenticating to Access Other Target Systems

The OES installation establishes a primary authentication domain for NetStorage. To access any storage location, users must exist somewhere in this primary domain. When it receives an authentication request, NetStorage searches for the username in the context you specified during OES installation and in all its subcontexts.

Authentication to other file systems is often controlled by other authentication domains. For example, you might create a storage location on the OES 2 server that points to a NetWare server that resides in a different eDirectory tree. To access this storage location, users must authenticate to the other tree.

This means that you must specify an additional context in the NetStorage configuration as a nonprimary authentication domain.

When defining a nonprimary authentication domain, you must

- ♦ Ensure that the username and password in the nonprimary domain matches the username and password in the primary domain.
- ♦ Specify the exact context where User objects reside. NetStorage doesn't search the subcontexts of nonprimary authentication domains.

For more information about managing NetStorage authentication domains, see [“Authentication Domains”](#) in the *OES 2: NetStorage for NetWare Administration Guide* and see [“Authentication Domains”](#) in the *OES 2 SP1: NetStorage for Linux Administration Guide*.

17.7.6 NetStorage Authentication Is Not Persistent by Default

By default, users must reauthenticate each time they access NetStorage in a browser. This is true even if another browser window is open and authenticated on the same workstation.

The reason for this is that persistent cookies are not enabled by default.

This setting can be changed. For more information, see “[Persistent Cookies](#)” in the *OES 2: NetStorage for NetWare Administration Guide* and “[Persistent Cookies](#)” in the *OES 2 SP1: NetStorage for Linux Administration Guide*.

17.7.7 NetStorage Maintenance

Your NetStorage installation can change as your network changes and evolves by providing access to new or consolidated storage locations. For information about the kinds of tasks you can perform to keep your NetStorage implementation current, see the following:

- ♦ For Linux: *OES 2 SP1: NetStorage for Linux Administration Guide*
- ♦ For NetWare: *OES 2: NetStorage for NetWare Administration Guide*

17.8 Novell AFP Implementation and Maintenance

To use the Novell implementation of AFP file services on your OES 2 Linux server, you must install the service by using the instructions in the *OES 2 SP1: Linux Installation Guide* (for a new installation) or install it after the initial OES installation, as explained in “[Installing AFP after the OES 2 SP 1 Installation](#)” in the *OES 2 SP1: Novell AFP For Linux Administration Guide*.

- ♦ [Section 17.8.1, “Implementing Novell AFP File Services,” on page 218](#)
- ♦ [Section 17.8.2, “Maintaining Novell AFP File Services,” on page 218](#)

17.8.1 Implementing Novell AFP File Services

NOTE: If you are new to OES, we recommend the *OES2 SP2: Lab Guide for Linux and Virtualized NetWare* for an introduction to creating and working with eDirectory objects and OES 2 file services, including Novell AFP.

All eDirectory users can access the AFP file services on an OES 2 Linux server as they would any Macintosh server.

17.8.2 Maintaining Novell AFP File Services

Information on maintaining your AFP installation is found in the *OES 2 SP1: Novell AFP For Linux Administration Guide*.

17.9 Novell CIFS Implementation and Maintenance

To use the Novell implementation of CIFS file services on your OES 2 Linux server, you must install the service by using the instructions in the *OES 2 SP1: Linux Installation Guide* (for a new installation) or install it after the initial OES installation, as explained in “[Installing and Configuring a CIFS Server through YaST](#)” in the *OES 2 SP1: Novell CIFS for Linux Administration Guide*.

- ♦ [Section 17.9.1, “Implementing Novell CIFS File Services,” on page 219](#)
- ♦ [Section 17.9.2, “Maintaining Novell CIFS File Services,” on page 219](#)

17.9.1 Implementing Novell CIFS File Services

NOTE: If you are new to OES, we recommend the *OES2 SP2: Lab Guide for Linux and Virtualized NetWare* for an introduction to creating and working with eDirectory objects and OES 2 file services, including Novell CIFS.

All eDirectory users can access the CIFS file services on an OES 2 Linux server as they would any Windows workgroup server.

For instructions on implementing Novell CIFS, see “Planning and Implementing CIFS on OES 2 SP1 Linux” in the *OES 2 SP1: Novell CIFS for Linux Administration Guide*.

17.9.2 Maintaining Novell CIFS File Services

Information on maintaining your CIFS installation is found in the *OES 2 SP1: Novell CIFS for Linux Administration Guide*.

17.10 Novell iFolder 3.7 Implementation and Maintenance

The following implementation pointers are provided only as introductory information. To begin using Novell iFolder, see the *OES 2 SP1: Novell iFolder 3.7 Administration Guide*.

- Section 17.10.1, “Managing Novell iFolder 3.7,” on page 219
- Section 17.10.2, “Configuring Novell iFolder 3.7 Servers,” on page 219
- Section 17.10.3, “Creating and Enabling Novell iFolder 3.7 Users,” on page 219
- Section 17.10.4, “Novell iFolder 3.7 Maintenance,” on page 220

17.10.1 Managing Novell iFolder 3.7

You manage Novell iFolder through the iFolder Management Console, which you can access directly or through iManager. For more information, see “Accessing iManager and the Novell iFolder Web Admin” in the *OES 2 SP1: Novell iFolder 3.7 Administration Guide*.

17.10.2 Configuring Novell iFolder 3.7 Servers

Before you let users log in to the Novell iFolder 3.7 server, be sure you complete all the setup tasks in “Installing and Configuring iFolder Services” (including “Configuring the iFolder Web Admin Server” if applicable) in the *OES 2 SP1: Novell iFolder 3.7 Administration Guide*.

17.10.3 Creating and Enabling Novell iFolder 3.7 Users

To provide user access to Novell iFolder 3.7:

1. Provision eDirectory User objects for iFolder 3.7.
2. Enable the User Account Policies for iFolder access.
3. (Optional) Enable Account Quotas (space limits) for the user accounts.

4. Create iFolders for users.
5. Distribute the iFolder Client to users.

For more information, see “[Managing iFolder Users](#)” in the *OES 2 SP1: Novell iFolder 3.7 Administration Guide*.

17.10.4 Novell iFolder 3.7 Maintenance

As the Novell iFolder service load increases, you might need to increase the server capacity or add additional servers. For help, see “[Deploying iFolder Server](#)” in the *OES 2 SP1: Novell iFolder 3.7 Administration Guide*. For a list of other common iFolder maintenance topics, see [iFolder 3.7](#) in the OES 2 online documentation.

17.11 Samba Implementation and Maintenance

To use the Novell implementation of Samba file services on your OES 2 server, you must install the service by using the instructions in the *OES 2 SP1: Linux Installation Guide* (for a new installation) or install it after the initial OES installation, as explained in “[Installing Samba for OES 2](#)” in the *OES2 SP1: Samba Administration Guide*.

- ♦ [Section 17.11.1, “Implementing Samba File Services,”](#) on page 220
- ♦ [Section 17.11.2, “Maintaining Samba File Services,”](#) on page 220

17.11.1 Implementing Samba File Services

All users whose accounts have been enabled for Samba access can access the OES 2 server as they would any Windows server.

For instructions on implementing Samba, see “[Installing Samba for OES 2](#)” in the *OES2 SP1: Samba Administration Guide*.

17.11.2 Maintaining Samba File Services

Information on maintaining your Samba installation is found in the *OES2 SP1: Samba Administration Guide*.

Print Services

Open Enterprise Server 2 includes Novell® iPrint, a powerful and easy-to-implement printing solution that provides print-anywhere functionality to network users. iPrint lets Windows, Linux, and Macintosh users quickly locate network printers through a Web browser, easily install and configure a located printer through a native printer installation method, and print to installed printers from any location through an IP connection.

This section contains the following information:

- ♦ [Section 18.1, “Overview of Print Services,” on page 221](#)
- ♦ [Section 18.2, “Planning for Print Services,” on page 224](#)
- ♦ [Section 18.3, “Coexistence and Migration of Print Services,” on page 224](#)
- ♦ [Section 18.4, “Print Services Implementation Suggestions,” on page 224](#)
- ♦ [Section 18.5, “Print Services Maintenance Suggestions,” on page 226](#)

18.1 Overview of Print Services

Novell iPrint lets Linux, Macintosh, and Windows users

- ♦ Quickly locate network printers through a Web browser.
- ♦ Easily install and configure a located printer through a native printer installation method.
- ♦ Print to installed printers from any location (including the Web) through an IP connection.

The information in this section provides a high-level overview of Novell iPrint print services. It is designed to acquaint you with basic iPrint functionality so you understand the configuration steps you need to perform to provide iPrint print services, and understand how iPrint functions from the user’s perspective.

- ♦ [Section 18.1.1, “Using This Overview,” on page 221](#)
- ♦ [Section 18.1.2, “iPrint Components,” on page 222](#)
- ♦ [Section 18.1.3, “iPrint Functionality,” on page 222](#)

18.1.1 Using This Overview

If you already know that you want to provide OES print services for your users and you understand how iPrint works, skip the overviews and continue with [Section 18.2, “Planning for Print Services,” on page 224](#).

If you want to learn more about iPrint, continue with this overview section.

18.1.2 iPrint Components

A Novell iPrint installation consists of various components, most of which are represented by objects in your eDirectory™ tree:

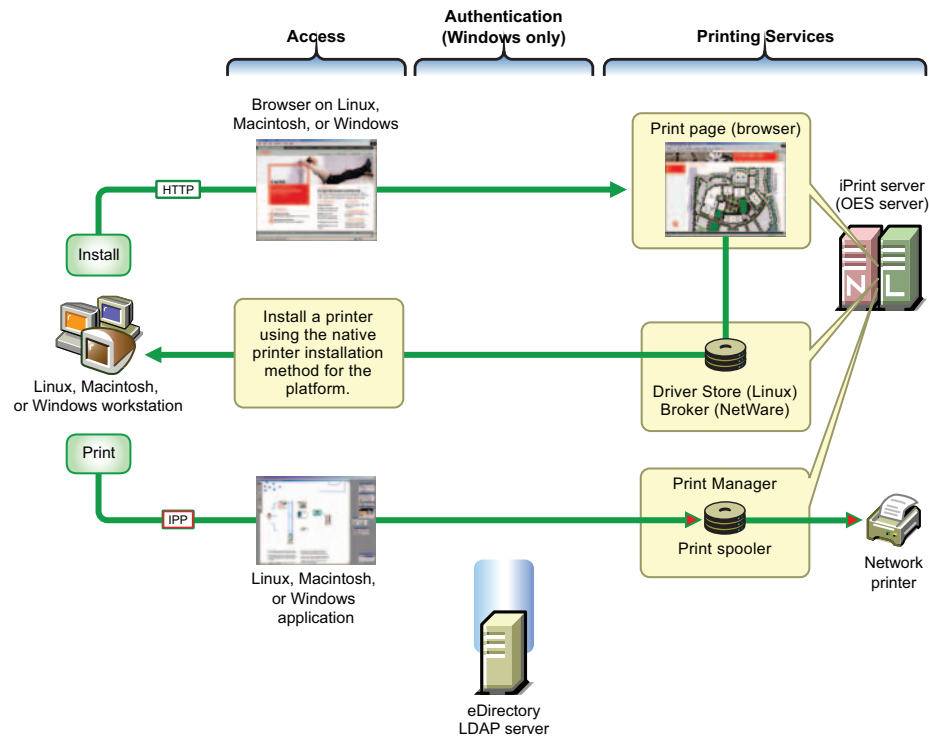
- ♦ **Print Driver Store (Linux):** This is a repository that stores the drivers on an OES 2 Linux server for your network printers. It is the first component you configure and is represented by an eDirectory object that you create.
- ♦ **Print Broker (NetWare):** This is a repository that stores the drivers on an OES 2 NetWare® server for your network printers. It is the first component you configure and is represented by an eDirectory object that you create.
- ♦ **Printer Drivers:** These are the platform-specific printer drivers and PostScript® Printer Description (PPD) files that are stored in the Driver Store or Broker and are installed on workstations when users select a target printer. Printer drivers and PPD files exist as file structures within the Driver Store and Broker and are not represented by objects in eDirectory.
- ♦ **Printer Objects:** These are eDirectory objects you create that store information about the printers available through iPrint. The information stored in an object is used each time its associated printer is added to a workstation's list of available printers.
- ♦ **Print Manager:** This is a daemon that runs on OES 2 Linux or an NLM™ that runs on the OES 2 NetWare server. It receives print jobs from users and forwards them to the target printer when it is ready. It is represented by and controlled through an eDirectory object that you can configure.
- ♦ **iPrint Client:** This is a set of browser plug-ins. On Macintosh and Windows workstations it is automatically installed the first time it interacts with iPrint. On Linux workstations, it must be installed manually. The client is required on each platform to navigate through the iPrint Web pages, select a target printer, and install the print driver.

For more information on iPrint, see “**Print Services**” in the OES online documentation.

18.1.3 iPrint Functionality

Figure 18-1 describes how iPrint functions from a user workstation perspective.

Figure 18-1 How iPrint Works



The following table explains the information illustrated in Figure 18-1.

Table 18-1 iPrint Functionality

Access	Authentication	Printing Services
The iPrint Client must be installed on each workstation accessing iPrint services.	You can require authentication for Windows users if needed. The option to require authentication is not available for Linux and Macintosh users.	Users with the iPrint Client installed and access to the OES 2 server can install printer drivers and print to iPrint printers.
A user needing to use a printer for the first time accesses the organization's print page on the Web.	Although shown separately, eDirectory could be installed on the OES 2 server.	By default, iPrint generates a printer list for the printers hosted on the server.
When the user selects the target printer, its platform-specific driver is automatically installed and configured.		A customized Web page lets users browse to the target printer by using location lists and maps that you have previously created for the site where the printer is located.
After printer installation, users can print to the printer from any application.		

18.2 Planning for Print Services

Consider the following information as you plan your iPrint installation:

- ♦ We recommend that you record your planning decisions on a planning worksheet for future reference.
- ♦ iPrint has no additional RAM requirements.
- ♦ Most iPrint installations (even in large enterprises) do not require additional disk space for associated print job spooling.

However, if you anticipate very heavy print usage and want to plan for additional disk space in that regard, the iPrint spooler area is located in the `/var` partition or directory structure on OES 2 Linux servers. On NetWare servers, you designate the location when creating the Print Manager object.

- ♦ To finish planning your iPrint installation, refer to the information for your server platform:
 - ♦ For NetWare: “**Novell iPrint Server**” in the *OES 2 SP1: NetWare Installation Guide*
 - ♦ For Linux: “**Novell iPrint**” in the *OES 2 SP1: Linux Installation Guide*

18.3 Coexistence and Migration of Print Services

If you select iPrint during the OES Linux server installation, the iPrint software components are automatically installed on the server. Although the Common UNIX Printing System (CUPS) software is also installed with SLES 10, CUPS is disabled to avoid port 631 conflicts.

For information on upgrading from NetWare queue-based printing, Novell Distributed Print Services™ (NDPS), or previous versions of iPrint, see “**Installing iPrint Software**” in the *OES 2 SP1: iPrint Administration Guide for NetWare*.

For more information on configuring iPrint on OES Linux, see “**Installing and Setting Up iPrint on Your Server**” in the *OES 2 SP1: iPrint for Linux Administration Guide*.

In OES SP2, migrating iPrint services from a NetWare server to an OES 2 Linux server is supported in Server Consolidation Utility 4.2, which is included in the Novell Server Consolidation and Migration Toolkit. For more information, see “**Migrating iPrint Printers and Print Managers from NetWare to Linux**” in the *Novell Server Consolidation and Migration Toolkit Administration Guide*.

18.4 Print Services Implementation Suggestions

This section provides only summary implementation information. For complete iPrint documentation, see the *OES 2 SP1: iPrint for Linux Administration Guide* and the *OES 2 SP1: iPrint Administration Guide for NetWare*.

- ♦ Section 18.4.1, “Initial Setup,” on page 225
- ♦ Section 18.4.2, “Implementation Caveats,” on page 226
- ♦ Section 18.4.3, “Other Implementation Tasks,” on page 226

18.4.1 Initial Setup

After your OES 2 server is installed, you must do the following to complete your iPrint installation:

- 1 Create a Driver Store on OES 2 Linux or a Broker on OES 2 NetWare to store the print drivers.

These eDirectory objects store the drivers for your network printers on Linux and NetWare servers, respectively. Each Printer object you create for your network needs to reference a printer driver in Driver Store/Broker. When users subsequently install printers, the correct drivers for the platform running on their workstation are downloaded from the Driver Store and installed.

You create the Driver Store through iManager. For specific instructions, see the following:

- ♦ For Linux: “**Creating a Driver Store**” in the *OES 2 SP1: iPrint for Linux Administration Guide*
- ♦ For NetWare: “**Creating a Broker**” in the *OES 2 SP1: iPrint Administration Guide for NetWare*

- 2 Add a printer driver to the Driver Store or Broker for each printer/platform combination needed.

For example, If you have Windows XP, Windows 2000, and Novell Linux Desktop (NLD) workstations on your network and you have four different printer types, you need to add four printer drivers for each platform (a total of 12 printer drivers) to the Driver Store or Broker.

You add printer drivers to the store through iManager. For specific instructions, see the following:

- ♦ For Linux: “**Updating Printer Drivers**” in the *OES 2 SP1: iPrint for Linux Administration Guide*
- ♦ For NetWare: “**Adding or Updating Printer Drivers**” in the *OES 2 SP1: iPrint Administration Guide for NetWare*

- 3 Create a Print Manager object.

The Print Manager receives print jobs from users and forwards them to the target printer when it is ready. The Print Manager must be running for you to create Printer objects.

The Print Manager is an object you create in eDirectory and is usually started and stopped through iManager.

You create the Print Manager object through iManager. For specific instructions, see the following:

- ♦ For Linux: “**Creating a Print Manager**” in the *OES 2 SP1: iPrint for Linux Administration Guide*
- ♦ For NetWare: “**Creating a Print Manager**” in the *OES 2 SP1: iPrint Administration Guide for NetWare*

- 4 Create Printer objects.

You must create a Printer object for each printer you want users to access through iPrint. These objects store information about the printer that is used each time the printer is installed on a workstation.

You create Printer objects through iManager. For specific instructions, see the following:

- ♦ For Linux: “**Creating a Printer**” in the *OES 2 SP1: iPrint for Linux Administration Guide*
- ♦ For NetWare: “**Creating a Printer**” in the *OES 2 SP1: iPrint Administration Guide for NetWare*

5 (Optional) Create location-based, customized printing Web pages.

By default, each iPrint installation includes the creation of a Default Printer List Web page that users can access to install iPrint printers.

You have the option of enhancing the browsing experience by creating location-based printing Web pages that feature either lists of printers by location, maps of the buildings showing each printer, or a combination of both.

If your organization is located at multiple sites or even in a building with multiple floors, providing location-based print Web pages can greatly simplify printing for your users.

Your iPrint installation contains the iPrint Map Designer to help you easily create location maps with clickable printer icons. For more information, see the following:

- ♦ For Linux: “[Setting Up Location-Based Printing](#)” in the *OES 2 SP1: iPrint for Linux Administration Guide*
- ♦ For NetWare: “[Setting Up Location-Based Printing](#)” in the *OES 2 SP1: iPrint Administration Guide for NetWare*

6 Provide instructions to users for accessing iPrint printers.

After performing the steps above, your network is ready for iPrint functionality. You need only tell users how to access your printing Web pages; Novell iPrint does the rest.

18.4.2 Implementation Caveats

There are a few implementation caveats relating to iPrint on Linux. See “[iPrint](#)” on page 68.

18.4.3 Other Implementation Tasks

In addition to the tasks described in [Section 18.4.1, “Initial Setup,”](#) on page 225, there are additional tasks you might want or need to consider. To see a list of potential tasks, refer to the “[Print Services](#)” links in the OES online documentation.

18.5 Print Services Maintenance Suggestions

As you add printers to your network or move them to different locations, be sure to update your iPrint installation to reflect these changes.

After your installation is completed and users are printing, you can monitor print performance by using the information located in the following locations:

- ♦ For Linux: “[Using the Print Manager Health Monitor](#)” in the *OES 2 SP1: iPrint for Linux Administration Guide*
- ♦ For NetWare: “[Using the Print Manager Health Monitor](#)” in the *OES 2 SP1: iPrint Administration Guide for NetWare*

For more information on iPrint and its functionality within OES, see the “[Print Services](#)” links in the online documentation.

Search Engine (QuickFinder)

Open Enterprise Server 2 includes the Novell® QuickFinder™ Server on both the NetWare® and Linux platforms. QuickFinder lets you add search and print functionality to any Web site or internal intranet. It can index and find matches within a wide variety of data types. It also supports rights-based searches so that users see only what they have rights to see, depending on the type of index created and the file system indexed.

QuickFinder replaces the NetWare Web Search Server that was available in NetWare 6.5 SP3 and earlier. When you upgrade a NetWare server running NetWare Web Search Server to OES NetWare (NetWare 6.5), Web Search Server is automatically upgraded to QuickFinder. The upgrade identifies all the configuration settings and indexes from Web Search and enables them to be used by QuickFinder.

When indexing a file system, the QuickFinder engine indexes only what it has rights to see. On NetWare, it has full access to all mounted volumes. On Linux, it has rights to only the files that the `wwwrun` user and the `www` group have rights to see.

For more information, see the topics in “[Search Engine](#)” in the OES 2 online documentation or refer to the *OES 2: Novell QuickFinder Server 5.0 Administration Guide*.

Web Services

The Web and application services in Open Enterprise Server 2 support the creation and deployment of Web sites and Web applications that leverage the widespread availability of Internet-based protocols and tools.

With the proper Web components in place, a server can host dynamic Web sites where the content changes according to selections made by the user. You can also run any of the hundreds of free Web applications that can be downloaded from the Internet. Web and application services make it easy to build your own dynamic Web content and create customized Web database applications.

See the topics in “[Web Services](#)” in the OES online documentation.

OES 2 also includes a Jakarta-Tomcat servlet container for both NetWare[®] and Linux, including Tomcat 4 for NetWare, a Tomcat 5 servlet container on NetWare (for compatibility with iManager 2.7), and Tomcat 5 for Linux. Tomcat is used to run basic Java servlet and JavaServer Pages* (JSP*) applications on either operating system platform.

Apache

Apache Web Server 2.0 is the most popular Web server on the Internet. For the most part, Apache functions the same on NetWare and Linux, although Apache for NetWare does include some additional functions to allow for directory-enabled administration.

For additional information, see the *Apache Web Server for NetWare Administration Guide for OES* and the [Apache.org Web site \(http://www.apache.org\)](http://www.apache.org).

Tomcat

OES 2 also includes a Jakarta-Tomcat servlet container for both NetWare and Linux, including Tomcat 4 for NetWare, a Tomcat 5 servlet container on NetWare (for compatibility with iManager 2.7), and Tomcat 5 for Linux. Tomcat is used to run basic Java servlet and JavaServer Pages (JSP) applications on either operating system platform.

For additional information, see the *Tomcat for NetWare Administration Guide for OES* and the [Apache Jakarta Tomcat 5.5 Web site \(http://tomcat.apache.org/tomcat-5.5-doc/index.html\)](http://tomcat.apache.org/tomcat-5.5-doc/index.html).

Security

This section contains the following topics:

- ♦ [Section 21.1, “Overview of OES Security Services,” on page 231](#)
- ♦ [Section 21.2, “Planning for Security,” on page 232](#)
- ♦ [Section 21.3, “Configuring and Administering Security,” on page 235](#)
- ♦ [Section 21.4, “Links to Product Security Considerations,” on page 235](#)

21.1 Overview of OES Security Services

This section provides specific overview information for the following key OES components:

- ♦ [Section 21.1.1, “Application Security \(AppArmor\),” on page 231](#)
- ♦ [Section 21.1.2, “Auditing,” on page 231](#)
- ♦ [Section 21.1.3, “Encryption \(NICI\),” on page 231](#)
- ♦ [Section 21.1.4, “General Security Issues,” on page 232](#)

For more authentication and security topics, see the [OES online documentation](#).

21.1.1 Application Security (AppArmor)

Novell® AppArmor® provides easy-to-use application security for both servers and workstations. You specify which files a program can read, write, and execute.

AppArmor enforces good application behavior without relying on attack signatures and prevents attacks even if they are exploiting previously unknown vulnerabilities.

For more information, see the [Novell AppArmor Documentation Web site \(http://www.novell.com/documentation/apparmor/index.html\)](http://www.novell.com/documentation/apparmor/index.html).

21.1.2 Auditing

OES 2 NetWare® includes Nsure™ Audit 1.0.3 Starter Pack, and the applicable documentation is included in the OES documentation set. For direct links to the documentation included with OES 2 NetWare, see the topics in “[auditing](#)” in the OES online documentation.

OES 2 Linux does not include an audit starter pack. However, the Novell Audit 2.0 Starter Pack is supported on OES 2 Linux and is available for download at no cost from the [Novell Download Site \(http://www.novell.com/downloads\)](http://www.novell.com/downloads). Documentation for Novell Audit 2.0 is available on the [Novell Documentation Web site \(http://www.novell.com/documentation/novellaudit20/treetitl.html\)](http://www.novell.com/documentation/novellaudit20/treetitl.html).

21.1.3 Encryption (NICI)

The Novell International Cryptography Infrastructure (NICI) is the cryptography service for Novell eDirectory™, Novell Modular Authentication Services (NMAS™), Novell Certificate Server™, Novell SecretStore®, and TLS/SSL.

Key Features

NICI includes the following key features:

- ♦ Industry standards: It implements the recognized industry standards.
- ♦ Certified: It is FIPS-140-1 certified on selected platforms.
- ♦ Cross-platform support: It is available on both OES platforms.
- ♦ Governmental export and import compliance: It has cryptographic interfaces that are exportable from the U.S. and importable into other countries with government-imposed constraints on the export, import, and use of products that contain embedded cryptographic mechanisms.
- ♦ Secure and tamper-resistant architecture: The architecture uses digital signatures to implement a self-verification process so that consuming services are assured that NICI has not been modified or tampered with when it is initialized.

Never Delete the NICI Configuration Files

In the early days of NICI development, some NICI problems could be solved only by deleting the NICI configuration files and starting over. The issues that required this were solved years ago, but as is often the case, the practice persists, and some administrators attempt to use this as a remedy when they encounter a NICI problem.

No one should ever delete the **NICI configuration files** unless they are directly told to do so by a member of the NICI development team. And in that rare case, they should be sure to **back up the files** before doing so. Failure to do this makes restoring NICI impossible.

More Information

For more information on how to use NICI, see the *Novell International Cryptographic Infrastructure (NICI) 2.7x Administration Guide*.

21.1.4 General Security Issues

In addition to the information explained and referenced in this section, the OES online documentation contains links to “General Security Issues” (<http://www.novell.com/documentation/oes2/security.html#b1349evx>).

21.2 Planning for Security

This section discusses the following topics. For additional planning topics, see the **Security section in the OES online documentation**.

- ♦ Section 21.2.1, “Comparing the Linux and the NetWare Core Protocol (NCP) File Security Models,” on page 233
- ♦ Section 21.2.2, “User Restrictions: Some OES 2 Linux Limitations,” on page 234

21.2.1 Comparing the Linux and the NetWare Core Protocol (NCP) File Security Models

The NetWare (NSS/NCP™) and Linux (POSIX) security models are quite different, as presented in [Table 21-1](#).

Table 21-1 *POSIX vs. NSS/NCP File Security Models*

Feature	POSIX / Linux	NSS/NCP on OES 2 Linux
Administrative principles	<p>Permissions are individually controlled and managed for each file and subdirectory.</p> <p>Because of the nature of the POSIX security model, users usually have read rights to most of the system.</p> <p>To make directories and files private, permissions must be removed.</p> <p>For more information on making existing directories private, see Section 17.4.2, “Providing a Private Work Directory,” on page 212.</p>	<p>Trustee assignments are made to directories and files and flow down from directories to everything below unless specifically reassigned.</p>
Default accessibility	<p>Users have permissions to see most of the file system.</p> <p>The contents of a few directories, such as the <code>/root</code> home directory, can only be viewed by the <code>root</code> user.</p> <p>Some system configuration files can be read by everyone, but the most critical files, such as <code>/etc/fstab</code>, can only be read and modified by <code>root</code>.</p>	<p>Users can see only the directories and files for which they are trustees (or members of a group that is a trustee).</p>
Home directories—an example of default accessibility	<p>By default, all users can see the names of directories and files in home directories.</p> <p>During LUM installation, you can specify that newly created home directories will be private.</p> <p>For more information on making existing home directories private, see Section 17.4.2, “Providing a Private Work Directory,” on page 212.</p>	<p>By default, only the system administrator and the home directory owner can see a home directory. Files in the directory are secure.</p> <p>If users want to share files with others, they can grant trustee assignments to the individual files, or they can create a shared subdirectory and assign trustees to it.</p>
Inheritance from parents	<p>Nothing is inherited.</p> <p>Granting permission to a directory or file affects only the directory or file.</p>	<p>Rights are inherited in all child subdirectories and files unless specifically reassigned.</p> <p>A trustee assignment can potentially give a user rights to a large number of subdirectories and files.</p>

Feature	POSIX / Linux	NSS/NCP on OES 2 Linux
Privacy	Because users have permissions to see most of the file system for reasons stated above, most directories and files are only private when you make them private.	Directories and files are private by default.
Subdirectory and file visibility	<p>Permissions granted to a file or directory apply to only the file or directory. Users can't see parent directories along the path up to the root unless permissions are granted (by setting the UID, GID, and mode bits) for each parent.</p> <p>After permissions are granted, users can see the entire contents (subdirectories and files) of each directory in the path.</p>	When users are given a trustee assignment to a file or directory, they can automatically see each parent directory along the path up to the root. However, users can't see the contents of those directories, just the path to where they have rights.

When an NCP volume is created on a Linux POSIX or NSS volume, some of the behavior described above is modified. For more information, see the *OES 2 SP1: NCP Server for Linux Administration Guide*, particularly the “NCP on Linux Security” section.

21.2.2 User Restrictions: Some OES 2 Linux Limitations

Seasoned NetWare administrators are accustomed to being able to set the following access restrictions on users:

- ♦ Account balance restrictions
- ♦ Address restrictions
- ♦ Intruder lockout
- ♦ Login restrictions
- ♦ Password restrictions
- ♦ Time restrictions

Many of the management interfaces that set these restrictions (iManager, for example), might seem to imply that these restrictions apply to users who are accessing an OES 2 server through any protocol.

This is generally true, with two important exceptions:

- ♦ Maximum number of concurrent connections in login restrictions
- ♦ Address restrictions

These two specific restrictions are enforced only for users who are accessing the server through NCP. Connections through other access protocols (for example, HTTP or CIFS) have no concurrent connection or address restrictions imposed.

For this reason, you probably want to consider not enabling services such as SSH and FTP for LUM when setting up Linux User Management. For more information on SSH and LUM, see [Section 11.4, “SSH Services on OES 2 Linux,” on page 100](#).

For more information on Linux User Management, see “[Linux User Management: Access to Linux for eDirectory Users](#)” on page 157. For more information on the services that can be PAM-enabled, see [Table 15-2](#) on page 160.

21.3 Configuring and Administering Security

For a list of configuration and administration topics, see the [Security section in the OES online documentation](#).

21.4 Links to Product Security Considerations

The following product documentation contains additional security information:

Table 21-2 *Security Consideration Links*

Product/Technology	Security Considerations Section Link
Archive and Version Services	<p>“Security Considerations for Archive and Version Services” in the <i>OES 2: Novell Archive and Version Services 2.1 for NetWare Administration Guide</i></p> <p>“Security Considerations for Archive and Version Services” in the <i>OES 2 SP1: Novell Archive and Version Services 2.1 for Linux Administration Guide</i></p>
Dynamic Storage Technology	“ Security Considerations ” in the <i>OES 2 SP1: Dynamic Storage Technology Administration Guide</i>
eDirectory	“ Security Considerations ” in the <i>Novell eDirectory 8.8 Administration Guide</i>
File Systems	<i>OES 2 SP1: File Systems Management Guide</i> (information throughout the guide)
Identity Manager 3.5	“ Security Best Practices (http://www.novell.com/documentation/idm36/idm_security/data/front.html) ” in the <i>Identity Manager 3.6 Documentation (http://www.novell.com/documentation/caribou/index.html)</i>
iPrint for OES 2 Linux	“ Setting Up a Secure Printing Environment ” in the <i>OES 2 SP1: iPrint for Linux Administration Guide</i>
iPrint for OES 2 NetWare	“ Setting Up a Secure Printing Environment ” in the <i>OES 2 SP1: iPrint Administration Guide for NetWare</i>
iSCSI for OES 2 NetWare	Enabling and Configuring iSCSI Initiator Security in the <i>OES 2 SP 1: iSCSI 1.1.3 for NetWare Administration Guide</i>
Linux User Management	“ Security Considerations ” in the <i>OES 2 SP1: Novell Linux User Management Technology Guide</i>
Native File Access Protocols	“ Enabling and Disabling SMB Signing ” in the <i>OES 2 SP1: AFP, CIFS, and NFS for NetWare (NFAP) Administration Guide</i> .

Product/Technology	Security Considerations Section Link
Novell AFP	“Security Guidelines for AFP” in the <i>OES 2 SP1: Novell AFP For Linux Administration Guide</i> Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide
Novell CIFS	“Security Considerations for CIFS on OES 2 Linux” in the <i>OES 2 SP1: Novell CIFS for Linux Administration Guide</i>.
Novell Client™ for Windows	“Managing File Security and Passwords” in the <i>Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide</i>
Novell Client for Linux	“Managing File Security” in the <i>Novell Client 2.0 SP1 for Linux Administration Guide</i>
Novell Remote Manager for OES 2 Linux	“Security Considerations” in the <i>OES 2 SP1: Novell Remote Manager for Linux Administration Guide</i>
Novell Remote Manager for OES 2 NetWare	“Security Considerations” in the <i>OES 2 SP1: Novell Remote Manager for NetWare Administration Guide</i>
Novell Storage Services	“Securing Access to NSS Volumes, Directories, and Files” and “Security Considerations” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Novell iFolder® 3.7	OES 2 SP1 Linux: Novell iFolder 3.7 Security Administration Guide
OES 2 Linux Installation	“Security Considerations” in the <i>OES 2 SP1: Linux Installation Guide</i>
OES 2 Migration Tools	“Security Considerations for Data Migration” in the <i>OES 2 SP1: Migration Tool Administration Guide</i>
OpenWBEM	“Ensuring Secure Access” in the <i>OES 2 SP1: OpenWBEM Services Administration Guide</i>
QuickFinder™	“Security Considerations for QuickFinder Server” in the <i>QuickFinder Server 4.0 Administration Guide</i>
Server Consolidation and Migration Toolkit	“Security Considerations” in the <i>Novell Server Consolidation and Migration Toolkit Administration Guide</i>

Certificate Management

By default, all SUSE® Linux Enterprise Server (SLES) 10 servers include self-generated server certificates to secure data communications with the servers. These certificates are self-signed and do not comply with the X.509 RFCs. They are provided only as a stop-gap and should be replaced as soon as possible by a certificate from a trusted Certificate Authority.

Unfortunately, many organizations ignore the vulnerabilities to mischievous or even malicious attacks that are created by not replacing these temporary certificates. Some of the reasons for this are

- ♦ Many administrators lack the knowledge required.
- ♦ Certificate maintenance can require a significant investment of time and effort.
- ♦ Obtaining third-party certificates for each server is expensive.

The problems are compounded by the fact that X.509 certificates are designed to expire regularly and should be replaced shortly before they do.

Open Enterprise Server 2 includes solutions that address each of these issues at no additional expense.

This section discusses the certificate management enhancements available in OES 2 and how simple and straightforward it is to take advantage of these.

- ♦ [Section 22.1, “Overview,” on page 237](#)
- ♦ [Section 22.2, “Setting Up Certificate Management,” on page 240](#)
- ♦ [Section 22.3, “If You Don’t Want to Use eDirectory Certificates,” on page 242](#)

22.1 Overview

The following sections outline how OES 2 lets you automate certificate management for OES 2 and all HTTPS services:

- ♦ [Section 22.1.1, “SLES Default Certificates,” on page 237](#)
- ♦ [Section 22.1.2, “OES 2 Certificate Management,” on page 238](#)
- ♦ [Section 22.1.3, “Multiple Trees Sharing a Common Root,” on page 240](#)

22.1.1 SLES Default Certificates

By default, HTTPS services on SLES 10 SP1 are configured to use two files that are located in `/etc/ssl/servercerts` and are protected so that only `root` and some specific groups can read them:

- ♦ **serverkey.pem:** This contains the server’s raw private key.
- ♦ **servercert.pem:** This contains the server’s certificates.

OES 2 services, such as Apache, OpenWBEM, and Novell Remote Manager, are also configured to use these certificates.

22.1.2 OES 2 Certificate Management

OES 2 enhances certificate management as follows:

- ♦ “Installation of eDirectory Certificates” on page 238
- ♦ “What Is Installed Where” on page 238
- ♦ “Novell Certificate Server” on page 239
- ♦ “Server Self-Provisioning” on page 239
- ♦ “PKI Health Check” on page 239

Installation of eDirectory Certificates

As you install eDirectory™ and OES 2, by default all HTTPS services are configured to use eDirectory certificates. This means that eDirectory is established as the Certificate Authority for the tree you are installing into, and it will generate keys and certificates for the server and replace the installed SLES certificates with the eDirectory certificates.

What Is Installed Where

Key and certificate files are installed in the following locations:

Table 22-1 *File Locations*

Location	Details
<code>/etc/ssl/certs</code>	<p>This is the default location of trusted root certificates for clients on the server.</p> <p>Most of the applications on the server are configured to use this directory. For example, the LDAP client uses one or more of the trusted certificates in this directory when establishing a secure LDAP connection.</p> <p>The OES 2 installation copies the eDirectory tree CA's certificate (<code>eDirCACert.pem</code>) here, thereby establishing the CA as a trusted root.</p> <p>Everyone (other) has rights to read the contents of this directory.</p>
<code>/etc/ssl/servercerts</code>	<p>The standard location for the server's raw private key (<code>serverkey.pem</code>) and certificates (<code>servercert.pem</code>).</p> <p>Applications on the server, including OES 2 applications, are configured to point to the files in this directory.</p> <p>Only <code>root</code> and some specific groups can read the files in this directory.</p>

Location	Details
/etc/opt/novell/certs	<p>This directory contains the eDirectory CA certificate in both DER and PEM formats for use by applications that need them. The files are named <code>SSCert.der</code> and <code>SSCert.pem</code>, respectively.</p> <p>For example, when PKI Health Check runs, it installs the CA certificate in the Java Keystore in DER format if the certificate needs replacing.</p>

Novell Certificate Server

The component that generates eDirectory keys and certificates is the Novell Certificate Server™.

This certificate server provides public key cryptography services that are natively integrated into Novell eDirectory. You use the server to can mint, issue, and manage both user and server certificates to protect confidential data transmissions over public communications channels such as the Internet.

For complete information on the Novell Certificate Server, see the *Novell Certificate Server 3.3.1 Administration Guide*.

Server Self-Provisioning

When activated, Server Self-Provisioning lets server objects in eDirectory create their own certificates. You must activate this option if you want PKI Health Check to automatically maintain your server certificates.

For more information on this feature, see “X.509 Certificate Self-Provisioning” in the *Novell Certificate Server 3.3.1 Administration Guide*.

PKI Health Check

The PKI health check runs whenever the certificate server starts.

If you have enabled Server Self-Provisioning, the health check routine automatically replaces server certificates when any of the following are detected:

- ♦ The certificates don't exist.
- ♦ The certificates have expired.
- ♦ The certificates are about to expire.
- ♦ The IP or DNS information on the certificates doesn't match the server configuration.
- ♦ The Certificate Authority (CA) that issued the certificate is different from the CA currently configured.

For more information on this feature, see “PKI Health Check” in the *Novell Certificate Server 3.3.1 Administration Guide*.

22.1.3 Multiple Trees Sharing a Common Root

The Organizational CA can be configured to act as a sub-CA. This lets multiple trees share a common root certificate. The root certificate can be stored in a physically protected tree. It can also integrate with a third-party PKI. For more information, see “[Subordinate Certificate Authority](#)” in the *Novell Certificate Server 3.3.1 Administration Guide*.

22.2 Setting Up Certificate Management

Use the information in the following sections to help you set up certificate management as you install OES 2.

- ♦ [Section 22.2.1, “Setting Up Automatic Certificate Maintenance,” on page 240](#)
- ♦ [Section 22.2.2, “Eliminating Browser Certificate Errors,” on page 240](#)

22.2.1 Setting Up Automatic Certificate Maintenance

To set up your server so that HTTPS services use eDirectory certificates, you must specify the *Use eDirectory Certificates for HTTP Services* option while installing or upgrading eDirectory.

This installs eDirectory keys and certificates on the server, but it does not configure the server to automatically replace the certificates when they expire. Automatic maintenance requires that Server Self-Provisioning be enabled as follows:

- 1 On the server you are configuring, in iManager > Roles and Tasks, click the *Novell Certificate Access > Configure Certificate Authority* option.
- 2 Click *Enable server self-provisioning*.

This causes automatic certificate replacement for the conditions described in “[PKI Health Check](#)” on page 239.

IMPORTANT: If you enable Server Self-Provisioning in an OES 2 tree and you have created a CRL configuration object but not yet configured any CRL distribution points, the PKI Health Check might replace the default certificates every time it runs.

To avoid this, you can either

- ♦ Finish configuring the CA's CRL capability by creating one or more CRL Distribution Points by using iManager's *Configure Certificate Authority* task.
 - or
 - ♦ Delete any CRL Configuration objects, for example CN=One - Configuration.CN=CRL Container.CN=Security.
-

- 3 If you also want the CA certificate to be replaced if it changes or expires, click the *Health Check - Force default certificate creation/update on CA change* option.

22.2.2 Eliminating Browser Certificate Errors

Because the Internet Explorer and Mozilla Firefox* browsers don't trust eDirectory certificate authorities by default, attempts to establish a secure connection with OES 2 servers often generate certificate errors or warnings.

These are eliminated by importing the eDirectory tree CA's self-signed certificate into the browsers.

Complete the instructions in the following sections as applicable to your network.

- ♦ “Exporting the CA’s Self-Signed Certificate” on page 241
- ♦ “Importing the CA Certificate into Mozilla Firefox on Linux” on page 241
- ♦ “Importing the CA Certificate into Mozilla Firefox on Windows” on page 241
- ♦ “Importing the CA Certificate into Internet Explorer 6 and 7 on Windows” on page 242

Exporting the CA’s Self-Signed Certificate

- 1 Launch Novell iManager.
- 2 Log into the eDirectory tree as the Admin user.
- 3 Select the *Roles and Tasks* menu, then click *Novell Certificate Server > Configure Certificate Authority*.
- 4 Click the *Certificates* tab, then select the self-signed certificate.
- 5 Click *Export*.
- 6 Deselect *Export Private Key*.
The *Export Format* changes to DER.
- 7 Click *Next*.
- 8 Click *Save the Exported Certificate* and save the file to the local disk, noting the filename and location if they are indicated.
- 9 Click *Close > OK*.
- 10 Find the file you just saved. By default it is usually on the desktop.
- 11 Complete the instructions in the follow sections that apply to your browsers.

Importing the CA Certificate into Mozilla Firefox on Linux

- 1 Launch Firefox.
- 2 Click *Edit > Preferences > Advanced*.
- 3 Select the *Encryption* tab.
- 4 Click *View Certificates*.
- 5 Select the *Authorities* tab, then click *Import*.
- 6 Browse to the certificate file you downloaded in “Exporting the CA’s Self-Signed Certificate” on page 241 and click *Open*.
- 7 Select *Trust this CA to identify Web sites*, then click *OK > OK > Close*.
Firefox now trusts certificates from the servers in the tree.

Importing the CA Certificate into Mozilla Firefox on Windows

- 1 Launch Firefox.
- 2 Click *Tools > Options > Advanced*.
- 3 Select the *Security* tab.
- 4 Click *View Certificates*.
- 5 Select the *Authorities* tab, then click *Import*.

- 6 Browse to the certificate file you downloaded in “Exporting the CA’s Self-Signed Certificate” on page 241 and click *Open*.
- 7 Select *Trust this CA to identify Web sites*, then click *OK > OK > OK*.
Firefox now trusts certificates from the servers in the tree.

Importing the CA Certificate into Internet Explorer 6 and 7 on Windows

- 1 Launch Internet Explorer.
- 2 Click *Tools > Internet Options*.
- 3 Select the *Content* tab.
- 4 Click *Certificates*.
- 5 Click *Import*.
The Certificate Import Wizard launches.
- 6 Click *Next*.
- 7 Click *Browse*,
- 8 In the *Files of Type* drop-down list, select *All Files(*.*)*, browse to the file you downloaded in “Exporting the CA’s Self-Signed Certificate” on page 241, then click *Open*.
- 9 Click *Next*.
- 10 Click *Next*.
Choose the default, *Automatically select the certificate store based on the type of certificate*.
- 11 Click *Finish > Yes > OK*.
Internet Explorer now trusts certificates from the servers in the tree.

22.3 If You Don’t Want to Use eDirectory Certificates

For most organizations, the eDirectory certificate solution in OES 2 is an ideal way to eliminate the security vulnerabilities mentioned at the beginning of this chapter. However, some administrators, such as those who have third-party keys installed on their servers, probably want to keep their installed certificates in place.

You can prevent the use of eDirectory certificates for HTTPS services by making sure that the option to use them is not selected on the first eDirectory configuration page. This might or might not require that you change the eDirectory installation option, depending on your scenario.

Table 22-2 outlines the default setting for each scenario.

Table 22-2 Default eDirectory Certificate for HTTPS Settings

Scenario	Certificate Option Setting	Default Result	If you Change the Default Setting
New install	Selected	All HTTPS services on the server are configured to use eDirectory certificates.	All HTTPS services on the server are configured to use the YaST-generated temporary certificates.

Scenario	Certificate Option Setting	Default Result	If you Change the Default Setting
Add-on to SLES 10 or post-install	Selected	All HTTPS services on the server are configured to use eDirectory certificates.	The current service certificates and configurations are retained.
Upgrade from OES 1	Selected	All HTTPS services are configured to use eDirectory certificates.	The current service certificates and configurations are retained.
Upgrade from OES 2	The same option is used as when OES 2 was installed	HTTPS service settings are retained.	No effect. Once the option to use eDirectory certificates has been used, the behavior can only be changed in eDirectory through iManager.

A

Adding Services to OES 2 Servers

You can add services to Open Enterprise Server 2 servers after they are installed.

OES 2 Linux

OES 2 Linux is a set of services that can be either added to an existing server or installed at the same time as SUSE[®] Linux Enterprise Server 10 SP1. After OES 2 services are added, we refer to the server as an OES 2 Linux server.

To add OES 2 Linux services to an OES 2 Linux server, follow the instructions in “[Installing or Configuring OES 2 Services on an Existing OES 2 SP1 Linux or SLES 10 SP2 Server](#)” in the *OES 2 SP1: Linux Installation Guide*.

OES 2 NetWare

Some products, such as Novell[®] Cluster Services[™], can be installed only after completing the server installation.

You can install additional products by using Novell Deployment Manager (remotely) or from the GUI server console page (locally). For more information, see “[Installing Additional Products](#)” in the *OES 2 SP1: NetWare Installation Guide*.

Changing an OES 2 Linux Server's IP Address

The instructions in this section let you change the IP address assigned to an Open Enterprise Server 2 or OES 2 SP1 Linux server and the services it hosts.

- ♦ [Section B.1, “Caveats and Disclaimers,” on page 247](#)
- ♦ [Section B.2, “Prerequisites,” on page 247](#)
- ♦ [Section B.3, “Changing the Server’s Address Configuration,” on page 248](#)
- ♦ [Section B.4, “Reconfiguring the OES Services,” on page 248](#)
- ♦ [Section B.5, “Repairing the eDirectory Certificates,” on page 249](#)
- ♦ [Section B.6, “Completing the Server Reconfiguration,” on page 249](#)
- ♦ [Section B.7, “Modifying a Cluster,” on page 251](#)
- ♦ [Section B.8, “Reconfiguring Services on Other Servers That Point to This Server,” on page 251](#)

B.1 Caveats and Disclaimers

The instructions in this section assume that only the IP address of the server is changing. They do not cover changing the DNS hostname of the server.

B.2 Prerequisites

- ♦ [Section B.2.1, “General,” on page 247](#)
- ♦ [Section B.2.2, “iPrint,” on page 248](#)
- ♦ [Section B.2.3, “Clustering,” on page 248](#)

B.2.1 General

Before starting the process, be sure you know the following:

- ❑ **Old IP Address:** The server’s IP address you are changing.
- ❑ **New IP Address:** The IP address the server will use after the change.
- ❑ **Old Master Server Address:** The IP address of the eDirectory™ server specified when the server was installed.
By default this is also the LDAP server address for OES services installed on the server.
- ❑ **New Master Server Address:** The IP address of the eDirectory server that the server should point to after the change. The old and new addresses might be the same, but you will be required to enter both.
- ❑ **Address of the Subnet for the New IP Address:** This is a subnet address, not the subnet mask. For example, 192.168.2.0, not 255.255.255.0.

B.2.2 iPrint

If your network users connect to their printers through the print manager on this server, you might want to consider setting up iPrint Client Management (ICM) prior to the change. ICM lets you centrally configure the iPrint configuration for your users. For more information, see “[Using iPrint Client Management](#)” in the *OES 2 SP1: iPrint for Linux Administration Guide*.

B.2.3 Clustering

If the server is running Novell Cluster Services:

- 1 Check your plans against the prerequisites for clusters in “[Configuration Requirements](#)” in the *OES 2 SP1: Novell Cluster Services 1.8.6 for Linux Administration Guide*.
- 2 Follow the instructions in “[Changing the IP Addresses of Cluster Resources](#)” in the same guide.

B.3 Changing the Server’s Address Configuration

- 1 Log into the server you are reconfiguring as the `root` user.
- 2 Download and save the `ipchangespl.sh` script file (<http://www.novell.com/documentation/oes2/scripts/ipchangespl.sh>) to the `root (/)` partition of the server you are reconfiguring.
The same script file works on both OES 2 and OES 2 SP1 servers.
- 3 Open the YaST Control Center.
- 4 In *Network Devices* select *Network Card*.
- 5 Confirm that the Old IP address you listed in [Section B.2.1, “General,” on page 247](#) is in fact the IP address currently configured for the network card. You need this later in the process.
- 6 Using the various dialog boxes associated with the network card configuration, change the card configuration to the new IP address settings you listed in [Section B.2.1, “General,” on page 247](#), changing each of the following as necessary:
 - ♦ IP Address
 - ♦ Subnet Mask
 - ♦ Router (Gateway)
- 7 Close YaST, then continue with [Section B.4, “Reconfiguring the OES Services,” on page 248](#).

B.4 Reconfiguring the OES Services

- 1 Open a terminal prompt.
- 2 At the terminal prompt, change to the root (`/`) directory, make the script executable, then run the script by entering the following commands:

```
cd /
chmod 744 ipchangespl.sh
./ipchangespl.sh oldip newip oldmasterip newmasterip
```

where *oldip* is the old IP address, *newip* is the new IP address, *oldmasterip* is the IP address of the eDirectory server specified when the server was installed, and *newmasterip* is the IP address of the new eDirectory server identified in **Prerequisites** above.

The *oldmasterip* and the *newmasterip* can be the same IP address, but they must both be included in the command.

IMPORTANT: By default, the master eDirectory address is also the LDAP server address for OES services installed on the server.

All services that are configured with the old master address as their LDAP address are reconfigured to use the new master address. On the other hand, if you specified a different LDAP server address for any of the installed services, and if that LDAP server's address is also changing, you need to manually reconfigure the services .

To see the IP addresses that your services were originally configured to use, use a text editor to open the files in `/etc/sysconfig/novell/`.

As the script runs, it changes all of the OES configuration files and does everything else that can be done automatically to change the IP address for all OES services.

- 3 Type the Admin password when prompted.

You might need to wait a few minutes for the LDAP server to restart.

- 4 When the script finishes, restart the server by entering the following command at the terminal prompt:

```
shutdown -r now
```

B.5 Repairing the eDirectory Certificates

- 1 Start iManager and click through the warnings about a DNS name mismatch.
- 2 In the Login dialog box, type the Admin username and password, type the *newmasterip* address in the *Tree* field, then click *Login*.
- 3 Click *Novell Certificate Server > Repair Default Certificates*.
- 4 In *Create Server Certificate > Step 1 of 3*, browse to and select the server object for the server you are changing.
- 5 Click *OK > Next*.
- 6 In *Step 2 of 3*, click *Next*.
- 7 Click *Finish*, then close the dialog box.

B.6 Completing the Server Reconfiguration

Some OES services require reconfiguration steps to be done manually.

Complete the steps in the following sections as they apply to the server you are changing.

- ♦ [Section B.6.1, “QuickFinder,” on page 250](#)
- ♦ [Section B.6.2, “DHCP,” on page 250](#)
- ♦ [Section B.6.3, “iPrint,” on page 250](#)
- ♦ [Section B.6.4, “NetStorage,” on page 250](#)

B.6.1 QuickFinder

- 1 If the IP address you have changed is listed as an alias for the virtual search server, modify the list by deleting the entry for the old address and adding an entry for the new one.

For instructions, see “[Deleting a Virtual Search Server](#)” and “[Creating a Virtual Search Server](#)” in the *OES 2: Novell QuickFinder Server 5.0 Administration Guide*.

- 2 Regenerate the QuickFinder™ index by completing the instructions in see “[Creating Indexes](#)” in the *OES 2: Novell QuickFinder Server 5.0 Administration Guide*.

B.6.2 DHCP

- 1 Make sure the DHCP configuration in eDirectory has a subnet declared for the new IP address.

For instructions, see “[Administering and Managing DHCP](#)” in the *OES 2 SP1: Novell DNS/DHCP Administration Guide for Linux*.

B.6.3 iPrint

- 1 Using your favorite text editor, open the following configuration file:

```
/etc/opt/novell/iprint/conf/DN_of_PSMipsmd.conf.
```

where *DN_of_PSM* is the name of the Print Manager in eDirectory.

- 2 Change any entries that list the old IP address to the new IP address.
- 3 Restart the Print Manager by entering the following command at a terminal prompt:

```
rcnovell-ipsmd restart
```

IMPORTANT: Users that have accessed printers through the modified Print Manager will lose access to their printers.

If you have set up iPrint Client Management on the server, you can automate the reconfiguration process. If not, users must reinstall the printers.

For more information on iPrint Client Management, see “[Using iPrint Client Management](#)” in the *OES 2 SP1: iPrint for Linux Administration Guide*.

B.6.4 NetStorage

- 1 At a terminal prompt, enter the following commands:

```
/opt/novell/xtier/bin/xsrvcfg -D
```

```
/opt/novell/xtier/bin/xsrvcfg -d newip -c AuthenticationContext
```

where *newip* is the new IP address used throughout this section and *AuthenticationContext* is the eDirectory context for NetStorage users. NetStorage searches the eDirectory tree down from this container. If you want NetStorage to search the entire eDirectory tree, specify the root context.

```
rcnovell-xregd restart
```

```
rcnovell-xsrzd restart
```

```
rcapache2 restart
```

B.7 Modifying a Cluster

If the server is running Novell Cluster Services™, complete the instructions in “**Modifying the Cluster Configuration Information**” in the the *OES 2 SP1: Novell Cluster Services 1.8.6 for Linux Administration Guide*.

B.8 Reconfiguring Services on Other Servers That Point to This Server

If you have services on other servers that point to the old IP address for this server, be sure to reconfigure those services to point to the new IP address.

C

Updating/Patching OES 2 Servers

One of a network administrator's biggest challenges is keeping installed software up-to-date on all servers and workstations.

Patching OES 2 Linux

You can install product updates as they are made available through the ZENworks® Linux Management update channel. For instructions on setting up the ZENworks Linux Management update channel for each OES 2 Linux server and running the patch process, see “**Updating (Patching) an OES 2 SP1 Linux Server**” in the *OES 2 SP1: Linux Installation Guide*.

Patching OES 2 NetWare

For best reliability and performance, you should download and install the latest product updates available at the [Novell® Downloads site \(http://download.novell.com\)](http://download.novell.com).

Backup Services

The following sections briefly outline the backup services available in Open Enterprise Server 2. For more information, see the topics listed under “**Backup**” in the OES 2 online documentation.

- ♦ [Section D.1, “Services for End Users,” on page 255](#)
- ♦ [Section D.2, “System-Wide Services,” on page 255](#)

D.1 Services for End Users

OES 2 offers a number of services to automatically back up your network users’ data files.

- ♦ **Archive and Version Services:** If you implement Archive and Version Services on your network, your users can instantly restore any previous version of a modified, renamed, or deleted network file on an NSS volume without requiring assistance from the IT staff.
- ♦ **iFolder 3.7:** By implementing Novell® iFolder® 3.7, you empower your users to have their local files automatically follow them everywhere—online, offline, all the time—across computers. Users can share files in multiple iFolders, and share each iFolder with a different group of users. Users control who can participate in an iFolder and their access rights to the files in it. Users can also participate in iFolders that others share with them.
- ♦ **Salvage and Purge:** By default, all NSS volumes have the Salvage system enabled at the time they are created. With Salvage enabled, deleted files are retained on the volume for a short time, during which users can restore (salvage) them. File are eventually purged from the system, either manually, or by the system when the Purge Delay setting times out or space is needed on the volume.

D.2 System-Wide Services

OES 2 offers both Novell Storage Management Services™ and services that are available as part of the SUSE® Linux Enterprise Server 10 distribution.

- ♦ [Section D.2.1, “Novell Storage Management Services \(SMS\),” on page 255](#)
- ♦ [Section D.2.2, “SLES 10 Backup Services,” on page 256](#)

D.2.1 Novell Storage Management Services (SMS)

- ♦ [“Understanding SMS” on page 255](#)
- ♦ [“SMS Coexistence and Migration Issues” on page 256](#)

Understanding SMS

Novell Storage Management Services (SMS) is not a backup application. Rather, it provides a standard framework and the necessary interfaces that can be used in developing a complete backup/restore solution. SMS helps back up file systems (such as NSS) on OES 2 NetWare® and OES 2 Linux servers to removable tape media or other media for offsite storage.

SMS is implemented as two independent components that provide functional abstractions:

- ♦ **Storage Management Data Requestor (SMDR)** defines the API framework, provides remote connectivity, and abstracts the details of communication between servers.
- ♦ **Target Service Agent (TSA)** provides an implementation of SMS APIs for a particular target. The TSA provides transparency by abstracting details of the specific service being backed up.

For example, various applications use the file system TSA to back up and restore NSS file system data and metadata (trustee assignments, file attributes, and name spaces).

SMS Coexistence and Migration Issues

In OES 2, the SMS API framework is available on SLES 10 so that there is a single consistent interface to back up file systems on NetWare, file systems on Linux, and Novell applications such as GroupWise® and Novell iFolder. The API set has been enhanced to include new functionality for OES.

Most of the SMS coexistence and migration issues are of concern only to backup application developers. However, administrators should be aware that SMS-based applications must be used to back up and restore NSS file system data on OES Linux servers. Although NSS is exposed as a Virtual File System-compliant file system, the Linux interfaces are inadequate to back up NSS file system attributes, rich ACLs, trustees, and multiple data streams.

For additional information, see “**Coexistence and Migration Issues**” in the *OES 2 SP1: Storage Management Services Administration Guide*.

D.2.2 SLES 10 Backup Services

Two SLES 10 services might be of interest.

- ♦ **DRDB:** This lets you to create a mirror of two block devices at two different sites across an IP network. When used with HeartBeat 2 (HB2), DRBD supports distributed high-availability Linux clusters. For more information, see “**Installing and Managing DRBD Services**” (http://www.novell.com/documentation/sles10/stor_evms/data/drdb.html) in the *SLES 10 SP2: Storage Administration Guide* (http://www.novell.com/documentation/sles10/stor_evms/data/bookinfo.html).
- ♦ **rsync:** This is useful when large amounts of data need to be backed up regularly or moved to another server, such as from a staging server to a Web server in a DMZ. For more information, see “**Introduction to rsync**” (http://www.novell.com/documentation/sles10/sles_admin/data/sec_net_sync_rsync.html) in the *SLES 10 SP2: Installation and Administration Guide* (http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html).



Quick Reference to OES 2 User Services

Use [Table E-1](#) as a quick reference for providing your network users with instructions for accessing each Novell® Open Enterprise Server 2 service.

Table E-1 OES User Services Quick Reference

services	Access Method or URL	Notes
iPrint	http://server_ip_address_or_dns_name/ipp https://server_ip_address_or_dns_name:443/ipp	
Native File Access Protocols (NFAP)	Use the standard file managers on a Linux, Macintosh, Windows, or UNIX workstation to access volumes on OES 2 NetWare that you have the appropriate file trustee rights to.	NFAP is installed and available by default on all NetWare servers.
NetStorage	For browser access, use: http: or https://server_ip_or_dns/netstorage For WebDAV access, use: http: or https://server_ip_or_dns/oneNet/NetStorage	The WebDAV URL is case sensitive.
Novell Client™	1. Install the Novell Client on a supported Windows workstation. 2. Log in to eDirectory™. 3. Access NCP™ volumes on NetWare or Linux that you have the appropriate file trustee rights to.	
Novell AFP	In the Chooser, click Go and browse to the server.	
Novell CIFS	Map a network drive in Windows Explorer. Create a Web Folder in Internet Explorer.	
Novell iFolder® 3.x Web Access server	https://server_ip_address_or_dns_name/ifolder	“ifolder” is the default name, but this can be customized by the administrator.
Novell Remote Manager	http://server_ip_address_or_dns_name:8008	Any LUM-enabled user can see their directories and files on OES 2 Linux servers.
Samba	Map a network drive in Windows Explorer. Create a Web Folder in Internet Explorer.	

OES 2 SP1 Browser Support

As a general rule, Open Enterprise Server 2 SP1 management tools support the following browsers as they are available on the workstation platforms listed in “[Client/Workstation OS Support](#)” on [page 261](#):

- ♦ Mozilla Firefox2.0.x
- ♦ Microsoft Internet Explorer 6 (latest SP)
- ♦ Microsoft Internet Explorer 7 (latest SP)
- ♦ Apple Safari* 3.1

Table F-1 provides service-specific links and information about browser support in Novell® OES.

Table F-1 *Browser Support in OES*

Management Tool	Supported Browser Information Link
iManager 2.7	<ul style="list-style-type: none"> ♦ “Using a Supported Web Browser” in the Novell iManager 2.7.2 Administration Guide <p>There are rendering differences for some iManager plug-ins between Internet Explorer 6 (IE) and Mozilla-based browsers. For example, options that are accessed through tabs in IE are sometimes accessed through drop-down lists in Firefox.</p>
iMonitor	<ul style="list-style-type: none"> ♦ “System Requirements” in “Using Novell iMonitor 2.4” in the Novell eDirectory 8.8 Administration Guide
IP Address Manager (NetWare®)	Same as Novell Remote Manager
iPrint	<ul style="list-style-type: none"> ♦ “Supported Browsers for iPrint” in the OES 2 SP1: iPrint for Linux Administration Guide ♦ “Supported Browsers for iPrint” in the OES 2 SP1: iPrint Administration Guide for NetWare
MySQL 4.0 (phpMyAdmin) (NetWare)	<ul style="list-style-type: none"> ♦ “Administering MySQL Using phpMyAdmin” in the OES 2 SP1: Novell MySQL for NetWare Administration Guide
Novell iFolder® 3.7	<ul style="list-style-type: none"> ♦ “Web Browser” in the OES 2 SP1: Novell iFolder 3.7 Administration Guide
Novell Remote Manager	<ul style="list-style-type: none"> ♦ “System Requirements” in the OES 2 SP1: Novell Remote Manager for Linux Administration Guide ♦ “System Requirements” in the OES 2 SP1: Novell Remote Manager for NetWare Administration Guide
OpenSSH Manager (NetWare)	<ul style="list-style-type: none"> ♦ “Added Functionality” in the OpenSSH Administration Guide
QuickFinder™ Server Manager	<ul style="list-style-type: none"> ♦ “Managing QuickFinder Server” in the OES 2: Novell QuickFinder Server 5.0 Administration Guide
TCP/IP Configuration (NetWare)	Same as Novell Remote Manager

Management Tool	Supported Browser Information Link
Tomcat Manager	♦ “Managing Tomcat with Tomcat Admin” in the <i>Tomcat for NetWare Administration Guide for OES</i>



Client/Workstation OS Support

As a general rule, Open Enterprise Server 2 services can be accessed and administered from workstations running the following operating systems:

- ♦ SUSE® Linux Enterprise Desktop 10 SP2
- ♦ Microsoft Windows XP SP2 and SP3
- ♦ Microsoft Windows Vista Business SP1
- ♦ Microsoft Windows Vista Business 64-bit SP1
- ♦ Microsoft Windows Vista Ultimate SP1
- ♦ Microsoft Windows Vista Ultimate 64-bit SP1
- ♦ Microsoft Windows Vista Enterprise SP1
- ♦ Microsoft Windows Vista Enterprise 64-bit SP1
- ♦ Macintosh OS X 10.4 Tiger* (Intel*) (non-administrative only)
- ♦ Macintosh OS X 10.5 Leopard* (Intel) (non-administrative only)
- ♦ Windows 2000 SP4 Server (iPrint Client only)
- ♦ Windows 2003 Server (iPrint Client only)
- ♦ Windows 2008 Server (iPrint Client only)

For specific information on a given service, consult the service documentation.

OES 2 Linux Service Scripts

Novell® Open Enterprise Server 2 services rely on specific service scripts located in `/etc/init.d`. The scripts used by OES 2, some of which are standard Linux scripts, are listed in [Table H-1](#).

IMPORTANT: For managing OES 2 services, we strongly recommend using the browser-based tools outlined in [Section 11.1, “Overview of Management Interfaces and Services,” on page 85](#). The browser-based tools provide error checking not available at the service-script level, and they ensure that management steps happen in the sequence required to maintain service integrity.

Table H-1 OES Service Scripts in `/etc/init.d`

Services Associated with Scripts	Script Name	Notes
Apache Web server	<code>apache2</code>	The <code>rcapache2</code> symbolic link, which is by default part of the path, can be used to start, stop, and restart the Apache Web Server, rather than referencing the init script directly.
Archive and Version Services	<code>novell-ark</code>	This lets you to start, stop, restart and display the status of the Archive and Version Service.
CASA	<code>micasad</code>	This is the CASA daemon.
Distributed File Services	<code>novell-dfs</code>	This lets you start and stop the VLDB service.
DNS (Novell eDirectory™ enhanced)	<code>novell-named</code>	This works in connection with <code>named</code> to provide Novell eDirectory DNS services.
DNS (SUSE® Linux Enterprise Server 10 base)	<code>named</code>	This is the SLES 10 DNS service daemon.
Dynamic Storage Technology	<code>novell-shadowfs</code>	This script starts and stops the shadowfs daemon and the kernel module fuse.
eDirectory	<code>ndsd</code>	This lets you start and stop eDirectory. It executes the <code>/usr/sbin/ndsd</code> binary.
eDirectory SNMP support	<code>ndssnmppsa</code>	
eDirectory LDAP support	<code>nldap</code>	This lets you load and unload the LDAP library that Novell eDirectory uses to provide LDAP support. It is not actually a service.
FTP	<code>pure-ftpd</code>	This is used by the Novell FTP Pattern.
iPrint	<code>cups</code>	
	<code>novell-idsd</code>	
	<code>novell-ipsmd</code>	

Services Associated with Scripts	Script Name	Notes
iPrint	cups	iPrint uses this daemon.
Linux User Management	namcd	These daemons are required by Linux User Management and work together to ensure good performance. The namcd daemon caches user and group names and IDs from eDirectory, speeding subsequent lookups of cached users and groups. The nscd daemon caches host names and addresses.
	nscd	
Logging	syslog	This is used for logging by many OES 2 services.
Novell AFP	novell-afptcpd	This script starts and stops the afptcpd daemon, which is the Novell AFP service daemon
Novell CIFS	novell-cifs	This script starts and stops the cifsd daemon, which is the Novell CIFS service daemon
NetStorage (actually XTier)	novell-xregd	NetStorage runs inside the novell-xsrzd XTier Web Services daemon, and also utilizes Tomcat services for certain other functions. novell-xregd is the init script for starting and stopping XTier's registry daemon. It is part of the <code>novell-xtier-base</code> RPM and is enabled by default for run levels 2, 3, and 5. novell-xsrzd is the init script for starting and stopping XTier's Web services daemon. It is also part of the <code>novell-xtier-web</code> RPM and is enabled for run levels 2, 3, and 5.
	novell-xsrzd	
Novell Cluster Services™ (NCS)	novell-ncs	NCS uses some shell scripts and utilities that come with the heartbeat package. For example, NCS uses a binary called <code>send_arp</code> to send out ARP packets when a secondary address is bound. NCS never runs the heartbeat daemons. In fact, NCS and heartbeat are mutually exclusive when it comes to execution, and heartbeat must always be configured to not run (<code>chkconfig heartbeat off</code>) when NCS is loaded on the server.

Services Associated with Scripts	Script Name	Notes
Novell Remote Manager	novell-httpstk	<p>This script runs by default on every OES 2 Linux server and enables access to NRM for Linux through a browser.</p> <p>Use this script followed by the status option to view current status. Or use stop, start, or restart options to alter the run state of the NRM daemon as needed.</p>
Novell Storage Services™	novell-nss	<p>This script runs by default on every OES 2 Linux server with NSS volumes and enables access to the NSS runtime environment.</p> <p>To see if the NSS kernel modules and NSS admin volume are running, enter <code>service novell-nss status</code>, <code>/etc/init.d/novell-nss status</code>, or <code>rcnovell-nss status</code> at a command prompt. If they are not running, use the <code>start</code> option to start them. You cannot stop NSS.</p>
Novell Remote Manager e-mail notifications	postfix	Novell Remote Manager uses this to send notifications as configured.
NTP	ntp	This is the SLES 10 Network Time Protocol daemon.
OpenWBEM CIMOM	owcimomd	<p>This is used to start the OpenWBEM CIMOM daemon, which is an integral part of the iManager plug-ins for LUM, Samba, NSS, SMS, and NCS. iPrint and NRM also use OpenWBEM.</p> <p>Novell Remote Manager on OES 2 Linux gets its server health information from CIMOM.</p>
Patching	novell-zmd	This is the GUI patch updater daemon.
Red Carpet®	rcd	This is the rug command line daemon.
Samba	nmb	This is the Samba NetBIOS naming daemon.
Samba CIFS support	smb	This script runs the Samba daemon.
SLP support	slpd	This lets you start and stop OpenSLP, which is a key component for eDirectory and certain other services and clients.
Storage Management Services™	novell-smldr	This lets you start and stop the SMDR daemon process. It also loads and unloads the NSS zapi kernel module used by SMS to back up the NSS volumes.
Tomcat	novell-tomcat5	This script sets up the SLES 10 Tomcat specifically for OES 2 services, such as the Welcome pages.

System User and Group Management in OES 2 SP1

This section discusses the users and groups that are used by Open Enterprise Server. Administrative users are discussed in [Appendix J, “Administrative Users in OES 2 SP1,” on page 287](#).

- ♦ [Section I.1, “About System Users and Groups,” on page 267](#)
- ♦ [Section I.2, “Understanding Proxy Users,” on page 269](#)
- ♦ [Section I.3, “Planning Your Proxy Users,” on page 274](#)
- ♦ [Section I.4, “Implementing Your Proxy User Plan,” on page 281](#)
- ♦ [Section I.5, “Proxy Users and Domain Services for Windows,” on page 282](#)
- ♦ [Section I.6, “System Users,” on page 282](#)
- ♦ [Section I.7, “System Groups,” on page 284](#)

I.1 About System Users and Groups

“Regular” network users rely on network services. System users and groups support those services.

Some NetWare administrators are concerned about the number of system users and groups on an OES Linux server. They wonder what functions system users perform, why there are “so many” of them, and how they impact licensing and network security.

The answers to these and other questions are found in the sections that follow.

- ♦ [Section I.1.1, “Types of OES System Users and Groups,” on page 267](#)
- ♦ [Section I.1.2, “OES System Users and Groups by Name,” on page 268](#)

I.1.1 Types of OES System Users and Groups

The users and groups that support OES services can be grouped into the three types shown in [Table I-1](#).

Table I-1 *Types of System Users and Groups with Examples*

System User or Group Type	Purpose	Examples
Proxy User	Perform very specific service-related functions, such as <ul style="list-style-type: none"> ♦ Retrieving passwords and service attributes ♦ Writing Service information in eDirectory. ♦ Providing a user ID (uid) that the associated service daemon uses to run. 	<ul style="list-style-type: none"> ♦ <code>afpProxyUser-servername</code> ♦ <code>cifsProxyUser-servername</code> ♦ <code>LUM_Proxy_user</code>

System User or Group Type	Purpose	Examples
System Group	<ul style="list-style-type: none"> ♦ Facilitate the management of system users ♦ Provide access rights to service data on the server or in the eDirectory tree. 	<ul style="list-style-type: none"> ♦ DHCP ♦ DNSDHCP
System User	The daemons associated with the respective services run as these users.	<ul style="list-style-type: none"> ♦ wwwrun ♦ iprint

I.1.2 OES System Users and Groups by Name

Table I-2 lists the users and groups that OES services depend on and use.

Table I-2 *System User and Groups Listing*

System User or Group	Object Type	Associated Service
AfpProxyUser- <i>servername</i>	Proxy User	AFP
(Archive Versioning Proxy)	Proxy User	Archive and Versioning Services
The install admin is always assigned.		
arkuser	System User	Archive and Versioning Services
CifsProxyUser- <i>servername</i>	Proxy User	CIFS
DHCP LDAP Proxy	Proxy User	DHCP
dhcpd	System User	DHCP
DHCPGroup	System Group	DHCP
DNS Proxy	Proxy User	DNS
DNSDHCP-GROUP	System Group	DNS
hacluster	System User	Heartbeat
iFolderProxy	Proxy User	iFolder 3
iprint	System User	iPrint
lprint (POSIX)	System Group	iPrint
lprintgrp (eDirectory)		
LUM proxy (optional)	Proxy User	Linux User Management
named	System User	DNS
ncsclient	System User	NCS
ncsgroup	System Group	NCS
NetStorage Proxy	Proxy User	NetStorage

System User or Group	Object Type	Associated Service
novell_nobody	System User	CIMOM
novell_nogroup	System Group	CIMOM
novlxregd	System User	XTier
novlxsrvd	System User	XTier
novlxtier	System Group	XTier
server_name-SambaProxy	Proxy User	Samba (Novell)
server_name-W-SambaUserGroup	System Group	Samba (Novell)
server_nameadmin	Proxy User	NSS
www	System Group	Apache
		Tomcat
		QuickFinder
wwwrun	System User	Apache

I.2 Understanding Proxy Users

The subject of OES proxy users is somewhat complex. Therefore, it's a good idea to understand the basics before planning your implementation strategy.

IMPORTANT: The information in the following sections only answers security questions and provides general information. It is not intended to be used for the manual configuration of proxy users.

- ♦ [Section I.2.1, “What Are Proxy Users?,” on page 269](#)
- ♦ [Section I.2.2, “Why Are Proxy Users Needed on OES Linux?,” on page 270](#)
- ♦ [Section I.2.3, “Which Services Require Proxy Users and Why?,” on page 270](#)
- ♦ [Section I.2.4, “What Rights Do Proxy Users Have?,” on page 271](#)

I.2.1 What Are Proxy Users?

As the name implies, proxy users are user objects that perform functions on behalf of OES services.

Proxy user accounts do not represent people, rather they are eDirectory objects that provide very specific and limited functionality to OES services. Generally, this includes only retrieving service-related information, such as user passwords and service attributes, but sometimes proxy users also write service information in eDirectory.

Many but not all OES services rely on proxy users to run on Linux (see [“Which Services Require Proxy Users and Why?” on page 270](#)). Proxy user creation and/or configuration is therefore an integral part of configuring OES.

None of the OES services require that you specify proxy user information during the OES installation, but some, such as DNS/DHCP, AFP, CIFS, and iFolder, give you the option to do so. Others, such as NCS and NSS create proxy users without user input, while Archive and Versioning Services always uses the install admin as its proxy user.

I.2.2 Why Are Proxy Users Needed on OES Linux?

OES Linux provides the Novell services that were previously only available on NetWare.

To make its services available on Linux, Novell had to accommodate a fundamental difference between the way services run on NetWare and the way they run on Linux.

- ♦ **NetWare Services:** The NetWare operating system and eDirectory are tightly integrated. This allows the services (NLMS) on NetWare to assume the identity of a server object in eDirectory, thus gaining access to the other objects and information in eDirectory that are needed for the services to run.
- ♦ **OES Linux Services:** eDirectory also runs very well on OES Linux, and it provides the infrastructure on which OES services rely, but it is not integrated with the Linux operating system.

On Linux servers there is no concept of a service, such as Apache or iFolder running as a server object. Instead, each service runs using a User ID (uid) and a Group ID (gid) that the Linux server recognizes as being valid.

I.2.3 Which Services Require Proxy Users and Why?

The following services utilize a proxy user.

Table I-3 Proxy Users Functions Listed by Service

Associated Service	Example Proxy User Name	Services That the User Provides
AFP	AfpProxyUser- <i>servername</i>	Retrieves passwords for AFP users.
Archive Versioning	admin The install admin is always specified.	The service runs as this user.
CIFS	CifsProxyUser- <i>servername</i>	Retrieves passwords for CIFS users.
DHCP	DHCP_LDAP_Proxy	This lets the service access DHCP objects in eDirectory.
DNS	DNS_Proxy	This lets the service access DNS objects in eDirectory.

Associated Service	Example Proxy User Name	Services That the User Provides
iFolder 3	iFolderProxy	<p>This Folder proxy user connects to the eDirectory server and retrieves the following information:</p> <ul style="list-style-type: none"> ♦ modifytimestamp ♦ cn ♦ mail ♦ sn ♦ GUID ♦ givenName ♦ member
Linux User Management	<i>LUM_proxy</i>	Searches the tree for LUM users.
NetStorage	<i>NetStorage_Proxy</i> The LDAP Admin user is specified by default, but another user can be created prior to installing and then specified.	Performs LDAP searches for users logging into NetStorage.
NSS	<i>server_nameadmin</i>	<p>Reads user objects and maintains the volume, pool, and other storage system objects.</p> <p>This user performs some of the same functions as proxy users do for other services. However, unlike other OES services that can share proxy users, NSS requires a unique proxy user for each server.</p>
Samba (Novell)	<i>server_name-SambaProxy</i>	Searches the LDAP tree (eDirectory) for Samba users.

I.2.4 What Rights Do Proxy Users Have?

Each OES service's YaST installation automatically adds the required rights to the proxy user specified for the service.

Unless otherwise specified, each of the following users has the standard set of user rights in eDirectory:

♦ **Self:**

Login Script:

Read Write, Not inheritable

Print Job Configuration:

Read Write, Not inheritable

[All Attribute Rights]:

Read, Inheritable

♦ **[Public]**

Message Server:

Read, Not inheritable

♦ **[Root]**

Group Membership

Read, Not inheritable

Network Address

Read, Not inheritable

In addition, each proxy user is granted additional rights as summarized in [Table I-4](#).

Table I-4 Proxy Users Rights

Associated Service	Example Proxy User Name	Default Rights Granted
AFP	AfpProxyUser- <i>servername</i>	♦ The Universal Password policy associated with the AFP users grants this proxy user the right to retrieve AFP user passwords.
Archive Versioning	<i>Archive Versioning Proxy</i>	♦ This user has Read and Write rights to the archived volume.
CIFS	CifsProxyUser- <i>servername</i>	♦ The Universal Password policy associated with the CIFS users grants this proxy user the right to retrieve CIFS user passwords.
DHCP	DHCP_LDAP_Proxy	♦ No rights are assigned directly, but membership in the DHCPGroup, which does have assigned rights, provides the rights it needs.
DNS	DNS_Proxy	♦ No rights are assigned directly, but membership in the DNS-DHCPGroup, which does have assigned rights, provides the rights it needs.

Associated Service	Example Proxy User Name	Default Rights Granted
iFolder 3	iFolderProxy	<ul style="list-style-type: none"> Additional eDirectory rights include: <p>[Entry Rights]</p> <p>Browse</p> <p>LDAP ACL representation:</p> <p>1#subtree#iFolderProxy#</p> <p>[All Attributes Rights]</p> <p>Read, Compare</p> <p>LDAP ACL representation:</p> <p>3#subtree#iFolderProxy#</p>
Linux User Management	LUM_proxy	<ul style="list-style-type: none"> If created, this proxy user has Search rights on Unix Config & Unix Workstation Objects.
NetStorage	NetStorage_Proxy	<ul style="list-style-type: none"> Additional eDirectory rights: <p>[Entry Rights]</p> <p>Browse</p> <p>LDAP ACL representation:</p> <p>1#subtree#NetStorage_Proxy#</p> <p>[All Attributes Rights]</p> <p>Read, Compare</p> <p>LDAP ACL representation:</p> <p>3#subtree#NetStorage_Proxy#</p>
NSS	server_nameadmin	<ul style="list-style-type: none"> Additional eDirectory rights: <p>Supervisor right to the container it was created in.</p>
Samba (Novell)	server_name-SambaProxy	<ul style="list-style-type: none"> The Universal Password policy associated with the Samba users grants this proxy user the right to retrieve user passwords. Additional eDirectory rights: <ul style="list-style-type: none"> Rights to itself – Supervisor attribute right Rights to the OU where it is located All Attribute rights – Read Write Entry rights – Browse Create samba* – Create Read Write

I.3 Planning Your Proxy Users

Because of the prominent role played by the proxy users on your OES network, it is important that you understand your implementation options and the implications for each option. You can then plan an overall proxy user implementation strategy.

- ♦ [Section I.3.1, “About Proxy User Creation,” on page 274](#)
- ♦ [Section I.3.2, “Proxy User Impacts on User Connection Licenses,” on page 277](#)
- ♦ [Section I.3.3, “Limiting the Number of Proxy Users in Your Tree,” on page 277](#)
- ♦ [Section I.3.4, “Proxy Users and Passwords,” on page 279](#)

I.3.1 About Proxy User Creation

The first step in planning your proxy user implementation strategy is understanding the do’s and don’ts of proxy user creation.

- ♦ [“Creation Options” on page 274](#)
- ♦ [“Do Not Manually Configure Proxy Users” on page 276](#)
- ♦ [“Avoid Assigning an Admin User As a Proxy User” on page 276](#)

Creation Options

[Table I-2](#) presents information about the creation options for each OES proxy user.

Table I-5 *Proxy User Creation Options*

Associated Service	Default Proxy User Name	Creation Information
AFP	AfpProxyUser- servername	<p>By default, the AFP YaST install automatically</p> <ul style="list-style-type: none"> ♦ Creates a proxy user named <code>afpProxyUser-servername</code> in the same context as the server. ♦ Creates a Universal Password Policy that you can assign to AFP users after the install. ♦ Generates a password and stores it in either CASA or in an encrypted file on the server, depending on which option you select. <p>Alternatively, you can modify any of the defaults, including the password. Or if you have already created a proxy user, you can specify that as well.</p> <p>If you access the AFP configuration pages and there are no Universal Password Policies in your tree, the install reminds you that AFP users must have a policy assigned.</p>
Archive Versioning	admin	<p>The admin account that installs the server is automatically assigned as the Archive and Versioning proxy user. This is not configurable.</p>

Associated Service	Default Proxy User Name	Creation Information
CIFS	CifsProxyUser- servername	<p>By default, the CIFS YaST install automatically</p> <ul style="list-style-type: none"> Creates a proxy user named cifsProxyUser-<i>servername</i> in the same context as the server. Creates a Universal Password Policy that you can assign to CIFS users after the install. Generates a password, and stores it in either CASA or in an encrypted file on the server, depending on which option you select. <p>Alternatively, you can modify any of the defaults, including the password. Or if you have already created a proxy user, you can specify that as well.</p> <p>If you access the CIFS configuration pages and there are no Universal Password Policies in your tree, the install reminds you that CIFS users must have a policy assigned.</p>
DHCP	Same as install admin	<p>By default, the admin account that installs the server is assigned as the DHCP proxy user.</p> <p>If you want to assign an alternate user account, it must already exist in the tree and be able to access the DHCP server object.</p>
DNS	Same as install admin	<p>By default, the admin account that installs the server is assigned as the DNS proxy user.</p> <p>If you want to assign an alternate user account, it must already exist in the tree and have Read, Write, and Browse rights in the contexts where the DNS Locator, Root Server, and Group Object are created.</p>
iFolder 3	iFolderProxy	<p>By default, the system automatically creates a proxy user named iFolderProxy.</p> <p>Alternatively, you can modify any of the defaults, including the password, or if you have already created a proxy user, you can specify that as well. The user must have the Read right to the LDAP service.</p>
Linux User Management	LUM_proxy (optional)	<p>(Optional) By default, no LUM proxy user is created. If you create one, it will be assigned rights to search the LDAP tree for LUM objects. If you assign an existing user, it must have the aforementioned LDAP search rights.</p>
NetStorage	Same as install admin	<p>By default, the admin account that installs the server is assigned as the NetStorage proxy user.</p> <p>Alternatively, you can specify an existing proxy user with rights to search the LDAP tree if desired.</p>
NSS	server_nameadmin	<p>This admin account must have full rights to administer NSS and must be unique to each server.</p>

Associated Service	Default Proxy User Name	Creation Information
Samba (Novell)	<code>server_name-SambaProxy</code>	<p>By default, the Samba proxy user is created in the container specified as the Base Context for Samba Users and is named <code>servername-sambaProxyUser</code>.</p> <p>You specify the password for this user when you configure Novell Samba.</p> <p>You can specify another eDirectory user as the Samba proxy user. If you do, be aware of the following:</p> <ul style="list-style-type: none"> ♦ If you specify a user that doesn't already exist in eDirectory, the user account is created and granted the necessary rights. You must also specify a password for the new user. ♦ If you specify an existing eDirectory user, it is assumed that you have already created the user account with the necessary rights and no modifications are made to the existing user. ♦ If you specify an existing eDirectory user but enter a new password, you are prompted to change the password for that user.

Do Not Manually Configure Proxy Users

Best practices for most OES installation scenarios dictate that proxy users be created in eDirectory prior to installing OES. For more information, see [“Limiting the Number of Proxy Users in Your Tree” on page 277](#).

After creation, proxy users should be configured for OES service use only by the YaST based install, not manually.

The information in these sections only answers security questions and provides general information. It is not intended to be used for the manual configuration of proxy users.

Avoid Assigning an Admin User As a Proxy User

We recommend using special-purpose proxy user accounts rather than specifying admin users as proxy users.

Although specifying an admin user as the proxy user appears to be an easy way of setting up OES services (and is the install default in some cases), there are potential problems. Mixing actual users with system-level functionality always creates some risk.

The following is a real-life example of risks that can occur when admin users are assigned as proxy users:

Novell Support received a call from an administrator who was getting locked out due to intruder detection after changing the administrator password. The lockout happened several times each day and seemed to be coming from the OES 2 servers. The support technician checked LUM and all of the services he could think of, and didn't see the admin credentials anywhere.

Further investigation revealed that the administrator credentials had been used to install OES 2 on multiple servers, and by default the credentials were therefore also used as the proxy user credentials for some of the OES services. Consequently, the credentials were stored in CASA for use when the OES services came up.

Because the Admin password had changed, the CASA credentials had expired and service authentication requests were failing, resulting in the intruder detection lockout.

I.3.2 Proxy User Impacts on User Connection Licenses

From a licensing standpoint, each proxy user counts as a user on the OES network and consumes one user connection license.

It is not unreasonable to expect that the OES servers you install could average five to six proxy users a piece, meaning that an organization that has three to five OES servers installed with the default settings, can expect that 15 to 30 of its user connection licenses might be taken by proxy users.

For large organizations with hundreds of servers, the user connections consumed by default installations would be substantial. Therefore, large organizations are especially interested in methods for limiting the number of proxy users on their network.

I.3.3 Limiting the Number of Proxy Users in Your Tree

Table I-6 outlines various options for limiting the number of proxy users in your tree and summarizes the licensing, security, and manageability considerations of each approach.

Table I-6 *Options for Limiting the Number of Proxy Users*

Approach	Licensing Impact	Security Considerations	Manageability Considerations
Per Service per Server (default)	One for each service on each server	For AFP, CIFS, iFolder 3, NSS, and Samba this is the most secure option. Passwords for these are system-generated and not known by anyone. For LUM there is no option to have a system-generated password. For DNS, DHCP, and NetStorage, the install admin's credentials are used by default. This has separate security implications as outlined in "Avoid Assigning an Admin User As a Proxy User" on page 276 .	This approach requires no proxy user planning. Services are installed at the same time as the OES server. This is a good option for small organizations or installations where only a few services are used. This is not a good option if security policies dictate that all passwords must be reset periodically.

Approach	Licensing Impact	Security Considerations	Manageability Considerations
Per Server	One for each server	This confines any security vulnerabilities to individual servers.	<p>This requires that a proxy user for the server is created before the server is installed.</p> <p>For the first server in the tree, eDirectory and iManager must be installed with the server. Then after the server installation finishes, the proxy user can be created. And finally the services can be installed and configured to use the proxy user for the server.</p> <p>This is not generally recommended. However, it can be useful when each OES server is managed by a separate administrator, or for enterprises where branch users access a server in the branch office.</p> <p>The install admin must know the proxy user's password.</p>
Per Partition	One for each partition	This confines any security vulnerabilities to individual partitions.	<p>This is useful when users are co-located with the OES servers in a single partition, and cross-partition access of users to services is rare.</p> <p>This is a good approach for organizations where eDirectory administration is done at a partition level.</p> <p>This requires that a proxy user for the partition is created before services are installed in the partition.</p> <p>The install admin must know the proxy user's password.</p>
Per Service	Up to nine licenses depending on the number of OES services deployed	<p>This confines any security vulnerabilities to individual services.</p> <p>It also ensures that proxy user rights are not overloaded but are distributed so that there is a single proxy user for each type of service</p>	<p>For example, you might have one proxy user for file-access (AFP, CIFS), one for DNS/DHCP, one for iFolder, one for iPrint etc.</p> <p>This is useful in trees where the users and servers are not co-located, and different services are administered by different administrators.</p> <p>This requires that a proxy user for the service is created before the service is installed in the tree.</p> <p>The install admin must know the proxy user's password.</p>

Approach	Licensing Impact	Security Considerations	Manageability Considerations
Per Tree	One license	This exposes all OES services and servers in the tree to any security vulnerabilities.	<p>This requires that a proxy user for the tree is created before any OES services are installed in the tree.</p> <p>This is suitable for organizations that have</p> <ul style="list-style-type: none"> ♦ Centralized eDirectory administration ♦ Users that are not confined to the partition or subtree where the OES servers reside, but instead access different OES servers from all over the tree. <p>The install admin must know the proxy user's password.</p>

I.3.4 Proxy Users and Passwords

Proxy user passwords must be stored on the individual OES servers where the services are installed because proxy users must be able to log in to eDirectory to perform their required functions.

- ♦ [“Auto-Generated vs. Specified Passwords” on page 279](#)
- ♦ [“Passwords Are Stored on the Server” on page 279](#)
- ♦ [“Avoid Password Expiration Problems” on page 280](#)

Auto-Generated vs. Specified Passwords

- ♦ **Auto-Generated Passwords:** AFP, CIFS, iFolder 3, NSS, and Samba use auto-generated passwords by default.

This offers the highest security because the passwords are known only to the system. However, this option generates one proxy user per service per server, and it is critical that the assigned password policies not cause passwords to expire.

- ♦ **Manually Specified Passwords:** For Archive and Versioning, DNS, DHCP, LUM, and NetStorage, this is the only available option, and it applies to the other OES services in all but the default (per service per server) installation scenario. It requires that someone keep track of the proxy user names and passwords for installation purposes.

Passwords Are Stored on the Server

Of course all proxy user passwords are stored in eDirectory. [Table I-7](#) explains where they are stored on the server and how they can be reset if needed.

Table I-7 Password Storage Locations

Associated Service	Where the Password Is Stored Locally	How the Password Can Be Reset
AFP	This password is stored in either CASA or in an encrypted file, depending on the configuration option specified during service installation.	You can use iManager to reset the password in CASA or in the encrypted file, or the CASAccli tool if it is stored in CASA.
Archive and Versioning	This password is stored in CASA.	You must use the script provided by Archive and Versioning Services to change the password on the server.
CIFS	This password is stored in either CASA or in an encrypted file, depending on the configuration option specified during service installation.	You can use iManager to reset the password in CASA or in the encrypted file, or the CASAccli tool if it is stored in CASA.
DHCP	This password is stored in CASA if it is available. If CASA is not available, it is stored in the <code>/etc/dhcpd.conf</code> file.	If the password is stored in CASA, you can set it using the CASAccli tool. If not, edit the <code>/etc/dhcpd.conf</code> file.
DNS	This password is stored in CASA if it is available. If CASA is not available, it is stored in an encrypted file.	??
iFolder 3	This password is stored in the iFolder store with PKI cryptography.	It can be changed either from a terminal prompt using the iFolder command line utilities or through the iFolder Admin Console.
Linux User Management	This is stored in the <code>/etc/nam.conf</code> file.	Edit the <code>/etc/nam.conf</code> file and change the password in eDirectory.
NetStorage	This password is stored in the XTier registry.	This can be changed in iManager through the NetStorage plug-in.
NSS	??	This password is system-generated at install time and cannot be reset.
Samba (Novell)	This password is stored in Samba.	You can change the password by using the <code>smbpasswd</code> command.

IMPORTANT: Although the YaST based install can sometimes be used successfully to reconfigure some OES services, Novell neither recommends nor supports that practice.

Avoid Password Expiration Problems

Many organizations require that all network users have password policies to enforce regular password expiration and change.

Such policies create complications for the proxy user design. Proxy user passwords are stored on the local system to enable the OES services to log in to eDirectory. Every time a password change is forced in eDirectory, services stop working until the password is synchronized on the server.

These problems can be avoided by:

- ♦ Not assigning proxy users a password policy that enforces password expiration.
- ♦ Not using real user credentials for proxy users. See [“Avoid Assigning an Admin User As a Proxy User” on page 276](#).

If password expiration policies cannot be avoided, or a security policy dictates that proxy user passwords must be changed periodically, you can do the following.

- ♦ Ensure that the responsible administrator knows or has a record of each proxy user’s password and is aware of when they expire.
- ♦ Before passwords expire, change them in eDirectory and reset them on the server. See the information in [Table I-7](#).

I.4 Implementing Your Proxy User Plan

The proxy users in OES can be configured at different levels within eDirectory, depending on your needs.

IMPORTANT: The brief instructions that follow assume that you are installing into an existing tree. For new trees you will need to install and configure eDirectory on the first server without configuring any other OES services.

After the server is installed and you have created the required proxy users and passwords, then you can install the OES services and configure them to use the proxy users you have created.

The exception to this is installing all services without changing the default configuration settings (see [Table I-5 on page 274](#)). In most cases a default configuration assigns the install admin as the proxy user for the service.

I.4.1 Tree-wide proxy users

Do the following:

1. Create a proxy user in the eDirectory tree where the OES servers will be installed, and set the password.

Consider naming the user to reflect its purpose. For example, name the proxy user `oes_service_proxy_user`.

2. Use this proxy user and password while configuring the services on all of the OES servers in that tree.

I.4.2 Service-specific proxy users

Do the following:

1. Create a proxy user in the eDirectory tree for each type of OES service and set the passwords.

Consider naming the user to reflect its purpose. For example, name the AFP proxy user, `afp_proxy_user`.

2. Use these proxy users and passwords appropriately for each of the OES services on all OES servers.

I.4.3 Partition-wide proxy users

Do the following:

1. Create one proxy user object per eDirectory partition in the OES tree, and set the password.

Consider naming the user to reflect its purpose. For example, name the proxy user for the London regional office, `london_office_proxy_user`.

2. Use this proxy user and password for configuring all of the OES services on all the OES servers in that partition.

I.4.4 Server-wide proxy user

Do the following:

1. Create one proxy user object per OES server (preferably in the same container as the server) and set the password
2. Use this proxy user and password as the proxy user for all the services on that particular OES server.

I.4.5 Individual proxy user per-server-per-service

This is the installation default as explained in [Table I-6, “Options for Limiting the Number of Proxy Users,” on page 277](#).

I.5 Proxy Users and Domain Services for Windows

Proxy users are not used in DSfW.

The Services part of the Trusted Computer Base has the rights to read users’ supplemental credentials for authentication. A separate KRB process reads user passwords and performs the authentication. Another event handler in eDirectory creates the supplemental credentials for the user whenever the password is changed for that user.

I.6 System Users

SLES and OES create system users on the local Linux system to provide user IDs (uids) to service processes. These users have rights to local files, such as configuration files.

The services that rely on system users do not have passwords because they don't need to log in. They simply use their associated user IDs.

When NSS is installed, some of these users are moved to eDirectory and LUM enabled. This is done to provide access to NSS data, to keep the user IDs the same across multiple servers, and to facilitate clustering and shared volumes.

Table I-2 lists the various system users that are used by OES services.

Table I-8 *System User Purposes*

System User or Group Name	Associated Service	Purpose
arkuser	Archive and Versioning Services	The service uses PostgreSQL as its metadata store, and PostgreSQL must run as a low-privileged user. arkuser is that low-privileged user.
dhcpcd	DHCP	DHCP accesses local resources through this or an alternatively specified user. If the DHCP lease and configuration files are stored on NSS, the user must be moved to eDirectory and LUM enabled. dhcpcd is used by default, but any local user can be used.
hacluster	Heartbeat	This user is created by Heartbeat, but it not used by Heartbeat nor by Novell Cluster Services.
iprint	iPrint	The iPrint daemons run as this user. If iPrint is moved to NSS, this user is created in eDirectory and the local user is removed.
named	DNS	This system user lets DNS access local resources. In case of clusters, DNS data is on NSS volume, and so the user has to be created in eDirectory as well. named is used by default, but any local user can be used.
ncsclient	NCS	Used by NCS to access the adminfs file system.
novell_nobody	CIMOM	This user is created by CIMOM but is not currently used.
novlxsregd	XTier	The XTier Registry Daemon (novell-xregd) runs as this user. When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.
novlxsrvd	XTier	The XTier Server Daemon (novell-xsrvd) runs as this user. When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.

System User or Group Name	Associated Service	Purpose
wwwrun	Apache	<p>The Apache daemon runs as this user.</p> <p>When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.</p>

I.7 System Groups

These are groups in the local Linux system that provide a group ID (gid) to an OES process.

When NSS is installed, some of these groups are moved to eDirectory and LUM enabled. This is done to provide access to NSS data and to keep group IDs the same across multiple servers.

Table I-2 lists the system groups that are used by OES services.

Table I-9 *System Group Purposes*

System User or Group Name	Associated Service	Purpose
DHCPGroup	DHCP	The DNS and DHCP servers and proxy users gain rights to DHCP data within the tree through this Group Object
DNSDHCP-GROUP	DNS	Linux DNS Servers gain rights to DNS data within the tree through this Group object. (The name reflects the fact that this group was used on NetWare for both DHCP and DNS.)
lprint (POSIX) iprintgrp (eDirectory)	iPrint	<p>The iPrint daemons use the group ID (gid) of this group to run.</p> <p>If iPrint is moved to NSS, the iprintgrp group is created in eDirectory.</p>
ncsgroup	NCS	<code>ncsclient</code> is a member of this group.
novell_nogroup	CIMOM	This group is created by CIMOM but is not currently used.
novlxtier	XTier	<p>The XTier daemons use the group id (gid) of this group to run.</p> <p>Apache (wwwrun) is a group member because it needs XTier socket access.</p> <p>When NSS is installed on the Linux server, this group is removed from the local system and created in eDirectory. This is required because members of this group must have access to NSS data, and all NSS access is controlled through eDirectory.</p>

System User or Group Name	Associated Service	Purpose
<code>server_name-W-SambaUserGroup</code>	Samba (Novell)	All users granted Samba access are originally assigned to this group, which disables SSH access for them on the server. For more information, see “The Samba connection:” on page 101 .
<code>shadow</code>	QuickFinder	Used by QuickFinder and other Web services.
<code>www</code>	Apache	Apache (<code>wwwrun</code>) and tomcat (<code>novlwww</code>) use the group ID (gid) of this group to run.
	Tomcat	
	QuickFinder	QuickFinder requires that all users who manage the service (including the eDirectory Admin user) belong to this group.
		User <code>novlxsrvd</code> is in the group because it needs access to an Apache domain socket.
		When NSS is installed on the Linux server, this group is removed from the local system and created in eDirectory. This is required because members of this group must have access to NSS data, and all NSS access is controlled through eDirectory.

Administrative Users in OES 2 SP1

Every OES network requires at least one administrative-level user to manage regular network users and system users.

Table J-1 *Administrative Users and Groups*

Administrative User or Group	Associated Service	Object Type	Purpose
Admin	eDirectory	Admin User	The eDirectory administrator that has all rights to manage the Tree. The default is Admin.
Container Admin	eDirectory	Admin User	These administrators are usually responsible for administering within a partition or subtree. They might be assigned only enough rights to install servers, or they might be assigned to specific roles in iManager.
admingroup	eDirectory	Admin Group	Provides LUM-enabling for the eDirectory administrator.
iFolderAdmin	iFolder 3	Service Admin	This is the default iFolder service administrator account. By default, the Tree Admin is specified.
QuickFinderAdmin	QuickFinder	Service Admin	This is the QuickFinder administrator. The default is the Tree Admin.



Documentation Updates

This section summarizes the changes made to this manual since the initial release of Novell® Open Enterprise Server 2 SP1.

July 31, 2009

Chapter or Section Changed	Summary of Changes
"System User and Group Management in OES 2 SP1" on page 267.	Completely reworked and expanded Section.
"Administrative Users in OES 2 SP1" on page 287.	New Section.

June 22, 2009

Chapter or Section Changed	Summary of Changes
"Avoid Uninstalling eDirectory" on page 66.	New Section.
"Web Services" on page 71.	New Section.

May 6, 2009

Chapter or Section Changed	Summary of Changes
"SLP" on page 120.	Removed all information and instructions that refer to incompatibilities between Novell SLP and OpenSLP. This information was outdated. Although there are differences in the two SLP services (see Table 12-4 on page 121), they are completely compatible regarding the sharing of service information.

May 4, 2009

Chapter or Section Changed	Summary of Changes
"Changing the Server's Address Configuration" on page 248.	In response to a user comment, correct link to wrong file.

April 23, 2009

Chapter or Section Changed	Summary of Changes
"What's New" on page 17.	In response to a user comment, reorganized section for clarity.

April 7, 2009

Chapter or Section Changed	Summary of Changes
Throughout the guide.	General editing changes. Nothing substantive.