

Planning and Implementation Guide

Novell® Open Enterprise Server

2 SP2

July 15, 2010

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 or Changed	17
1.1 Where's NetWare?	17
1.1.1 NetWare References in This Guide and Elsewhere	17
1.1.2 NetWare Documentation	17
1.2 Links to What's New Sections	17
1.3 New or Changed in OES 2 SP2	19
1.3.1 Auditing	19
1.3.2 Base Platform Is SLES 10 SP3	19
1.3.3 CIFS DFS Support	19
1.3.4 Create EVMS Proposal Option	19
1.3.5 Cross-Protocol File Locking Change	20
1.3.6 Domain Services for Windows Installation	20
1.3.7 Java Console for DNS/DHCP	20
1.3.8 Performance Increases	20
1.3.9 PureFTP	20
1.3.10 Upgrading Online	20
1.3.11 Windows 7 Client Support	20
1.4 New in OES 2 SP1	20
1.4.1 YaST Install Changes	21
1.4.2 Novell AFP	21
1.4.3 Novell CIFS	21
1.4.4 Novell Domain Services for Windows	22
1.4.5 Migration Tool	22
1.5 New in OES 2 (Initial Release)	23
1.5.1 Dynamic Storage Technology	23
1.5.2 OES 2 Migration Tools	23
1.5.3 Xen Virtualization Technology	23
2 Welcome to Open Enterprise Server 2	25
3 Planning Your OES 2 Implementation	27
3.1 What Services Are Included in OES 2?	27
3.2 Which Services Do I Need?	34
3.3 Exploring OES 2 services	34
3.4 Plan for eDirectory	34
3.5 Prepare Your Existing eDirectory Tree for OES 2	35
3.6 Identify a Purpose for Each Server	35
3.7 Understand Server Requirements	35
3.8 Understand User Restrictions and Linux User Management	36
3.9 Caveats to Consider Before You Install	36
3.9.1 Adding a Linux Node to a Cluster Ends Adding More NetWare Nodes	37
3.9.2 Always Double-Check Service Configurations Before Installing	37
3.9.3 Back Button Doesn't Reset Configuration Settings	37
3.9.4 Cluster Upgrades Must Be Planned Before Installing OES 2	37
3.9.5 Cross-Protocol File Locking Has Changed	38
3.9.6 Do Not Create Local (POSIX) Users	38

3.9.7	Do Not Upgrade to eDirectory 8.8 Separately	39
3.9.8	Follow the Instructions for Your Chosen Platforms	39
3.9.9	If You've Ever Had OES 1 Linux Servers with LUM and NSS Installed.	39
3.9.10	iFolder 3.8 Considerations	42
3.9.11	Incompatible TLS Configurations Give No Warning	42
3.9.12	Installing into an Existing eDirectory Tree	43
3.9.13	NetWare Caveats	43
3.9.14	Novell Distributed Print Services Cannot Migrate to Linux	44
3.9.15	NSS Caveats	44
3.9.16	Plan eDirectory Before You Install	45
3.9.17	Samba Enabling Disables SSH Access.	45
3.9.18	Unsupported Service Combinations	45
3.9.19	VNC Install Fails to Set the IP Address in /etc/hosts	48
3.10	Consider Coexistence and Migration Issues	48
3.11	Understand Your Installation Options	49
3.11.1	OES 2 Installation Overview	49
3.11.2	About Your Installation Options	50
3.11.3	Use Predefined Server Types (Patterns) When Possible	51
3.11.4	If You Want to Install in a Lab First	51
3.11.5	If You Want to Install NSS on a Single-Drive Linux Server	52
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?	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 SP2 Software from the Novell Web Site.	55
4.4.3	Preparing the Installation Media	56
4.4.4	Installing OES 2 for Evaluation Purposes	56
4.4.5	Evaluating OES 2	57
4.4.6	Installing Purchased Activation Codes after the Evaluation Period Expires	57
4.5	Licensing	57
4.5.1	The OES 2 Licensing Model	57
4.5.2	SLES Licensing Entitlements in OES 2	58
4.5.3	OES 2 Doesn't Support NLS	58
5	Installing OES 2	59
5.1	Installing OES 2	59
5.1.1	What's Next	59
5.2	Installing OES 2 Servers in a Xen VM	60
6	Caveats for Implementing OES 2 Services	61
6.1	AFP	61
6.1.1	Anti-Virus Solutions and AFP	61
6.2	Avoiding POSIX and eDirectory Duplications	62
6.2.1	The Problem	62
6.2.2	Three Examples.	62
6.2.3	Avoiding Duplication	63
6.3	CIFS	64
6.3.1	Changing the Server IP Address	64
6.4	ConsoleOne Can Cause JClient Errors	64
6.5	CUPS on OES 2.	64

6.6	eDirectory	64
6.6.1	Avoid Uninstalling eDirectory	65
6.6.2	Avoid Renaming Trees and Containers	65
6.6.3	Default Static Cache Limit Might Be Inadequate	65
6.6.4	eDirectory Fails to Start Automatically After a Command Prompt Install	65
6.6.5	One Instance Only	66
6.6.6	Special Characters in Usernames and Passwords	66
6.7	iFolder 3.8	66
6.8	iPrint	66
6.8.1	Cluster Failover Between Mixed Platforms Not Supported	66
6.8.2	Printer Driver Uploading on OES 2 Might Require a CUPS Administrator Credential	67
6.8.3	Printer Driver Uploading Support	67
6.8.4	iManager Plug-Ins Are Platform-Specific	67
6.8.5	iPrint Client for Linux Doesn't Install Automatically	67
6.8.6	iPrint Disables CUPS Printing on the OES 2 Server	67
6.9	LDAP—Preventing “Bad XML” Errors	67
6.10	Management	68
6.10.1	iManager RBS Configuration with OES 2	68
6.10.2	Storage Error in iManager When Accessing a Virtual Server	69
6.10.3	Truncated DOS-Compatible Short Filenames Are Not Supported at a Terminal Prompt	69
6.11	NCP Doesn't Equal NSS File Attribute Support	69
6.12	Novell-tomcat Is for OES Use Only	70
6.13	NSS (OES 2)	70
6.13.1	Understanding Name Space Support	70
6.13.2	The Role of EVMS	70
6.14	OpenLDAP on OES 2	71
6.15	Samba	71
6.16	Virtualization Issues	71
6.16.1	Always Close Virtual Machine Manager When Not in Use	71
6.16.2	Always Use Timesync Rather Than NTP	71
6.16.3	Backing Up a Xen Virtual Machine	71
6.16.4	Time Synchronization and Virtualized OES 2	71
6.16.5	NSS Considerations	72
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 Service Differences	73
7.1.4	Only One eDirectory Instance Is Supported on OES Servers	74
7.2	OES 2 SP2 Upgrade Paths	74
7.3	NetWare 6.5 SP8 Upgrade Paths	74
8	Migrating and Consolidating Existing Servers and Data	75
8.1	Supported OES 2 SP2 Migration Paths	75
8.2	Migration Tools and Purposes	75
8.2.1	OES 2 SP2 Migration Tool	75
8.2.2	Migrate Windows Shares Utility	75
9	Virtualization in OES 2	77
9.1	Graphical Overview of Virtualization in OES 2	77
9.2	Why Install OES Services on Your VM Host?	77

9.3	Services Supported on VM Hosts and Guests	78
10	Clustering and High Availability	81
11	Managing OES 2	83
11.1	Overview of Management Interfaces and Services	83
11.2	Using OES 2 Welcome Pages	84
11.2.1	The Welcome Site Requires JavaScript, Apache, and Tomcat	84
11.2.2	<<<Accessing the Welcome Web Site.	85
11.2.3	The Welcome Web Site Is Available to All Users	85
11.2.4	Administrative Access from the Welcome Web Site	85
11.3	OES Utilities and Tools	85
11.4	SSH Services on OES 2	93
11.4.1	Overview	93
11.4.2	Setting Up SSH Access for LUM-enabled eDirectory Users	95
12	Network Services	99
12.1	TCP/IP	99
12.1.1	Coexistence and Migration Issues.	99
12.2	DNS and DHCP	99
12.2.1	DNS Differences Between NetWare and OES 2	100
12.2.2	DHCP Differences Between NetWare and OES 2.	101
12.3	Time Services	101
12.3.1	Overview of Time Synchronization	102
12.3.2	Planning for Time Synchronization	105
12.3.3	Coexistence and Migration of Time Synchronization Services	108
12.3.4	Implementing Time Synchronization	110
12.3.5	Configuring and Administering Time Synchronization	111
12.3.6	Daylight Saving Time.	112
12.4	Discovery Services.	112
12.4.1	Novell SLP and OpenSLP	112
12.4.2	WinSock and Discovery Is NetWare only	113
12.4.3	UDDI and Discovery	113
12.4.4	CIMOM and Discovery.	113
12.5	SLP	113
12.5.1	Why SLP Is Needed	113
12.5.2	Comparing Novell SLP and OpenSLP.	114
12.5.3	Setting Up OpenSLP on OES 2 Networks.	115
12.5.4	Using Novell SLP on OES 2 Networks	119
13	Storage and File Systems	123
13.1	Overview of OES 2 Storage	123
13.1.1	Databases	123
13.1.2	iSCSI	124
13.1.3	File System Support in OES	124
13.1.4	Storage Basics by Platform	126
13.1.5	Storage Options.	126
13.1.6	NetWare Core Protocol Support (Novell Client Support) on Linux	128
13.2	Planning OES File Storage	128
13.2.1	Directory Structures	128
13.2.2	File Service Support Considerations	129
13.2.3	General Requirements for Data Storage	129
13.2.4	OES 2 Storage Planning Considerations.	129

13.2.5	NSS Planning Considerations	134
13.3	Coexistence and Migration of Storage Services	135
13.3.1	MySQL	135
13.3.2	OES 2 Options	135
13.3.3	NetWare 6.5 SP8 Options	136
13.4	Configuring and Maintaining Storage	136
13.4.1	Managing Directories and Files	137
13.4.2	Managing NSS	137
13.4.3	Optimizing Storage Performance	138
14	eDirectory, LDAP, and Domain Services for Windows	139
14.1	Overview of Directory Services	139
14.2	eDirectory	140
14.2.1	Installing and Managing eDirectory on OES	140
14.2.2	Planning Your eDirectory Tree	141
14.2.3	eDirectory Coexistence and Migration	141
14.3	LDAP (eDirectory)	141
14.3.1	Overview of eDirectory LDAP Services	142
14.3.2	Planning eDirectory LDAP Services	142
14.3.3	Migration of eDirectory LDAP Services	142
14.3.4	eDirectory LDAP Implementation Suggestions	142
14.4	Domain Services for Windows	142
14.4.1	Graphical Overview of DSfW	143
14.4.2	Planning Your DSfW Implementation	146
14.4.3	Implementing DSfW on Your Network	146
15	Users and Groups	149
15.1	Creating Users and Groups	149
15.2	Linux User Management: Access to Linux for eDirectory Users	149
15.2.1	Overview	150
15.2.2	Planning	155
15.2.3	LUM Implementation Suggestions	155
15.3	Identity Management Services	158
15.4	Using the Identity Manager 3.6.1 Bundle Edition	158
15.4.1	What Am I Entitled to Use?	159
15.4.2	System Requirements	159
15.4.3	Installation Considerations	159
15.4.4	Getting Started	159
15.4.5	Activating the Bundle Edition	160
16	Access Control and Authentication	163
16.1	Controlling Access to Services	163
16.1.1	Overview of Access Control	163
16.1.2	Planning for Service Access	169
16.1.3	Coexistence and Migration of Access Services	172
16.1.4	Access Implementation Suggestions	172
16.1.5	Configuring and Administering Access to Services	172
16.2	Authentication Services	174
16.2.1	Overview of Authentication Services	174
16.2.2	Planning for Authentication	177
16.2.3	Authentication Coexistence and Migration	177
16.2.4	Configuring and Administering Authentication	177

17 File Services 179

17.1	Overview of File Services	179
17.1.1	Using the File Services Overviews	180
17.1.2	FTP Services	180
17.1.3	NetWare Core Protocol	180
17.1.4	NetStorage.	181
17.1.5	Novell AFP.	184
17.1.6	Novell CIFS	185
17.1.7	Novell iFolder 3.8.	186
17.1.8	Novell Samba	188
17.2	Planning for File Services	189
17.2.1	Deciding Which Components Match Your Needs	189
17.2.2	Comparing Your CIFS File Service Options	190
17.2.3	Planning Your File Services.	192
17.3	Coexistence and Migration of File Services.	193
17.3.1	Novell Client (NCP)	193
17.3.2	NetStorage.	194
17.3.3	Novell AFP.	194
17.3.4	Novell CIFS	194
17.3.5	Novell iFolder 3.8.	194
17.3.6	Samba	194
17.4	Aligning NCP and POSIX File Access Rights	195
17.4.1	Managing Access Rights	195
17.4.2	Providing a Private Work Directory	196
17.4.3	Providing a Group Work Area	197
17.4.4	Providing a Public Work Area	197
17.4.5	Setting Up Rights Inheritance	198
17.5	PureFTP Remote Access Implementation	198
17.5.1	Configuring FTP.	199
17.5.2	Path Formats	199
17.5.3	SITE Command	200
17.6	NCP Implementation and Maintenance	200
17.6.1	The Default NCP Volume	201
17.6.2	Creating NCP Home and Data Volume Pointers	201
17.6.3	Assigning File Trustee Rights	201
17.6.4	NCP Caveats	201
17.6.5	NCP Maintenance	202
17.7	NetStorage Implementation and Maintenance.	202
17.7.1	About Automatic Access and Storage Locations.	202
17.7.2	About SSH Storage Locations.	202
17.7.3	Assigning User and Group Access Rights.	202
17.7.4	Authenticating to Access Other Target Systems	203
17.7.5	NetStorage Authentication Is Not Persistent by Default	203
17.7.6	NetStorage Maintenance	204
17.8	Novell AFP Implementation and Maintenance.	204
17.8.1	Implementing Novell AFP File Services.	204
17.8.2	Maintaining Novell AFP File Services	204
17.9	Novell CIFS Implementation and Maintenance	204
17.9.1	Implementing Novell CIFS File Services	204
17.9.2	Maintaining Novell CIFS File Services.	205
17.10	Novell iFolder 3.8 Implementation and Maintenance.	205
17.10.1	Managing Novell iFolder 3.8	205
17.10.2	Configuring Novell iFolder 3.8 Servers	205
17.10.3	Creating and Enabling Novell iFolder 3.8 Users	205
17.10.4	Novell iFolder 3.8 Maintenance	206
17.11	Samba Implementation and Maintenance	206

17.11.1	Implementing Samba File Services	206
17.11.2	Maintaining Samba File Services	206
18	Search Engine (QuickFinder)	207
19	Print Services	209
19.1	Overview of Print Services	209
19.1.1	Using This Overview	209
19.1.2	iPrint Components	210
19.1.3	iPrint Functionality	210
19.2	Planning for Print Services	211
19.3	Coexistence and Migration of Print Services	212
19.4	Print Services Implementation Suggestions	212
19.4.1	Initial Setup	212
19.4.2	Implementation Caveats	213
19.4.3	Other Implementation Tasks	213
19.5	Print Services Maintenance Suggestions	214
20	Web Services	215
21	Security	217
21.1	Overview of OES Security Services	217
21.1.1	Application Security (AppArmor)	217
21.1.2	NSS Auditing Engine	217
21.1.3	Encryption (NICI)	218
21.1.4	General Security Issues	219
21.2	Planning for Security	219
21.2.1	Comparing the Linux and the Novell Trustee File Security Models	219
21.2.2	User Restrictions: Some OES 2 Limitations	221
21.3	Configuring and Administering Security	221
21.4	Links to Product Security Considerations	221
21.5	Links to Anti-Virus Partners	223
22	Certificate Management	225
22.1	Overview	225
22.1.1	SLES Default Certificates	225
22.1.2	OES 2 Certificate Management	226
22.1.3	Multiple Trees Sharing a Common Root	228
22.2	Setting Up Certificate Management	228
22.2.1	Setting Up Automatic Certificate Maintenance	228
22.2.2	Eliminating Browser Certificate Errors	228
22.3	If You Don't Want to Use eDirectory Certificates	230
A	Adding Services to OES 2 Servers	233
B	Changing an OES 2 Server's IP Address	235
B.1	Caveats and Disclaimers	235
B.2	Prerequisites	235
B.2.1	General	235
B.2.2	iPrint	236

B.2.3	Clustering	236
B.3	Changing the Server's Address Configuration	236
B.4	Reconfiguring the OES Services	236
B.5	Repairing the eDirectory Certificates	237
B.6	Completing the Server Reconfiguration	237
B.6.1	QuickFinder	238
B.6.2	DHCP	238
B.6.3	DSfW	238
B.6.4	iPrint	240
B.6.5	NetStorage	241
B.7	Modifying a Cluster	241
B.8	Reconfiguring Services on Other Servers That Point to This Server	241
C	Updating/Patching OES 2 Servers	243
D	Backup Services	245
D.1	Services for End Users	245
D.2	System-Wide Services	245
D.2.1	Links to Backup Partners	245
D.2.2	Novell Storage Management Services (SMS)	245
D.2.3	SLES 10 Backup Services	246
E	Quick Reference to OES 2 User Services	247
F	OES 2 SP2 Browser Support	249
G	Client/Workstation OS Support	251
H	OES 2 Service Scripts	253
I	System User and Group Management in OES 2 SP2	257
I.1	About System Users and Groups	257
I.1.1	Types of OES System Users and Groups	257
I.1.2	OES System Users and Groups by Name	258
I.2	Understanding Proxy Users	259
I.2.1	What Are Proxy Users?	260
I.2.2	Why Are Proxy Users Needed on OES?	260
I.2.3	Which Services Require Proxy Users and Why?	260
I.2.4	What Rights Do Proxy Users Have?	261
I.3	Planning Your Proxy Users	264
I.3.1	About Proxy User Creation	264
I.3.2	Proxy User Impacts on User Connection Licenses	267
I.3.3	Limiting the Number of Proxy Users in Your Tree	267
I.3.4	Proxy Users and Passwords	269
I.4	Implementing Your Proxy User Plan	271
I.4.1	Tree-Wide Proxy Users	271
I.4.2	Service-Specific Proxy Users	271
I.4.3	Partition-Wide Proxy Users	272
I.4.4	Server-Wide Proxy User	272
I.4.5	Individual Proxy User Per-Server-Per-Service	272
I.5	Proxy Users and Domain Services for Windows	272

I.6	System Users	272
I.7	System Groups	274
I.8	Auditing System Users	275
J	Administrative Users in OES 2 SP2	277
K	Coordinating Password Policies Among Multiple File Services	279
K.1	Overview	279
K.2	Concepts and Prerequisites	279
K.2.1	Prerequisites for File Service Access	279
K.2.2	eDirectory contexts	280
K.2.3	Password Policies and Assignments	280
K.3	Examples	281
K.3.1	Example 1: Complex Mixed Tree with a Mix of File Access Services and Users from across the Tree	281
K.3.2	Example 2: Mutually Exclusive Users	282
K.4	Deployment Guidelines for Different Servers and Deployment Scenarios	283
K.4.1	Deployment Scenario 1: Complex Mixed Scenario with a Mix of File Access Services	284
K.4.2	Deployment Scenario 2: Mutually /Exclusive Users	286
K.4.3	Deployment Scenario 3: Simple deployments	286
K.4.4	Modifying User Password Policies after AFP/CIFS/Samba/DSfW Is Installed	286
K.4.5	Adding New User eDirectory Contexts to AFP/CIFS after AFP/CIFS/Samba/DSfW Is Installed.	287
K.4.6	Enabling File Access for DSfW Servers Across Domains	287
L	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 *OES 2 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 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 SP2 are both used in this guide. Generally, OES 2 SP2 is used to differentiate something that is new or changed for the SP2 release of OES 2. Unless otherwise indicated, all statements that refer to OES 2 also apply to OES 2 SP2 unless otherwise indicated.

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 or Changed

1

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

- ♦ [Section 1.1, “Where’s NetWare?,” on page 17](#)
- ♦ [Section 1.2, “Links to What's New Sections,” on page 17](#)
- ♦ [Section 1.3, “New or Changed in OES 2 SP2,” on page 19](#)
- ♦ [Section 1.4, “New in OES 2 SP1,” on page 20](#)
- ♦ [Section 1.5, “New in OES 2 \(Initial Release\),” on page 23](#)

1.1 Where’s NetWare?

Novell® Open Enterprise Server 2 SP2 does not include NetWare®. Anyone who wants to deploy NetWare in an OES 2 SP2 environment should download NetWare 6.5 SP8 from the [Novell download site](http://download.novell.com/Download?buildid=dpIR3H1ymhk~) (<http://download.novell.com/Download?buildid=dpIR3H1ymhk~>).

1.1.1 NetWare References in This Guide and Elsewhere

Because many organizations are transitioning their network services from NetWare to OES, information to assist with upgrading from NetWare to OES 2 is included in this guide and in the OES 2 SP2 documentation set—especially in the [OES 2 SP2: Upgrading to OES—Best Practices Guide](#).

1.1.2 NetWare Documentation

For NetWare documentation, including installation and configuration instructions, see the [NetWare 6.5 SP8 Online Documentation Web site](http://www.novell.com/documentation/nw65) (<http://www.novell.com/documentation/nw65>).

1.2 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 User Guide
DHCP	Administration Guide
Distributed File Services	Administration Guide
DNS	Administration Guide

Product	Link to What's New Section
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/be1l5dw.html)
iManager 2.7	Administration Guide
Installation	Installation Guide
iPrint	Administration Guide
Migration Tool	Administration Guide
NCP Server for OES 2	Administration Guide
NetStorage	Administration Guide
Novell AFP	Administration Guide
Novell CIFS	Administration Guide
Novell Client™	Linux Windows XP/2003 Administration Guide Windows Vista* Administration Guide
Novell Cluster Services™ (High Availability)	Administration Guide
Novell iFolder® 3.8	Administration Guide User Guide
Novell Remote Manager	Administration Guide
Novell Storage Services (NSS)	Administration Guide
OES 2	Installation Guide
OpenWBEM	Administration Guide
QuickFinder™ 5	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 86.
Shadow Volumes	See “Overview of Dynamic Storage Technology” in the <i>OES 2 SP2: Dynamic Storage Technology Administration Guide</i> .
Storage Management Services (SMS)	Administration Guide
Virtualization (Xen*)	Virtualization Overview

1.3 New or Changed in OES 2 SP2

This section summarizes the new features introduced in Novell® Open Enterprise Server (OES) 2 SP2 that either involve multiple services or are not covered in service-specific documentation. For information on service-specific new features, see [Section 1.2, “Links to What's New Sections,” on page 17](#).

- ♦ [Section 1.3.1, “Auditing,” on page 19](#)
- ♦ [Section 1.3.2, “Base Platform Is SLES 10 SP3,” on page 19](#)
- ♦ [Section 1.3.3, “CIFS DFS Support,” on page 19](#)
- ♦ [Section 1.3.4, “Create EVMS Proposal Option,” on page 19](#)
- ♦ [Section 1.3.5, “Cross-Protocol File Locking Change,” on page 20](#)
- ♦ [Section 1.3.6, “Domain Services for Windows Installation,” on page 20](#)
- ♦ [Section 1.3.7, “Java Console for DNS/DHCP,” on page 20](#)
- ♦ [Section 1.3.8, “Performance Increases,” on page 20](#)
- ♦ [Section 1.3.9, “PureFTP,” on page 20](#)
- ♦ [Section 1.3.10, “Upgrading Online,” on page 20](#)
- ♦ [Section 1.3.11, “Windows 7 Client Support,” on page 20](#)

1.3.1 Auditing

OES 2 SP2 includes support for third-party developers to create auditing products. For more information, see [Section 21.1.2, “NSS Auditing Engine,” on page 217](#).

1.3.2 Base Platform Is SLES 10 SP3

- ♦ With the release of OES 2 SP2, the Linux platform on which OES services run is changed from SUSE® Linux Enterprise Server (SLES) 10 SP2 to SLES 10 SP3 and includes Tomcat 5.5.

1.3.3 CIFS DFS Support

This has been added in OES 2 SP2.

1.3.4 Create EVMS Proposal Option

The Partitioner in the YaST Install offers an option to “Create an EVMS Proposal.”

For unpartitioned devices over 20 GB in size, this option creates a boot partition and a container for the `swap` and `/` (root) volumes in up to the first 20 GB, and leaves the remainder of the space on the device as unpartitioned free space. The default `/` partition size is 10 GB. The swap size is 1 GB or larger, depending on the amount of RAM the server has.

IMPORTANT: This option applies only if you are installing an NSS volume on the same disk as your Linux root (`/`) partition.

1.3.5 Cross-Protocol File Locking Change

Starting with OES 2 SP2, cross-protocol file locking (CPL) is enabled by default as follows:

- ♦ All new servers with NCP installed have CPL turned on.
- ♦ If an upgraded server was not configured for CPL prior to the upgrade, CPL will be turned on.
- ♦ If an upgraded server was configured for CPL prior to the upgrade, the CPL setting immediately preceding the upgrade is retained.

If a server is only accessed through NCP (AFP and CIFS are not installed), you can achieve an NCP performance gain of about 10%. However, there is a critical caveat. If you later install AFP or CIFS and you forget to re-enable CPL, data corruption can occur.

There are also obvious implications for clustering because the CPL settings for clustered nodes must match. For example, if an unmodified OES 2 SP1 node is clustered with an unmodified OES 2 SP2 node, their CPL settings will conflict and one of the nodes must be modified.

For more information about cross-protocol locking, see [“Configuring Cross-Protocol File Locks for NCP Server”](#) in the *OES 2 SP2: NCP Server for Linux Administration Guide*.

1.3.6 Domain Services for Windows Installation

The DSfW installation has been rearchitected with a focus on usability and simplicity.

1.3.7 Java Console for DNS/DHCP

The Java Console for DNS/DHCP management is now available for Linux.

1.3.8 Performance Increases

AFP, NCP, and Samba all have improved performance in OES 2 SP2.

1.3.9 PureFTP

Gateway parity with NetWare.

1.3.10 Upgrading Online

Support for upgrading through the SP Channel is included. For more information, see [“Using the Patch Channel to Upgrade \(Online\)”](#) in the *OES 2 SP2: Installation Guide*.

1.3.11 Windows 7 Client Support

OES 2 SP2 service clients are supported on Windows 7.

1.4 New in OES 2 SP1

- ♦ [Section 1.4.1, “YaST Install Changes,” on page 21](#)
- ♦ [Section 1.4.2, “Novell AFP,” on page 21](#)

- ♦ [Section 1.4.3, “Novell CIFS,” on page 21](#)
- ♦ [Section 1.4.4, “Novell Domain Services for Windows,” on page 22](#)
- ♦ [Section 1.4.5, “Migration Tool,” on page 22](#)

1.4.1 YaST Install Changes

The default behavior of the option to use eDirectory™ certificates for HTTPS services 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 230](#).

1.4.2 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. 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 SP2: Novell AFP For Linux Administration Guide](#).

1.4.3 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 SP2: Novell CIFS for Linux Administration Guide](#).

1.4.4 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 SP2 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 SP2: Domain Services for Windows Administration Guide](#).

1.4.5 Migration Tool

The new OES 2 SP2 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 SP2: Migration Tool Administration Guide](#).

1.5 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 1.4, “New in OES 2 SP1,” on page 20](#).

- ♦ [Section 1.5.1, “Dynamic Storage Technology,” on page 23](#)
- ♦ [Section 1.5.2, “OES 2 Migration Tools,” on page 23](#)
- ♦ [Section 1.5.3, “Xen Virtualization Technology,” on page 23](#)

1.5.1 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 Novell Storage Services (NSS) volumes on the same or different servers.

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 123](#) and the *OES 2 SP2: Dynamic Storage Technology Administration Guide*.

1.5.2 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.

For more information, see [Chapter 8, “Migrating and Consolidating Existing Servers and Data,” on page 75](#).

1.5.3 Xen Virtualization Technology

Both OES 2 and NetWare 6.5 SP8 can run in virtual machines on either an OES 2 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.

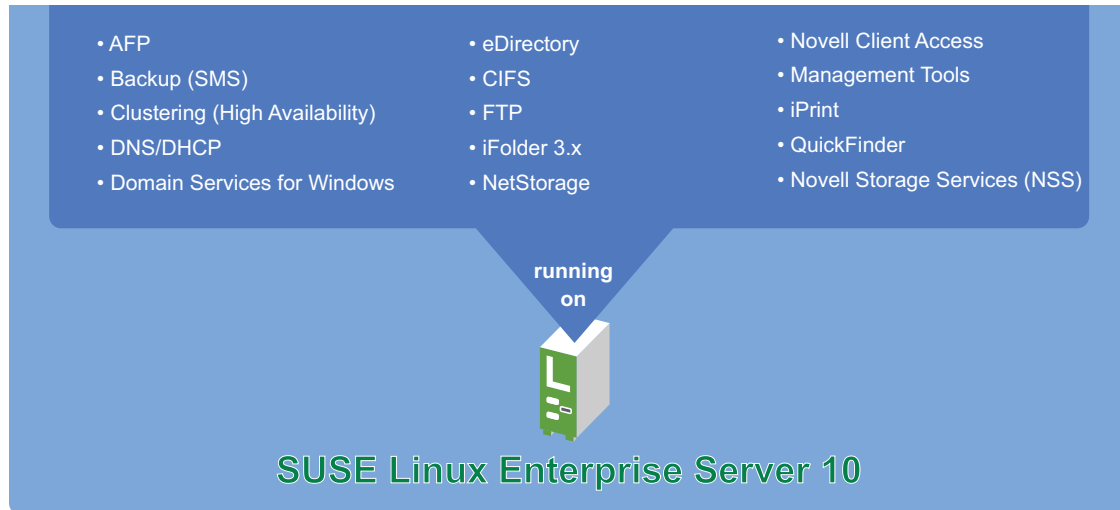
For more information, see [Chapter 9, “Virtualization in OES 2,” on page 77](#).

Welcome to Open Enterprise Server 2

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, see [Table 3-1, “Service Comparison Between NetWare 6.5 SP8 and OES 2 SP2 Linux,”](#) on page 27.

Planning Your OES 2 Implementation

3

As you plan which OES services to install, 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 27
- ♦ Section 3.2, “Which Services Do I Need?,” on page 34
- ♦ Section 3.3, “Exploring OES 2 services,” on page 34
- ♦ Section 3.4, “Plan for eDirectory,” on page 34
- ♦ Section 3.5, “Prepare Your Existing eDirectory Tree for OES 2,” on page 35
- ♦ Section 3.6, “Identify a Purpose for Each Server,” on page 35
- ♦ Section 3.7, “Understand Server Requirements,” on page 35
- ♦ Section 3.8, “Understand User Restrictions and Linux User Management,” on page 36
- ♦ Section 3.9, “Caveats to Consider Before You Install,” on page 36
- ♦ Section 3.10, “Consider Coexistence and Migration Issues,” on page 48
- ♦ Section 3.11, “Understand Your Installation Options,” on page 49

3.1 What Services Are Included in OES 2?

Table 3-1 summarizes OES services 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 SP2 Linux

Service	NetWare 6.5 SP8	OES 2	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 are proprietary and tightly integrated with eDirectory™ and Novell Storage Services (NSS).

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
Apache Web Server	Yes - NetWare® port of open source product	Yes - Standard Linux	Administration Instance vs. Public Instance on NetWare (http://www.novell.com/documentation/oes2/web_apache_nw/data/aipcu6x.html#aipcu6x). What's Different about Apache on NetWare (http://www.novell.com/documentation/oes2/web_apache_nw/data/ail8hvj.html).
Archive and Version Services (Novell)	Yes	Yes	Setup varies slightly, but there are no functional differences.
Backup (SMS) ♦ SMS ♦ NSS-Xattr	Yes	Yes	SMS provides backup applications with a framework to develop complete backup and restore solutions. For information, see the OES 2 SP2: Storage Management Services Administration Guide. NSS provides extended attribute handling options for NSS on Linux. For information, see “Using Extended Attributes (xAttr) Commands (Linux)” in the OES 2 SP2: NSS File System Administration Guide.
CIFS (Windows File Services)	Yes - NFAP	Yes - Novell CIFS and Novell Samba	Both NFAP and Novell CIFS are Novell proprietary and tightly integrated with eDirectory and Novell Storage Services (NSS). Samba is an open source product distributed with SUSE® Linux Enterprise Server (SLES). 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.
Clustering	Yes	Yes	“Product Features” in the OES 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide. “Product Features” in the NW6.5 SP8: Novell Cluster Services 1.8.5 Administration Guide.
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.

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
DHCP	Yes	Yes	For a comparison between what is available on OES 2 and NetWare, see Section 12.2.2, “DHCP Differences Between NetWare and OES 2,” on page 101. To plan your DHCP implementations, see “Planning a DHCP Strategy” in the <i>OES 2 SP2: Novell DNS/DHCP Administration Guide for Linux</i> and “Planning a DHCP Strategy” in the <i>NW 6.5 SP8: Novell DNS/DHCP Services Administration Guide</i>.
DNS	Yes	Yes	For a comparison between what is available on OES 2 and NetWare, see Section 12.2.1, “DNS Differences Between NetWare and OES 2,” on page 100. See “Planning a DNS Strategy” in the <i>OES 2 SP2: Novell DNS/DHCP Administration Guide for Linux</i> and “Planning a DNS Strategy” in the <i>NW 6.5 SP8: Novell DNS/DHCP Services Administration Guide</i>.
Dynamic Storage Technology	No	Yes	DST runs on OES 2. 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.
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).
FTP Server	Yes	Yes	Support for eDirectory LDAP authentication has been added to PureFTP on OES 2. The FTP/SFTP gateway available on NetWare is not currently available on Linux. See Section 17.1.2, “FTP Services,” on page 180. See “Features of the NetWare FTP Server” in the <i>NW 6.5 SP8: Novell FTP Administration Guide</i>.

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
Health Monitoring Services	Yes	Yes	The Health Monitoring Server, which was included in OES 1, has been removed in OES 2. This is now available in various Novell Remote Manager dialog boxes on both platforms. For more information, see “Health Monitoring Services” on page 86.
Identity Manager 3.6.1 Bundle Edition	No	Yes	IDM 3.6.1 is not available on NetWare.
iPrint	Yes	Yes	See “Overview” in the <i>OES 2 SP2: iPrint for Linux Administration Guide</i> , and “Overview” in the <i>NW 6.5 SP8: iPrint Administration Guide</i> .
IPX™ (Internetwork Packet Exchange™) from Novell	Yes	No	Novell has no plans to port IPX to OES.
iSCSI	Yes	Yes	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 integrated with NetWare Remote Manager management. You use YaST management tools instead. On the other hand, the iSCSI implementation for Linux is newer and performs better. See Linux-iSCSI Project on the Web (http://linux-iscsi.sourceforge.net). See “Overview” in the <i>NW 6.5 SP8: iSCSI 1.1.3 Administration Guide</i>.
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.
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>NW 6.5 SP8: Novell MySQL Administration Guide</i>.

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
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 SP2: NCP Server for Linux Administration Guide</i>.
NCP Server	Yes	Yes	NCP services are native to NetWare 6.5 and NSS volumes; to have NCP services on OES, the NCP Server must be installed. See “Benefits of NCP Server” in the <i>OES 2 SP2: 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 181.
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>NW 6.5 SP8: AFP, CIFS, and NFS (NFAP) Administration Guide</i> .
NICI (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. However, the Novell Audit 2.0 Starter pack is available for download at no cost on Novell.com (http://www.novell.com/downloads).
Novell Client™ for Windows and Linux support	Yes	Yes	Novell Client connectivity to OES 2 requires that the NCP Server be installed.
Novell Cluster Services™	Yes	Yes	See “Product Features” in the <i>OES 2 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide</i>. See “Product Features” in the <i>NW6.5 SP8: Novell Cluster Services 1.8.5 Administration Guide</i>.

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
Novell iFolder® 2.x	Yes	No	For migration information, see “ Migrating iFolder 2.x ” in the <i>OES 2 SP2: Migration Tool Administration Guide</i> .
Novell iFolder 3.8	No	Yes	OES 2 SP2 includes Linux, Macintosh*, and Windows clients.
Novell Licensing Services	Yes	No	See Section 4.5.3, “OES 2 Doesn’t Support NLS,” on page 58.
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 SP2: NSS File System Administration Guide</i> .
NTPv3	Yes	Yes	The <code>ntpd.conf</code> file on NetWare can replace an OES 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>NW 6.5 SP8: 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 iPrint .
QuickFinder™	Yes	Yes	See Search .
RADIUS	Yes	Yes	See the information on forge.novell.com (http://forge.novell.com/modules/xfmod/project/?edirfreeradius) .
Samba	No	Yes	Samba is an open source technology available on OES. Novell provides automatic configuration for authentication through eDirectory. For more information, see the <i>OES2 SP2: Samba Administration Guide</i> .

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
Search (QuickFinder)	Yes	Yes	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 novlwww user in the www group has rights to see. 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>.
SLP	Yes - Novell SLP	Yes - OpenSLP	For OES 2, see “SLP Services in the Network” (http://www.novell.com/documentation/sles10/sles_admin/data/cha_slp.html) in the <i>SLES 10 SP3: 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/a2iimc.html). NetWare uses Novell SLP, which provides caching of Directory Agent scope information in eDirectory. This provides for sharing of scope information among DAs. 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.
Software RAIDS (NSS volumes)	Yes (0, 1, 5, 10, 15)	Yes (0, 1, 5)	See “ Understanding Software RAID Devices ” in the <i>OES 2 SP2: NSS File System Administration Guide</i> .
Storage Management Services™ (SMS)	Yes	Yes	No functional differences, except that the SBCON backup engine is not supported on Linux. The nbackup engine is available for exploring SMS capabilities, but in a production environment, you should use a third-party, full-featured backup engine.
TCP/IP	Yes	Yes	No functional differences.
Timesync NLM™	Yes	No	Timesync will not be ported to Linux. However, NTPv3 is available on both Linux and NetWare. See “Time Services” on page 101.

Service	NetWare 6.5 SP8	OES 2	Platform Differences / Migration Issues
Tomcat	Yes	Yes	NetWare includes Tomcat 4 and a Tomcat 5 servlet container for iManager 2.7. OES 2 includes Tomcat 5. There is no impact to any of the OES 2 administration tools, which are tested and supported on both platforms. See " Administration Instance vs. Public Instance on NetWare " (http://www.novell.com/documentation/oes2/web_tomcat_nw/data/ahdyran.html#ahdyran)
Virtual Office (Collaboration)	Yes	No	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).
WAN Traffic Manager	Yes	No	
Xen Virtualization Guest	Yes	Yes	NetWare 6.5 SP8 (and NetWare 6.5 SP 7) can run on a paravirtualized machine. OES 2 can run on a paravirtualized machine or fully virtualized machine.
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 commonly used OES services by following the step-by-step instructions provided in the [OES 2 SP2: Lab Guide for Linux and Virtualized NetWare](#).

3.4 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 141.

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 101](#).
- ♦ **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 *OES 2 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.

3.5 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 “[Preparing to Install NetWare 6.5 SP8](#)” in the *NW65 SP8: Installation Guide*.

3.6 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 and see how it will integrate into your overall network service infrastructure.

3.7 Understand Server Requirements

OES 2 and NetWare 6.5 SP8 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 Server (Physical):** “[Preparing to Install OES 2 SP2](#)” in the *OES 2 SP2: Installation Guide*.
- ♦ **OES 2 Server (Virtual):** “[System Requirements](#)” in the *OES 2 SP2: Installation Guide*.

- ♦ **NetWare 6.5 SP8 Server (Physical):** “[Meeting System Requirements](#)” in the *NW65 SP8: Installation Guide*.
- ♦ **NetWare 6.5 SP8 Server (Virtual):** “[Planning for NetWare VM Guest Servers](#)” in the *OES 2 SP2: Installation Guide*.

3.8 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 Limitations,”](#) on page 221.

3.9 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 3.9.1, “Adding a Linux Node to a Cluster Ends Adding More NetWare Nodes,”](#) on page 37
- ♦ [Section 3.9.2, “Always Double-Check Service Configurations Before Installing,”](#) on page 37
- ♦ [Section 3.9.3, “Back Button Doesn’t Reset Configuration Settings,”](#) on page 37
- ♦ [Section 3.9.4, “Cluster Upgrades Must Be Planned Before Installing OES 2,”](#) on page 37
- ♦ [Section 3.9.5, “Cross-Protocol File Locking Has Changed,”](#) on page 38
- ♦ [Section 3.9.6, “Do Not Create Local \(POSIX\) Users,”](#) on page 38
- ♦ [Section 3.9.7, “Do Not Upgrade to eDirectory 8.8 Separately,”](#) on page 39
- ♦ [Section 3.9.8, “Follow the Instructions for Your Chosen Platforms,”](#) on page 39
- ♦ [Section 3.9.9, “If You’ve Ever Had OES 1 Linux Servers with LUM and NSS Installed,”](#) on page 39
- ♦ [Section 3.9.10, “iFolder 3.8 Considerations,”](#) on page 42
- ♦ [Section 3.9.11, “Incompatible TLS Configurations Give No Warning,”](#) on page 42
- ♦ [Section 3.9.12, “Installing into an Existing eDirectory Tree,”](#) on page 43
- ♦ [Section 3.9.13, “NetWare Caveats,”](#) on page 43
- ♦ [Section 3.9.14, “Novell Distributed Print Services Cannot Migrate to Linux,”](#) on page 44
- ♦ [Section 3.9.15, “NSS Caveats,”](#) on page 44
- ♦ [Section 3.9.16, “Plan eDirectory Before You Install,”](#) on page 45
- ♦ [Section 3.9.17, “Samba Enabling Disables SSH Access,”](#) on page 45
- ♦ [Section 3.9.18, “Unsupported Service Combinations,”](#) on page 45
- ♦ [Section 3.9.19, “VNC Install Fails to Set the IP Address in /etc/hosts,”](#) on page 48

3.9.1 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 SP2: Novell Cluster Services 1.8.7 for Linux Administration Guide*.

3.9.2 Always Double-Check Service Configurations Before Installing

It is critical and you double-check your service configurations on the Novell Open Enterprise Server Configuration summary page before proceeding with an installation. Two reasons for this are explained in [Section 3.9.3, “Back Button Doesn’t Reset Configuration Settings,”](#) on page 37 and

3.9.3 Back Button Doesn’t Reset Configuration Settings

During an installation, after you configure eDirectory and reach the Novell Open Enterprise Server Configuration summary screen, service configuration settings have been “seeded” from the eDirectory configuration.

If you discover at that point that something in the eDirectory configuration needs to change, you can change the settings by clicking the *eDirectory* link on the summary page or by clicking the Back button.

In both cases when you return to the summary page, the eDirectory configuration has changed, but the individual service configurations have the same eDirectory settings you originally entered. These must each be changed manually.

For example, if you specified the wrong server context while initially configuring eDirectory, the NSS and LUM configurations still have the wrong context. You must select each service individually and change the server context in them.

Unless you manually change the services affected by changes to eDirectory, your services will at best not work as expected and at worst completely fail.

3.9.4 Cluster Upgrades Must Be Planned Before Installing OES 2

Because of differences between Novell Cluster Services on NetWare 6.5 SP8 and OES 2, 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 38
- ♦ [“Working with Mixed Node Clusters”](#) on page 38

Service Failover in a Mixed Cluster

The only cluster-enabled service that can fail over cross-platform (run on either OES 2 or NetWare 6.5 SP8) 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 server can fail over to another OES 2 server in the cluster, but the service cannot fail over to a NetWare 6.5 SP8 server.

Working with Mixed Node Clusters

The following points apply to working with mixed NetWare and OES 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.

3.9.5 Cross-Protocol File Locking Has Changed

If you plan to use Novell CIFS, Novell AFP and/or NCP file services in combination with each other, be sure to read “[Cross-Protocol File Locking Change](#)” in the *OES 2 SP2: Planning and Implementation Guide*.

3.9.6 Do Not Create Local (POSIX) Users

During the OES 2 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 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 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 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 149.

3.9.7 Do Not Upgrade to eDirectory 8.8 Separately

If you are running OES 1 SP2, do not upgrade to eDirectory™ 8.8 independently of upgrading to OES 2 SP2.

For example, do not upgrade from eDirectory 8.7.3 to eDirectory 8.8.2 through the oes-edir88 patch channel prior to upgrading to OES 2 SP2. Doing so causes configuration problems that the OES 2 SP2 install is not designed to handle.

3.9.8 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.

3.9.9 If You've Ever Had OES 1 Linux Servers with LUM and NSS Installed

Having NSS volumes on OES 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 SP2,” on page 257](#).

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 39](#)
- ♦ [“An NSS Complication” on page 39](#)
- ♦ [“eDirectory Solves the Basic Problem” on page 40](#)
- ♦ [“ID Mismatches on OES 1” on page 40](#)
- ♦ [“The OES 1 Solution: The nssid.sh Script” on page 40](#)
- ♦ [“OES 2 SP1 or Later Requires a New Approach” on page 40](#)
- ♦ [“The OES 2 Solution: Standardizing the UIDs on all OES servers” on page 40](#)

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 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 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 149](#).

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 or Later Requires a New Approach

Unfortunately, system-level changes in SUSE Linux Enterprise Server 10 SP2 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 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 novlxxregd
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) (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 40](#).

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 40](#).

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 40](#).

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 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.

3.9.10 iFolder 3.8 Considerations

For best results, be sure you read and carefully follow the instructions in the [Novell iFolder 3.8 Administration Guide](#), starting with “[Deploying iFolder Server](#).” This is especially critical if you plan to use NSS for your iFolder 3.8 data volume.

3.9.11 Incompatible TLS Configurations Give No Warning

When you install a new eDirectory tree, the eDirectory Configuration - New or Existing Tree screen has the *Require TLS for Simple Binds with Password* option selected by default. If you keep this configuration setting, the eDirectory LDAP server requires that all communications come through the secure LDAP port that you specified on the eDirectory Configuration - Local Server Configuration screen. By default, this is port 636.

Unfortunately, the OES install doesn't display a warning if you subsequently configure OES services to use non-TLS (non-secure) LDAP communications (port 389). The installation proceeds normally but the service configuration fails.

For example, if you accept the TLS default, then configure Novell DHCP to use non-secure communications (by deselecting the *Use secure channel for configuration* option), the OES install doesn't warn that you have created an incompatible configuration.

After eDirectory and the iManager plug-ins install successfully, the Novell DHCP configuration fails. You must then use iManager to change either the LDAP server configuration or the Novell DHCP configuration to support your preferred communication protocol.

Simply enabling non-TLS LDAP communications doesn't disable TLS. It merely adds support for non-secure communications with the LDAP server.

3.9.12 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 43](#)
- ♦ [“Do Not Add OES to a Server That Is Already Running eDirectory” on page 43](#)
- ♦ [“Be Sure That eDirectory Is Healthy” on page 43](#)
- ♦ [“Be Sure That Network Time Is Synchronized” on page 43](#)
- ♦ [“Be Sure that OpenSLP on OES 2 Is Configured Properly” on page 43](#)

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 [“Preparing eDirectory for OES 2 SP2”](#) in the *OES 2 SP2: 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 NetWare 6.5 SP8 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 101](#).

Be Sure that OpenSLP on OES 2 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 113](#).

3.9.13 NetWare Caveats

- ♦ [“NetWare Licenses and OES 2 Trees” on page 44](#)
- ♦ [“NetWare 6.5 Servers Must Be Running SP3 or Later” on page 44](#)

NetWare Licenses and OES 2 Trees

OES doesn't use Novell Licensing Services ([Section 4.5, "Licensing," on page 57](#)). As a result, OES servers don't need a license container in eDirectory as part of the server installation.

In a mixed OES 2 and NetWare eDirectory tree, at least one NetWare server must hold a replica for each partition where there is a NetWare server object. Without this configuration, it is impossible to install licenses or to service requests from NetWare servers to consume those licenses.

If you need to install a NetWare server in an OES tree, you must do the following after installing the first NetWare server in a partition:

- 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 *NW 6.5 SP8: Licensing Services Administration Guide*.
The iManager Licensing plug-in is not installed on OES servers. If you have configured Role-Based Services, you need to make sure the licensing plug-in is installed and added to the RBS collection. For more information, see ["Upgrading iManager"](#) in the *Novell iManager 2.7 Installation Guide*.

NetWare 6.5 Servers Must Be Running SP3 or Later

If you are installing OES 2 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:

- ♦ **SLP Directory Agents:** If the SLP Directory Agents on your network are not running NetWare 6.5 SP3 or later, installing an OES 2 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 might abend during a schema extension operation.

3.9.14 Novell Distributed Print Services Cannot Migrate to Linux

NDPS® clients are not supported on OES. You must therefore migrate any NDPS clients to iPrint before you migrate your print services to OES. For more information, see ["Migrating NDPS Printers to iPrint"](#) in the *NW 6.5 SP8: iPrint Administration Guide*.

3.9.15 NSS Caveats

- ♦ ["About New Media Support and Clusters"](#) on page 45
- ♦ ["Removable Media Cannot Be Mounted on OES 2"](#) on page 45

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 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 until you have upgraded the node to OES 2.

Removable Media Cannot Be Mounted on OES 2

CD and DVD media and image files cannot be mounted as NSS volumes on OES; 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 SP2: NSS File System Administration Guide*.

3.9.16 Plan eDirectory Before You Install

Although the default eDirectory settings work for simple trees, they are not usually practical for a production implementation. For example, by default the tree Admin user and the server are installed in the same context.

Some administrators, when they discover that the tree structure doesn't meet their needs, assume they can rectify the situation by uninstalling and then reinstalling eDirectory. This simply cannot be done.

In fact, OES services cannot be uninstalled. For more information, see “[Disabling OES 2 Services](#)” in the *OES 2 SP2: Installation Guide*.

3.9.17 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,” on page 93](#).

3.9.18 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 3-2](#) cause pattern conflict warnings, Novell does not support any of them.

Table 3-2 *Unsupported Service Combinations*

Service	Unsupported on the Same Server
Novell AFP	◆ File Server (Samba) ◆ Netatalk ◆ Novell Domain Services for Windows ◆ Novell Samba ◆ Xen Virtual Machine Host Server

Service	Unsupported on the Same Server
Novell Archive and Version Services	◆ Novell Domain Services for Windows (DSfW) ◆ Xen Virtual Machine Host Server
Novell Backup / Storage Management Services	No restrictions
Novell CIFS	◆ File Server (Samba) ◆ Novell Domain Services for Windows ◆ Novell Samba ◆ Xen Virtual Machine Host Server
Novell Cluster Services (NCS)	◆ High Availability ◆ Novell Domain Services for Windows DSfW can actually be installed and run on the same server as NCS, but DSfW cannot run as a clustered service.
Novell DHCP	◆ Xen Virtual Machine Host Server
Novell DNS	◆ DHCP and DNS Server ◆ Xen Virtual Machine Host Server
Novell Domain Services for Windows	◆ File Server (Samba) ◆ Novell AFP ◆ Novell Archive and Version Services ◆ Novell CIFS ◆ Novell Cluster Services (NCS) NCS can actually be installed and run on the server, but DSfW cannot run as a clustered service. ◆ Novell FTP ◆ Novell iFolder ◆ Novell NetStorage ◆ Novell Pre-Migration Server ◆ Novell QuickFinder ◆ Novell Samba ◆ Xen Virtual Machine Host Server
Novell eDirectory	◆ Directory Server (LDAP) ◆ Xen Virtual Machine Host Server
Novell FTP	◆ Novell Domain Services for Windows ◆ Xen Virtual Machine Host Server
Novell iFolder	◆ Novell Domain Services for Windows ◆ Xen Virtual Machine Host Server
Novell iManager	◆ Xen Virtual Machine Host Server

Service	Unsupported on the Same Server
Novell iPrint	♦ Print Server (CUPS) CUPS components are actually installed, but CUPS printing is disabled. For more information, see Section 6.8.6, "iPrint Disables CUPS Printing on the OES 2 Server," on page 67. ♦ Xen Virtual Machine Host Server
Novell Linux User Management (LUM)	No restrictions
Novell NCP Server / Dynamic Storage Technology	♦ Xen Virtual Machine Host Server
Novell NetStorage	♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell Pre-Migration Server	♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell QuickFinder	♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell Remote Manager (NRM)	♦ Xen Virtual Machine Host Server
Novell Samba	♦ File Server (Samba) ♦ Novell CIFS ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell Storage Services (NSS)	♦ Xen Virtual Machine Host Server

Service	Unsupported on the Same Server
Xen Virtual Machine Host Server	◆ 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)

3.9.19 VNC Install Fails to Set the IP Address in /etc/hosts

If you install through a VNC connection, the `/etc/hosts` file is configured with a loop back address assigned to the hostname. This can cause problems with services.

Using a text editor, modify `/etc/hosts` so that the hostname is associated with its actual IP address.

3.10 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.

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 75](#).

3.11 Understand Your Installation Options

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

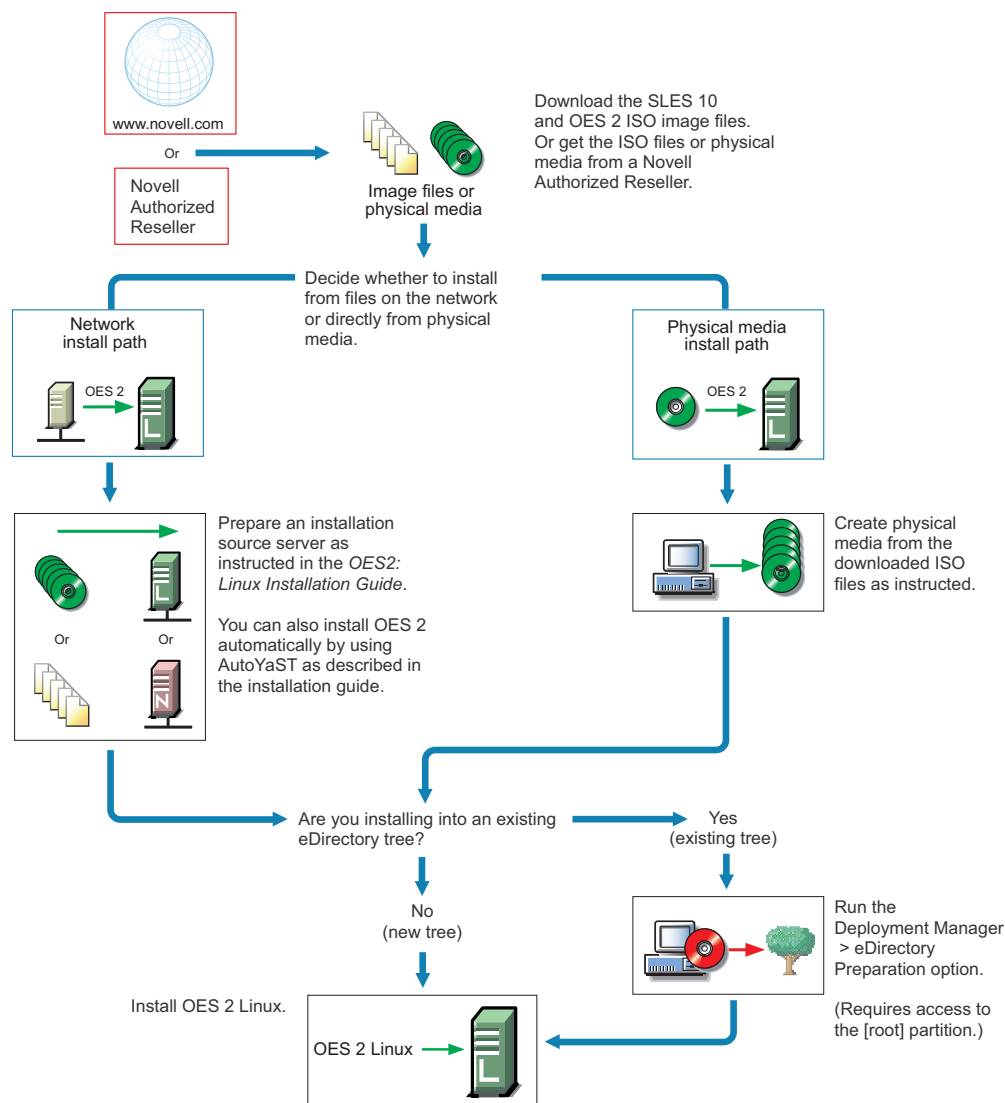
- ♦ [Section 3.11.1, “OES 2 Installation Overview,” on page 49](#)
- ♦ [Section 3.11.2, “About Your Installation Options,” on page 50](#)
- ♦ [Section 3.11.3, “Use Predefined Server Types \(Patterns\) When Possible,” on page 51](#)
- ♦ [Section 3.11.4, “If You Want to Install in a Lab First,” on page 51](#)
- ♦ [Section 3.11.5, “If You Want to Install NSS on a Single-Drive Linux Server,” on page 52](#)

3.11.1 OES 2 Installation Overview

The software and network preparation processes required to install OES 2 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 referred to in the following illustration.

Figure 3-1 OES 2 Install Preparation



For detailed instructions, see “[Setting Up an Installation Source](#)” in the *OES 2 SP2: Installation Guide*.

3.11.2 About Your Installation Options

As illustrated in the previous section, OES 2 lets you install from either physical media or from files on the network.

- ♦ “[OES 2 Options](#)” on page 51
- ♦ “[Virtual Machine Installation Options](#)” on page 51

OES 2 Options

OES 2 includes numerous installation options as documented in the [OES 2 SP2: Installation Guide](#).

- ♦ **CD/DVD Install:** You can install SLES 10 SP1 by using CDs or a DVD and then install OES 2 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 SP2: 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 SP2: 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 Servers](#)” in the [OES 2 SP2: Installation Guide](#).

Virtual Machine Installation Options

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

- ♦ “[Installing, Upgrading, or Updating OES on a Xen-based VM](#)” in the [OES 2 SP2: Installation Guide](#)
- ♦ “[Installing and Managing NetWare on a Xen-based VM](#)” in the [OES 2 SP2: Installation Guide](#)

3.11.3 Use Predefined Server Types (Patterns) When Possible

Both OES 2 and NetWare 6.5 SP8 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:** “[OES Services Pattern Descriptions](#)” in the [OES 2 SP2: Installation Guide](#)
- ♦ **NetWare 6.5 SP8:** “[Choosing a Server Pattern](#)” in the [NW65 SP8: Installation Guide](#)

3.11.4 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 [OES 2 SP2: Lab Guide for Linux and Virtualized NetWare](#) walks you through installing and exploring all the basic OES 2 services.

3.11.5 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 with EVMS as the Volume Manager of the System Device](#)” in the *OES 2 SP2: Installation Guide*.

Getting and Preparing OES 2 Software

4

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?,” 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 57](#)

If you have not already done so, we recommend that you review the information in [Section 3.11, “Understand Your Installation Options,” on page 49](#).

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?

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

OES 2 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 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 SP2 Version	SLES 10 SP3	Server Hardware	Notes
32-bit (i386)	32-bit (i386)	32-bit	The 32-bit version of OES 2 SP2 requires the 32-bit version of SLES 10 SP3.
		64-bit	If you plan to install 64-bit SLES, you should also install 64-bit OES. 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 and is not supported. 32-bit software (OES and SLES) can be installed on either 32-bit or 64-bit hardware.
64-bit (x86_64)	64-bit (x86_64)	64-bit	The 64-bit version of OES 2 SP2 requires the 64-bit version of SLES 10 SP3, 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 (one for OES 2 services and one for SUSE Linux Enterprise Server 10). Both codes are required for registering an OES 2 system in the Novell Customer Center. After it is registered, your server can receive online updates, including the latest support pack.

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 57](#).

After completing your purchase, the installation process goes more smoothly if you understand your installation options. If you haven’t already done so, be sure to review the information in [Section 3.11, “Understand Your Installation Options,” on page 49](#) and then skip to [Chapter 5, “Installing OES 2,” on page 59](#).

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 SP2 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 56](#)

- [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 57](#)

4.4.1 Understanding OES 2 Software Evaluation Basics

You can evaluate the full OES 2 product. 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.

Briefly, the evaluation period for OES 2 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.

4.4.2 Downloading OES 2 SP2 Software from the Novell Web Site

If you already have OES 2 SP2 ISO image files, skip to [Section 4.4.3, “Preparing the Installation Media,” on page 56](#).

If you have OES 2 SP2 product media (CDs and DVDs), skip to [Section 4.4.4, “Installing OES 2 for Evaluation Purposes,” on page 56](#).

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 SP2*, then click the *Open Enterprise Server 2 SP2 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 from files on your network, see the instructions in “[Preparing a Network Installation Source](#)” in the *OES 2 SP2: 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 SP2: Installation Guide*.

### 4.4.4 Installing OES 2 for Evaluation Purposes

If you followed the instructions in [Section 4.4.2, “Downloading OES 2 SP2 Software from the Novell Web Site,” on page 55](#), you now have two activation/evaluation codes: one for OES 2 and another for SLES 10. As you install OES 2, you should register with the Novell Customer Center and use these codes to enable your server for online updates from the OES 2 and SLES 10 patch channels.

---

**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 SP2: Installation Guide*.

The evaluation period begins when the codes are issued. Use the same activation codes for each OES 2 server you install during the evaluation period.

### 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 and virtualized NetWare on a second OES 2 virtual machine host 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 *OES 2 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 SP2: 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 57](#)
- ♦ [Section 4.5.2, “SLES Licensing Entitlements in OES 2,” on page 58](#)
- ♦ [Section 4.5.3, “OES 2 Doesn’t Support NLS,” on page 58](#)

### 4.5.1 The OES 2 Licensing Model

The only OES 2 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 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 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, 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.

To report piracy and infringement violations, please call 1-800-PIRATES (800-747-2837) or send e-mail to [pirates@novell.com](mailto: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 SLES Licensing Entitlements in OES 2**

SUSE Linux Enterprise Server (SLES) entitlements in OES 2 have changed. For more information, refer to the [EULA \(http://www.novell.com/licensing/eula/oes/oes\\_2\\_english.pdf\)](http://www.novell.com/licensing/eula/oes/oes_2_english.pdf) on the Web.

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 Doesn't Support NLS**

Novell Licensing Services (NLS) are not available on OES 2, nor does an OES 2 installation require a license/key file pair (\*.nlf and \*.nfk). Therefore, in a mixed OES 2 and NetWare eDirectory tree, at least one NetWare server must hold a replica for each partition where there is a NetWare server object. For more information about licensing for NetWare servers in OES trees, see [“NetWare Licenses and OES 2 Trees” on page 44](#).

---

**IMPORTANT:** Before you install Open Enterprise Server 2, be sure to review the information in [Chapter 3, “Planning Your OES 2 Implementation,” on page 27](#), especially [Section 3.9, “Caveats to Consider Before You Install,” on page 36](#).

---

This section briefly covers the following:

- ♦ [Section 5.1, “Installing OES 2,” on page 59](#)
- ♦ [Section 5.2, “Installing OES 2 Servers in a Xen VM,” on page 60](#)

## 5.1 Installing OES 2

The OES 2 installation leverages the SUSE® Linux YaST graphical user interface. You can install OES 2 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 all 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 SP2: Installation Guide*, especially those found in
  - ♦ [“Preparing to Install OES 2 SP2”](#)
  - ♦ [“Installing OES 2 SP2”](#)
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 server reboots as part of the upgrade process and the `root` password is no longer in memory.

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 for later 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 SP2 on an Existing Server”](#) in the *OES 2 SP2: Installation Guide*.

### 5.1.1 What's Next

After installing OES 2 and before starting to use your new OES 2 server, be sure to review the information in [Chapter 6, “Caveats for Implementing OES 2 Services,” on page 61](#).

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 83.

## 5.2 Installing OES 2 Servers in a Xen VM

Installing OES 2 servers on a Xen virtual machine involves installing an OES 2 SP2 or SUSE® Linux Enterprise Server (SLES) 10 SP3 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](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](http://www.novell.com/documentation/sles10/xen_admin/data/bookinfo.html)) guide.
- ♦ “Installing OES as a Xen VM Host Server” in the *OES 2 SP2: Installation Guide*.
- ♦ “Installing, Upgrading, or Updating OES on a Xen-based VM” in the *OES 2 SP2: Installation Guide*.
- ♦ “Installing and Managing NetWare on a Xen-based VM” in the *OES 2 SP2: Installation Guide*.

# Caveats for Implementing OES 2 Services

# 6

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, “AFP,” on page 61](#)
- ♦ [Section 6.2, “Avoiding POSIX and eDirectory Duplications,” on page 62](#)
- ♦ [Section 6.3, “CIFS,” on page 64](#)
- ♦ [Section 6.4, “ConsoleOne Can Cause JClient Errors,” on page 64](#)
- ♦ [Section 6.5, “CUPS on OES 2,” on page 64](#)
- ♦ [Section 6.6, “eDirectory,” on page 64](#)
- ♦ [Section 6.7, “iFolder 3.8,” on page 66](#)
- ♦ [Section 6.8, “iPrint,” on page 66](#)
- ♦ [Section 6.9, “LDAP—Preventing “Bad XML” Errors,” on page 67](#)
- ♦ [Section 6.10, “Management,” on page 68](#)
- ♦ [Section 6.11, “NCP Doesn’t Equal NSS File Attribute Support,” on page 69](#)
- ♦ [Section 6.12, “Novell-tomcat Is for OES Use Only,” on page 70](#)
- ♦ [Section 6.13, “NSS \(OES 2\),” on page 70](#)
- ♦ [Section 6.14, “OpenLDAP on OES 2,” on page 71](#)
- ♦ [Section 6.15, “Samba,” on page 71](#)
- ♦ [Section 6.16, “Virtualization Issues,” on page 71](#)

## 6.1 AFP

- ♦ [Section 6.1.1, “Anti-Virus Solutions and AFP,” on page 61](#)

### 6.1.1 Anti-Virus Solutions and AFP

The Apple Filing Protocol (AFP) support for NSS files on OES 2 SP2 is implemented via a technology that bypasses the real-time scanning employed by most anti-virus solutions for OES.

NSS files shared through an AFP connection can be protected by on-demand scanning on the OES 2 server or by real-time and on-demand scanning on the Apple\* client.

## 6.2 Avoiding POSIX and eDirectory Duplications

OES 2 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 6.2.1, “The Problem,” on page 62](#)
- ♦ [Section 6.2.2, “Three Examples,” on page 62](#)
- ♦ [Section 6.2.3, “Avoiding Duplication,” on page 63](#)

### 6.2.1 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 server.

### 6.2.2 Three Examples

The following examples illustrate the issue.

- ♦ [“The shadow Group” on page 62](#)
- ♦ [“The users Group” on page 63](#)
- ♦ [“Other Non-System Groups” on page 63](#)

#### 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) 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 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.

## 6.2.3 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 63](#)
- ♦ [“Create Only eDirectory Users and Groups” on page 64](#)

### 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 SP2,” on page 257](#) is not exhaustive. For example, the `users` group is not listed.

---

## Create Only eDirectory Users and Groups

For OES 2 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.

## 6.3 CIFS

- ♦ [Section 6.3.1, “Changing the Server IP Address,” on page 64](#)

### 6.3.1 Changing the Server IP Address

Reconfiguring CIFS in YaST might not take effect if the server IP address was changed on the server but not in the OES LDAP server configuration.

To work around this:

- 1 Reconfigure the LDAP server IP address with the IP address changes.
- 2 Then change the CIFS IP address configuration.

## 6.4 ConsoleOne Can Cause JClient Errors

ConsoleOne support is now limited to management of GroupWise and ZENworks for Desktops 7.

If you need to use ConsoleOne® to manage either of these supported products on OES 2, make sure you have installed version 1.3.6h or later.

Earlier versions of ConsoleOne cause JClient errors in iManager.

## 6.5 CUPS on OES 2

iPrint is the print solution for OES 2 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 server.

## 6.6 eDirectory

- ♦ [Section 6.6.1, “Avoid Uninstalling eDirectory,” on page 65](#)
- ♦ [Section 6.6.2, “Avoid Renaming Trees and Containers,” on page 65](#)
- ♦ [Section 6.6.3, “Default Static Cache Limit Might Be Inadequate,” on page 65](#)
- ♦ [Section 6.6.4, “eDirectory Fails to Start Automatically After a Command Prompt Install,” on page 65](#)

- ♦ [Section 6.6.5, “One Instance Only,” on page 66](#)
- ♦ [Section 6.6.6, “Special Characters in Usernames and Passwords,” on page 66](#)

## 6.6.1 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.

## 6.6.2 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.

## 6.6.3 Default Static Cache Limit Might Be Inadequate

The eDirectory install in OES 2 SP2 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.

## 6.6.4 eDirectory Fails to Start Automatically After a Command Prompt Install

Although it is somewhat rare, if you install and configure eDirectory as an OES component 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
```

## 6.6.5 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.

## 6.6.6 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'
```

## 6.7 iFolder 3.8

Implementation caveats for iFolder 3.8 are documented in “[Caveats for Implementing iFolder 3.7 and Later Services](#)” in the *Novell iFolder 3.8 Administration Guide*.

## 6.8 iPrint

iPrint has the following implementation caveats:

- ♦ [Section 6.8.1, “Cluster Failover Between Mixed Platforms Not Supported,” on page 66](#)
- ♦ [Section 6.8.2, “Printer Driver Uploading on OES 2 Might Require a CUPS Administrator Credential,” on page 67](#)
- ♦ [Section 6.8.3, “Printer Driver Uploading Support,” on page 67](#)
- ♦ [Section 6.8.4, “iManager Plug-Ins Are Platform-Specific,” on page 67](#)
- ♦ [Section 6.8.5, “iPrint Client for Linux Doesn't Install Automatically,” on page 67](#)
- ♦ [Section 6.8.6, “iPrint Disables CUPS Printing on the OES 2 Server,” on page 67](#)

### 6.8.1 Cluster Failover Between Mixed Platforms Not Supported

Clustered iPrint services can only fail over to the same platform, either OES 2 or NetWare.

## 6.8.2 Printer Driver Uploading on OES 2 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.

## 6.8.3 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.

## 6.8.4 iManager Plug-Ins Are Platform-Specific

The iManager plug-ins are different for each server platform. Therefore, if you have both OES 2 and NetWare 6.5 SP8 servers running iPrint services, you need two instances of iManager to manage iPrint—one on each platform.

## 6.8.5 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 SP2: iPrint for Linux Administration Guide*.

## 6.8.6 iPrint Disables CUPS Printing on the OES 2 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.

## 6.9 LDAP—Preventing “Bad XML” Errors

If you are using Novell eDirectory 8.7.3x, time outs are possible when you search from iManager for eDirectory objects, such as NCP™ Server objects, Volume objects, and Cluster objects. This is because the Object Class attribute is not indexed by default. The LDAP sub-tree search can take over 30 seconds, which causes the query to time out. For example, a Cluster objects search from the Cluster Options page returns the error:

Bad XML found during parsing when accessing cluster options

We recommend that you create a value index on the objects' Object Class attribute. (Object Class is considered an attribute for indexing purposes.) This helps to reduce the time needed for the subtree search from over 30 seconds to 10 to 50 milliseconds. For instructions, see “[Creating an Index](#)” in the *Novell eDirectory 8.8 Administration Guide*.

Building indexes speeds up the subtree search, even if some partitions being searched do not contain these types of objects. For example, searching for a Cluster object in a context that contains only users is not expected to return results; however, the Object Class search is still performed, and benefits from having an index present.

The subtree search performance issue is resolved in the eDirectory 8.8.x release with the addition of the AncestorID feature.

## 6.10 Management

- ♦ [Section 6.10.1, “iManager RBS Configuration with OES 2,” on page 68](#)
- ♦ [Section 6.10.2, “Storage Error in iManager When Accessing a Virtual Server,” on page 69](#)
- ♦ [Section 6.10.3, “Truncated DOS-Compatible Short Filenames Are Not Supported at a Terminal Prompt,” on page 69](#)

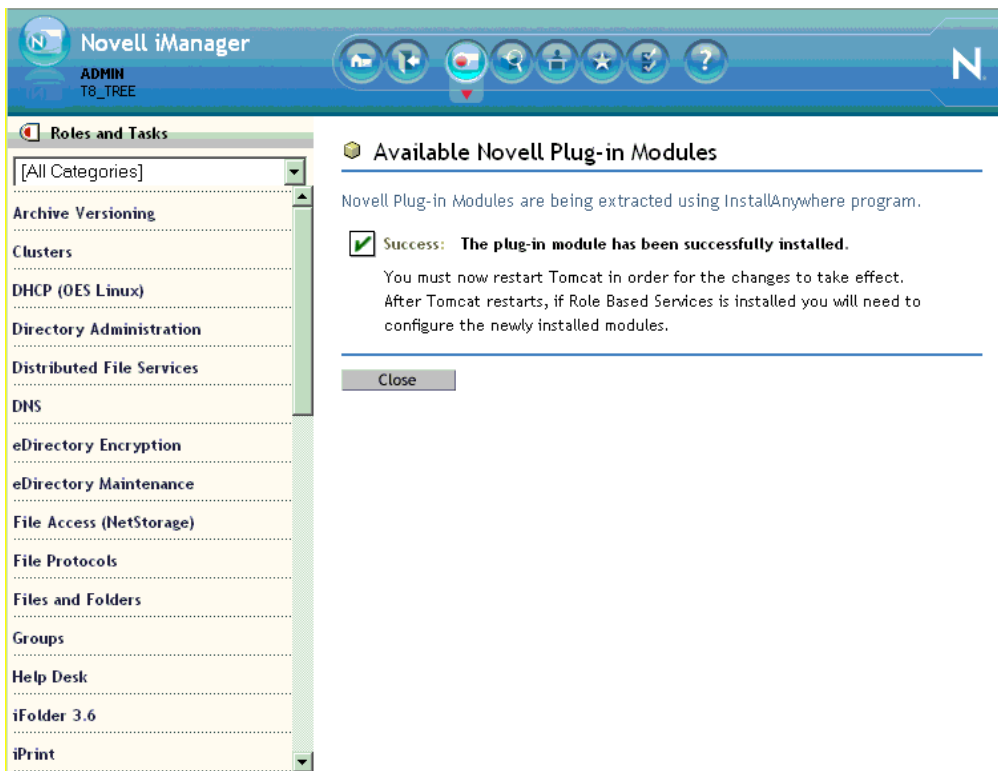
### 6.10.1 iManager RBS Configuration with OES 2

In “[Installing RBS](#)” in the *Novell iManager 2.7.3 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 2.7.3 Administration Guide](#).

## 6.10.2 Storage Error in iManager When Accessing a Virtual Server

iManager returns a `Storage Error` when you access the Authentication tab for a virtual server object. This is working as designed.

## 6.10.3 Truncated DOS-Compatible Short Filenames Are Not Supported at a Terminal Prompt

Use the actual filenames instead of names such as `filena~1.txt` during file operations from the command prompt.

## 6.11 NCP Doesn't Equal NSS File Attribute Support

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.

## 6.12 Novell-tomcat Is for OES Use Only

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.

## 6.13 NSS (OES 2)

- ♦ [Section 6.13.1, “Understanding Name Space Support,” on page 70](#)
- ♦ [Section 6.13.2, “The Role of EVMS,” on page 70](#)

### 6.13.1 Understanding Name Space Support

NSS stores LONG, UNIX, DOS, and AFP name spaces for all files. The default name space sets which name space will be exposed.

In OES 2 the LONG name space was made the default to help performance of NCP, CIFS, and Samba file services. If your primary use is for GroupWise, we recommend changing the default name space to UNIX.

### 6.13.2 The Role of EVMS

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

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 SP2: 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 with EVMS as the Volume Manager of the System Device”](#) in the *OES 2 SP2: Installation Guide*.

---

## 6.14 OpenLDAP on OES 2

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

## 6.15 Samba

For Samba implementation caveats, see “[Samba Caveats](#)” in the *OES2 SP2: Samba Administration Guide*.

## 6.16 Virtualization Issues

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

- ♦ [Section 6.16.1, “Always Close Virtual Machine Manager When Not in Use,” on page 71](#)
- ♦ [Section 6.16.2, “Always Use Timesync Rather Than NTP,” on page 71](#)
- ♦ [Section 6.16.3, “Backing Up a Xen Virtual Machine,” on page 71](#)
- ♦ [Section 6.16.4, “Time Synchronization and Virtualized OES 2,” on page 71](#)
- ♦ [Section 6.16.5, “NSS Considerations,” on page 72](#)

### 6.16.1 Always Close Virtual Machine Manager When Not in Use

You should always close Virtual Machine Manager (VMM) when you are not actively using it. Virtual Machines are not affected.

Leaving VMM open can affect the system resources available to the VMs.

### 6.16.2 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.

### 6.16.3 Backing Up a Xen Virtual Machine

When backing up a Xen virtual machine running virtualized NetWare, we recommend using a remote backup source rather than a local tape device because of limitations in detecting a local tape device.

### 6.16.4 Time Synchronization and Virtualized OES 2

eDirectory relies on time being synchronized and connections with eDirectory are lost if the system time varies in the host operating system. Be sure you understand and follow the instructions in [Virtual Machine Clock Settings \(http://www.novell.com/documentation/sles10/book\\_virtualization\\_xen/data/sec\\_guest\\_suse.html#sec\\_xen\\_time\)](http://www.novell.com/documentation/sles10/book_virtualization_xen/data/sec_guest_suse.html#sec_xen_time) in the “Virtual Machine Clock Settings” ([http://www.novell.com/documentation/sles10/book\\_virtualization\\_xen/data/book\\_virtualization\\_xen.html](http://www.novell.com/documentation/sles10/book_virtualization_xen/data/book_virtualization_xen.html)) guide.

## 6.16.5 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:** Data shredding is not supported.

# Upgrading to OES 2

# 7

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 SP2 Upgrade Paths,” on page 74](#)
- ♦ [Section 7.3, “NetWare 6.5 SP8 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 Service Differences,” on page 73](#)
- ♦ [Section 7.1.4, “Only One eDirectory Instance Is Supported on OES Servers,” 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 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 SP2](#)” in the *OES 2 SP2: 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 upgrade it to NetWare 6.5 SP8, iManager and its associated plug-ins are automatically updated to version 2.7. For more information about iManager 2.7, see the *Novell iManager 2.7.3 Administration Guide*.

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

### 7.1.3 OES 1 Linux to OES 2 Service Differences

eGuide, Novell iFolder® 2, and Virtual Office are not supported on OES 2. If you upgrade an OES 1 Linux server with any of these installed to OES 2 SP2, 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 6.6.5, “One Instance Only,” on page 66](#).

## 7.2 OES 2 SP2 Upgrade Paths

The following are supported upgrade paths for OES 2 SP2:

**Table 7-1** *Supported OES 2 SP2 Upgrade Paths*

| Source                                                | Destination                            |
|-------------------------------------------------------|----------------------------------------|
| OES 1 SP2 32-bit (Latest Patch Level) (Physical only) | OES 2 SP2 32-bit (Physical only)       |
| OES 2 32-bit (Physical or virtual)                    | OES 2 SP2 32-bit (Physical or virtual) |
| OES 2 64-bit (Physical or virtual)                    | OES 2 SP2 64-bit (Physical or virtual) |
| OES 2 SP1 32-bit (Physical or virtual)                | OES 2 SP2 32-bit (Physical or virtual) |
| OES 2 SP1 64-bit (Physical or virtual)                | OES 2 SP2 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 SP2](#)” in the *[OES 2 SP2: Installation Guide](#)*.

In addition to upgrading the server itself, data and service migrations from OES 1 to OES 2 are also supported. For more information, see the *[OES 2 SP2: Migration Tool Administration Guide](#)*.

## 7.3 NetWare 6.5 SP8 Upgrade Paths

For help upgrading from NetWare to OES 2, see the *[OES 2 SP2: Upgrading to OES—Best Practices Guide](#)*.

# Migrating and Consolidating Existing Servers and Data

# 8

This section briefly outlines the following migration topics:

- ♦ [Section 8.1, “Supported OES 2 SP2 Migration Paths,” on page 75](#)
- ♦ [Section 8.2, “Migration Tools and Purposes,” on page 75](#)

## 8.1 Supported OES 2 SP2 Migration Paths

For a complete list of Open Enterprise Server 2 SP2 migration scenarios and paths, see “[Migration Scenarios](#)” in the *OES 2 SP2: Migration Tool Administration Guide*.

## 8.2 Migration Tools and Purposes

The following sections briefly explain the migration tools included in OES 2 SP2:

- ♦ [Section 8.2.1, “OES 2 SP2 Migration Tool,” on page 75](#)
- ♦ [Section 8.2.2, “Migrate Windows Shares Utility,” on page 75](#)

### 8.2.1 OES 2 SP2 Migration Tool

The OES 2 SP2 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 SP2 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 SP2: 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 SP2: Migration Tool Administration Guide*.

### 8.2.2 Migrate Windows Shares Utility

OES 2 SP2 includes the Migrate Windows Shares utility to help you migrate data from Windows NT\*, 2000, or 2003 servers to OES 2 SP2.

For more information, see “[Migrating Data from Windows to OES 2 SP2 Linux](#)” in the *OES 2 SP2: Migration Tool Administration Guide*.



# Virtualization in OES 2

# 9

In Open Enterprise Server 2, you can host multiple OES 2 and NetWare servers on Xen virtual machines (VMs) on a single Xen host server.

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 77](#)
- ♦ [Section 9.2, “Why Install OES Services on Your VM Host?,” on page 77](#)
- ♦ [Section 9.3, “Services Supported on VM Hosts and Guests,” on page 78](#)

---

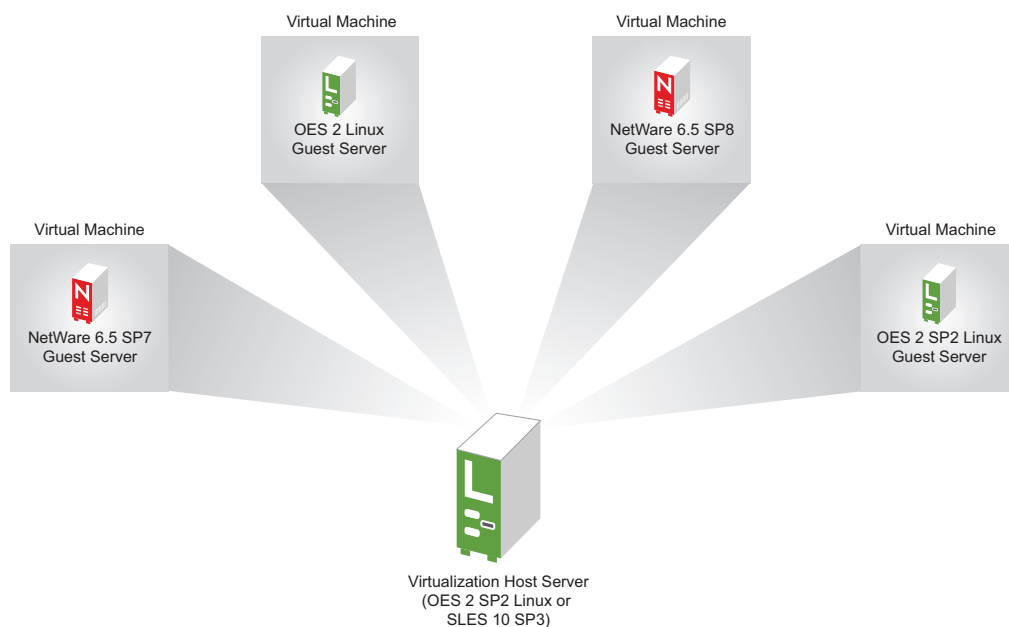
**IMPORTANT:** Support for Xen virtualization of NetWare 6.5 SP7 and later is an OES 2 product feature and is available only to OES 2 registered customers.

---

## 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 OES 2 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](#)” in the *OES 2 SP2: 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 3.9.18, “Unsupported Service Combinations,”](#) on page 45).

**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                                |                                    | ✓              | ✓                |
| Novell iFolder®                    |                                    | ✓ (3.7)        | ✓ (2.1x)         |
| iManager                           |                                    | ✓              | ✓                |
| iPrint                             |                                    | ✓              | ✓                |
| Linux User Management              | ✓                                  | ✓              |                  |

| OES 2 Service                         | Linux VM Host | Linux VM Guest | NetWare VM Guest |
|---------------------------------------|---------------|----------------|------------------|
| 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 SP2: Installation Guide*.

---



# Clustering and High Availability

# 10

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 supported 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.



This section includes the following topics:

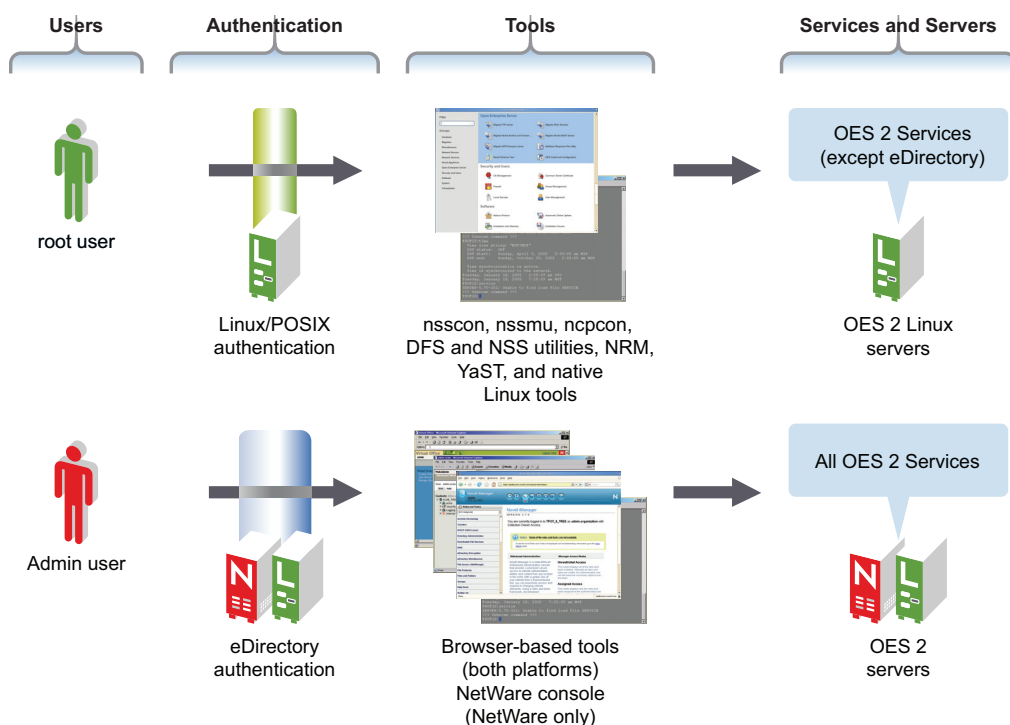
- [Section 11.1, “Overview of Management Interfaces and Services,” on page 83](#)
- [Section 11.2, “Using OES 2 Welcome Pages,” on page 84](#)
- [Section 11.3, “OES Utilities and Tools,” on page 85](#)
- [Section 11.4, “SSH Services on OES 2,” on page 93](#)

## 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 85](#).

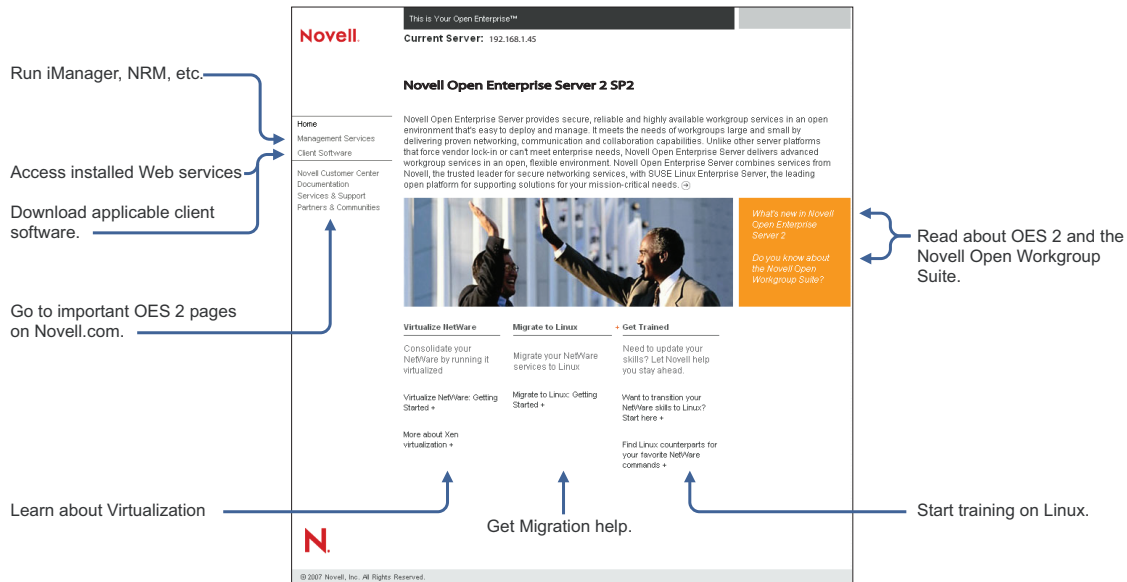
**Figure 11-1** Management Interfaces and Services



## 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 84
- ♦ [Section 11.2.2, “<<<<Accessing the Welcome Web Site,”](#) on page 85
- ♦ [Section 11.2.3, “The Welcome Web Site Is Available to All Users,”](#) on page 85
- ♦ [Section 11.2.4, “Administrative Access from the Welcome Web Site,”](#) on page 85

### 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, the Apache server and Tomcat container are included with many of the OES 2 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.

If the Welcome page disappears, include /welcome in the access URL.

For additional information, see “[Verifying That the Installation Was Successful](#)” in the *OES 2 SP2: Installation Guide*.

---

## 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

---

**TIP:** NetWare administrators who are new to Linux will also be interested in “[OES2 SP2: Linux Tips for NetWare Administrators](#),” a reference that outlines the OES equivalents for most of the familiar CLI tools on NetWare.

---

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/<br>Username                                                                                                                                                                                                                                                                                                                                                              | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bash                       | <ul style="list-style-type: none"> <li>♦ Manage the Linux server.</li> <li>♦ Manage many services running on the server.</li> </ul> | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Health Monitoring Services | <ul style="list-style-type: none"> <li>♦ Monitor the health of OES servers.</li> </ul>                                              | <ol style="list-style-type: none"> <li>1. In a <a href="#">supported Web browser</a>, access Novell Remote Manager by entering <code>http://IP_Address:8008</code></li> <li>2. Specify the eDirectory Admin username and password, or on Linux you can use the <code>root</code> user and password if needed.</li> <li>3. Click <i>Health Monitor</i> under <i>Diagnose Server</i>.</li> </ol> | <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 <a href="#">OES 2 SP2: Novell Remote Manager for Linux Administration Guide</a>.</p> <p>Health Monitoring Services on OES 2 use a Common Information Model (CIM) provided by the Web-Based Enterprise Management (WBEM) Initiative. For more information on WBEM, visit the <a href="http://www.dmtf.org/standards/wbem">DMTF Web site (http://www.dmtf.org/standards/wbem)</a>.</p> |

| Tool                                            | Tasks                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Access Method or URL/<br>Username                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Notes                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| iManager 2.7                                    | <ul style="list-style-type: none"> <li>♦ Access various other management tools and plug-ins.</li> <li>♦ Configure OES network services.</li> <li>♦ Create and manage users, groups, and other objects.</li> <li>♦ Delegate administration through Role-Based Services (RBS).</li> <li>♦ Manage eDirectory objects, schema, partitions, and replicas.</li> <li>♦ Manage OES 2 services</li> <li>♦ Set up and manage your Novell eDirectory tree.</li> </ul> | <ol style="list-style-type: none"> <li>1. In a <a href="#">supported Web browser</a>, enter the following URL:<br/><br/><code>http://<br/>IP_or_DNS/<br/>iManager.html</code></li> <li>2. Specify the eDirectory Admin username and password.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                           | <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 <a href="#">Novell iManager 2.7.3 Administration Guide</a>.</p> <p>See also <a href="#">iManager Workstation</a>.</p>                                                     |
| iManager Workstation (formerly Mobile iManager) | <ul style="list-style-type: none"> <li>♦ Manage eDirectory.</li> <li>♦ Create and manage users, groups, and other objects.</li> <li>♦ Manage OES 2 services.</li> <li>♦ Access various other management tools and plug-ins.</li> </ul>                                                                                                                                                                                                                     | <p>On a Linux workstation:</p> <ol style="list-style-type: none"> <li>1. At the <code>bin</code> directory of the expanded <code>iMan_25_Mobile_iManager_linux.tar</code> directory, run <code>imanager.sh</code>.</li> <li>2. Log in, using the eDirectory Admin username, password, and eDirectory tree name.</li> </ol> <p>On a Windows workstation:</p> <ol style="list-style-type: none"> <li>1. At the <code>bin</code> directory of the unzipped <code>iMan_25_Mobile_iManager_win</code> directory, run <code>imanager.bat</code>.</li> <li>2. Log in, using the eDirectory Admin username, password, and eDirectory tree name.</li> </ol> | <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 <a href="#">"Accessing iManager Workstation"</a> in the <a href="#">Novell iManager 2.7.3 Administration Guide</a>.</p> <p>See also <a href="#">iManager</a>.</p> |

| Tool                     | Tasks                                                                                                                                                                                                                                         | Access Method or URL/<br>Username                                                                                                                                                                                                                                                                                                                    | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| iMonitor                 | <ul style="list-style-type: none"> <li>♦ Monitor and diagnose all the servers in your eDirectory tree.</li> <li>♦ Examine eDirectory partitions, replicas, and servers.</li> <li>♦ Examine current tasks taking place in the tree.</li> </ul> | <ol style="list-style-type: none"> <li>1. In a <a href="#">supported Web browser</a>, enter one of the following URLs:<br/><br/>(On NetWare)<br/><code>http://<br/>IP_or_DNS:81/<br/>nds</code><br/><br/>(On Linux)<br/><code>https://<br/>IP_or_DNS:8030/<br/>nds</code></li> <li>2. Specify the eDirectory Admin username and password.</li> </ol> | <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 <a href="#">"Using Novell iMonitor 2.4"</a> in the <i>Novell eDirectory 8.8 Administration Guide</i>.</p> |
| iPrint Map Designer      | <ul style="list-style-type: none"> <li>♦ Create a printer map to aid in printer selection/installation.</li> <li>♦ Edit an existing printer map.</li> </ul>                                                                                   | <ol style="list-style-type: none"> <li>1. In a <a href="#">supported Web browser</a>, enter the following URL:<br/><br/><code>http://<br/>IP_or_DNS/<br/>ippdocs/<br/>maptool.htm</code></li> <li>2. Specify the eDirectory Admin username and password.</li> </ol>                                                                                  | <p>For OES 2 server instructions, see <a href="#">"Setting Up Location-Based Printing"</a> in the <i>OES 2 SP2: iPrint for Linux Administration Guide</i>.</p>                                                                                                                                                                                                                                                                                                                                                            |
| NetStorage Web Interface | <ul style="list-style-type: none"> <li>♦ Manage file system access.</li> <li>♦ Manage file system space restrictions.</li> <li>♦ Salvage and purge deleted files.</li> </ul>                                                                  | 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 <a href="#">"Viewing or Modifying Directory and File Attributes and Rights"</a> in the <i>OES 2 SP2: NetStorage for Linux Administration Guide</i>.</p>                                                                    |

| Tool                | Tasks                                                                                                                                                                        | Access Method or URL/<br>Username                                                | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Novell Client       | <ul style="list-style-type: none"> <li>♦ Manage file system access.</li> <li>♦ Manage File System Space Restrictions.</li> <li>♦ Salvage and purge deleted files.</li> </ul> | 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 <a href="#">“Managing File Security and Passwords”</a> in the <i>Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide</i>.</p> |
| Novell iFolder® 3.8 | <ul style="list-style-type: none"> <li>♦ Manage various aspects of iFolder 3.8.</li> </ul>                                                                                   | 1. In iManager 2.7, click <i>iFolder 3.8 &gt; Launch iFolder Admin Console</i> . | <p>For more information on managing iFolder 3.8, see the following in the <i>Novell iFolder 3.8 Administration Guide</i>:</p> <ul style="list-style-type: none"> <li>♦ <a href="#">iFolder Enterprise Server</a></li> <li>♦ <a href="#">iFolder Services via Web Admin</a></li> <li>♦ <a href="#">iFolder Users</a></li> <li>♦ <a href="#">iFolder Web Access Server</a></li> <li>♦ <a href="#">Managing iFolders</a></li> </ul>                          |

| Tool                           | Tasks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Access Method or URL/<br>Username                                                                                                                                                                                                                                                     | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Novell Remote Manager (NRM)    | <ul style="list-style-type: none"> <li>♦ Manage file system access and attributes for the NetWare Traditional File System and the NSS File System on NetWare.</li> <li>♦ Manage the NCP™ Server (Linux)</li> <li>♦ Manage NCP connections to NSS and NCP volumes (Linux)</li> <li>♦ Manage Dynamic Storage Technology (Linux)</li> <li>♦ Manage NetWare Traditional File Systems (NetWare).</li> <li>♦ Manage OES 2 servers from a remote location.</li> <li>♦ Monitor your server's health.</li> <li>♦ Change server configurations.</li> <li>♦ Perform diagnostic and debugging tasks.</li> <li>♦ View volume inventories (Linux)</li> </ul> | <ol style="list-style-type: none"> <li>1. In a <a href="#">supported Web browser</a>, enter the following URL:<br/><br/><code>https://<br/>IP_or_DNS:8009</code></li> <li>2. Specify either the eDirectory username and password or a Linux (POSIX) username and password.</li> </ol> | <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 <a href="#">OES 2 SP2: Novell Remote Manager for Linux Administration Guide</a>.</p>                                                                                                                                                           |
| NSS Management Utility (NSSMU) | <ul style="list-style-type: none"> <li>♦ Manage the Novell Storage Services™ file system.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <p>At a terminal prompt:</p> <ol style="list-style-type: none"> <li>1. Load NSSMU by entering<br/><br/><code>/opt/novell/<br/>nss/sbin/nssmu</code></li> </ol>                                                                                                                        | <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 <a href="#">OES 2 SP2: NSS File System Administration Guide</a>.</p> |

| Tool                    | Tasks                                                                                                                                                                                                                                                                          | Access Method or URL/<br>Username                      | Notes                                                                                                                                                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OpenSSH (client access) | <ul style="list-style-type: none"> <li>Securely run commands on remote servers.</li> <li>Securely copy files and directories to and from other servers using SSH utilities.</li> </ul>                                                                                         | Connect to the server using your favorite SSH client.  | On Linux, OpenSSH is installed by default and is accessed by eDirectory users as a LUM-enabled service. For more information, see <a href="#">Section 11.4, "SSH Services on OES 2," on page 93.</a>                                                           |
| OpenSSH (Linux)         | <ul style="list-style-type: none"> <li>Manage a SLES 10 SP1 (OES 2) server by using OpenSSH.</li> </ul>                                                                                                                                                                        | 1. Use standard SSH connection and management options. | Requirements: <ul style="list-style-type: none"> <li>The firewall must allow for SSH access.</li> <li>eDirectory users must be enabled for SSH access. For more information, see <a href="#">Section 11.4, "SSH Services on OES 2," on page 93.</a></li> </ul> |
| OpenWBEM                | <ul style="list-style-type: none"> <li>Perform tasks instrumented by specific providers.</li> </ul>                                                                                                                                                                            | Access <code>/etc/openwbem</code> .                    | For more information, see the <a href="#">OES 2 SP2: OpenWBEM Services Administration Guide</a> .                                                                                                                                                              |
| Perl                    | A programming language developed by Larry Wall that <ul style="list-style-type: none"> <li>Runs faster than shell script programs.</li> <li>Reads and writes binary files.</li> <li>Processes very large files.</li> <li>Lets you quickly develop CGI applications.</li> </ul> | Install the associated RPM files.                      | 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/<br>Username                                                                                                                                                                                                                                                       | Notes                                                                                                                                                                                                                               |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| QuickFinder™<br>Server Manager | <ul style="list-style-type: none"> <li>♦ Create search indexes for any Web site or attached file systems.</li> <li>♦ 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.</li> <li>♦ Configure and maintain your indexes remotely from anywhere on the Net.</li> </ul>                                                                                                                                                                     | <ol style="list-style-type: none"> <li>1. In a <a href="#">supported Web browser</a>, enter the following URL:<br/><br/>http://<br/>IP_or_DNS/<br/>qfsearch/admin</li> <li>2. Specify the root or other user as documented.</li> </ol>                                                  | <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 <a href="#">QuickFinder 5.0 Server Administration Guide</a>.</p> |
| Remote<br>Manager              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                         | See <a href="#">Novell Remote Manager</a> .                                                                                                                                                                                         |
| SNMP for<br>eDirectory         | <p>Lets you use standard SNMP tools to</p> <ul style="list-style-type: none"> <li>♦ Monitor an eDirectory server.</li> <li>♦ Track the status of eDirectory to verify normal operations.</li> <li>♦ Spot and react to potential problems when they are detected.</li> <li>♦ Configure traps and statistics for selective monitoring.</li> <li>♦ Plot a trend on the access of eDirectory.</li> <li>♦ Store and analyze historical data that has been obtained through SNMP.</li> <li>♦ Use the SNMP native master agent on all eDirectory platforms.</li> </ul> | <ol style="list-style-type: none"> <li>1. Configure SNMP for eDirectory as documented for your platform.</li> <li>2. Access SNMP for eDirectory services using the SNMP management interface of your choice.</li> <li>3. Specify the eDirectory Admin username and password.</li> </ol> | <p>SNMP support is installed with eDirectory.</p> <p>For more information on SNMP for eDirectory, see “<a href="#">SNMP Support for Novell eDirectory</a>” in the <a href="#">Novell eDirectory 8.8 Administration Guide</a>.</p>   |

| Tool                             | Tasks                                                                                                                                                                           | Access Method or URL/<br>Username                                                                                                                                                   | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SUSE® Linux Monitoring Utilities | <ul style="list-style-type: none"> <li>♦ Manage the Linux server and standard Linux services from the command prompt.</li> </ul>                                                | Enter the desired command at the command prompt.                                                                                                                                    | For more information, see “System Monitoring Utilities” ( <a href="http://www.novell.com/documentation/sles10/sles_admin/data/cha_util.html">http://www.novell.com/documentation/sles10/sles_admin/data/cha_util.html</a> ) in the <i>SLES 10 SP3: Installation and Administration Guide</i> ( <a href="http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html">http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html</a> ).                                                                                                                                                                                                       |
| YaST (SUSE Linux)                | <ul style="list-style-type: none"> <li>♦ Install OES 2.</li> <li>♦ Configure the server and standard Linux services.</li> <li>♦ Install OES components and services.</li> </ul> | <p>To access YaST from the GNOME* interface, start the YaST Control Center by clicking <i>Computer &gt; YaST</i>.</p> <p>To access YaST at a command prompt, enter <i>yast</i>.</p> | For more information, see “Installation with YaST” ( <a href="http://www.novell.com/documentation/sles10/sles_admin/data/cha_inst.html">http://www.novell.com/documentation/sles10/sles_admin/data/cha_inst.html</a> ) and “System Configuration with YaST” ( <a href="http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast2.html">http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast2.html</a> ) in the <i>SLES 10 SP3: Installation and Administration Guide</i> ( <a href="http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html">http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html</a> ). |

## 11.4 SSH Services on OES 2

This section documents the following topics:

- ♦ [Section 11.4.1, “Overview,” on page 93](#)
- ♦ [Section 11.4.2, “Setting Up SSH Access for LUM-enabled eDirectory Users,” on page 95](#)

### 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 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.

This section discusses the following topics:

- ♦ [“When Is SSH Access Required?” on page 94](#)

- ♦ “How SSH Access for eDirectory Users Works” on page 94
- ♦ “SSH Security Considerations” on page 95

## 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 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 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, 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 95](#)
- ♦ [“Adding SSH as an Allowed Service in LUM” on page 95](#)
- ♦ [“Enabling Users for LUM” on page 96](#)
- ♦ [“Restricting SSH Access to Only Certain LUM-Enabled Users” on page 96](#)
- ♦ [“Providing SSH Access for Samba Users” on page 97](#)

#### Allowing SSH Access Through the Firewall

- 1 On the OES 2 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 96](#).
- or
- If SSH is not an allowed service for Linux User Management on the server, continue with [Step 2](#).
- 2 On the OES 2 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 SP2: 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 97.

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 96.

## 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 96](#) 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 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 99](#)
- ♦ [Section 12.2, “DNS and DHCP,” on page 99](#)
- ♦ [Section 12.3, “Time Services,” on page 101](#)
- ♦ [Section 12.4, “Discovery Services,” on page 112](#)
- ♦ [Section 12.5, “SLP,” on page 113](#)

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 standard Linux TCP/IP support on SUSE® Linux Enterprise Server 10.

### 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.

To aid with migrations from NetWare to OES, coexistence between IPX and TCP/IP networks is still supported on NetWare, but IPX is not supported on Linux.

## 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.

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

- ♦ [Section 12.2.1, “DNS Differences Between NetWare and OES 2,” on page 100](#)
- ♦ [Section 12.2.2, “DHCP Differences Between NetWare and OES 2,” on page 101](#)

## 12.2.1 DNS Differences Between NetWare and OES 2

As you plan to upgrade from NetWare to OES 2, consider the following differences between DNS on NetWare and OES 2:

**Table 12-1** DNS: NetWare 6.5 SP8 vs. OES 2

| Feature or Command                          | NetWare 6.5 SP8                                                         | OES 2                                                                                                                                             |
|---------------------------------------------|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Auditing                                    | Yes                                                                     | No                                                                                                                                                |
| DNSMaint                                    | Yes                                                                     | No                                                                                                                                                |
| Fault Tolerance                             | Yes                                                                     | Yes                                                                                                                                               |
| Filenames and paths:                        |                                                                         |                                                                                                                                                   |
| ♦ Server binary                             | ♦ <code>sys:/system/named.nlm</code>                                    | ♦ <code>/opt/novell/named/bin/novell-named</code>                                                                                                 |
| ♦ <code>.db</code> , <code>.jnl</code> file | ♦ <code>sys:/etc/dns</code>                                             | ♦ <code>/etc/opt/novell/named/named.conf</code>                                                                                                   |
| ♦ Stat file, info file                      |                                                                         | ♦ <code>/var/opt/novell/log/named/named.run</code>                                                                                                |
| Console commands:                           |                                                                         |                                                                                                                                                   |
| ♦ Start the server                          | ♦ <code>named</code>                                                    | ♦ <code>rcnovell-named</code> or <code>novell-named</code>                                                                                        |
| ♦ Stop the server                           | ♦ <code>named stop</code>                                               | ♦ <code>rcnovell-named stop</code>                                                                                                                |
| ♦ Check Status                              | ♦ <code>named status</code>                                             | ♦ <code>rcnovell-named status</code>                                                                                                              |
| ♦ Unsupported command parameters            | ♦ N/A                                                                   | ♦ <code>[-dc categories]</code><br>♦ <code>[-mstats]</code><br>♦ <code>[-nno_of_cpus]</code><br>♦ <code>[-qstats]</code>                          |
| Journal log size                            | Specify at the command prompt by using the <code>jsize</code> argument. | Specify by using the iManager plug-in <code>&gt; max-journal-size</code> field.                                                                   |
| Management                                  | iManager<br>Command Line Interface                                      | iManager<br>Command Line Interface<br><br>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

As you plan to upgrade from NetWare to OES 2, consider the following differences between DHCP on NetWare and OES 2:

**Table 12-2** *DHCP: NetWare 6.5 SP8 vs. OES 2*

| Feature or Command   | NetWare 6.5 SP8             | OES 2                                                                                                                                   |
|----------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 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<br><br>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)<br><br>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.                                     |
| 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 as you move from NetWare to OES 2:

- ♦ [Section 12.3.1, “Overview of Time Synchronization,” on page 102](#)
- ♦ [Section 12.3.2, “Planning for Time Synchronization,” on page 105](#)
- ♦ [Section 12.3.3, “Coexistence and Migration of Time Synchronization Services,” on page 108](#)
- ♦ [Section 12.3.4, “Implementing Time Synchronization,” on page 110](#)

- ♦ [Section 12.3.5, “Configuring and Administering Time Synchronization,” on page 111](#)
- ♦ [Section 12.3.6, “Daylight Saving Time,” on page 112](#)

## 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 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 102](#)
- ♦ [“OES 2 Servers as Time Providers” on page 104](#)
- ♦ [“OES 2 Servers as Time Consumers” on page 105](#)

### Understanding Time Synchronization Modules

During the upgrade to OES 2, your eDirectory tree might contain servers running OES 2, NetWare 6.5 SP8, or previous versions of NetWare. Therefore, you must understand the differences in the time synchronization modules that each operating system uses and how these modules can interact with each other.

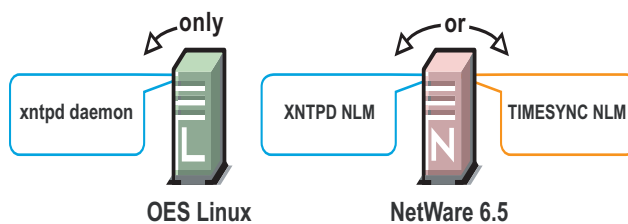
- ♦ [“OES 2 vs. NetWare 6.5” on page 102](#)
- ♦ [“OES 2 Servers Use the Network Time Protocol \(NTP\) to Communicate” on page 102](#)
- ♦ [“Compatibility with Earlier Versions of NetWare” on page 103](#)

#### OES 2 vs. NetWare 6.5

As illustrated in [Figure 12-1](#), NetWare 6.5 can use either the Network Time Protocol (NTP) or Timesync modules for time synchronization. Both modules can communicate with OES 2 by using NTP. However, when installing virtualized NetWare, Timesync should always be used (see [Section 6.16.2, “Always Use Timesync Rather Than NTP,” on page 71](#)).

OES 2 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 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 and NetWare 6.5 servers can freely interchange time synchronization information because NetWare 6.5 includes the following:

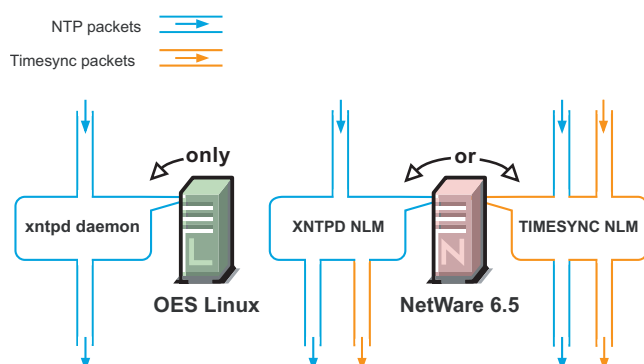
- ♦ A TIMESYNC NLM™ that both consumes and provides NTP time packets in addition to Timesync packets.
- ♦ An XNTPD NLM that can provide Timesync packets in addition to offering standard NTP functionality.

---

**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



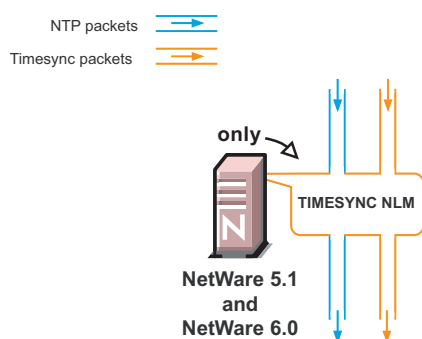
## Compatibility with Earlier Versions of NetWare

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.

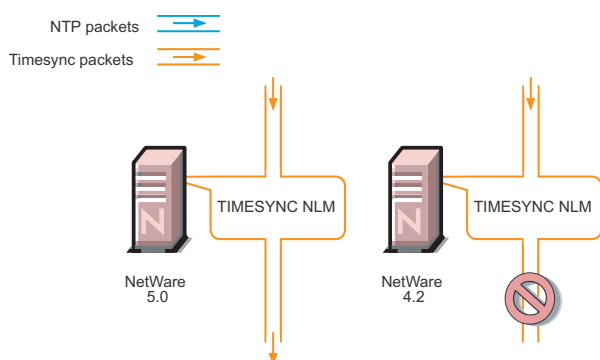
**Figure 12-3** NTP Compatibility of NetWare 5.1 and 6.0



### 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 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 104](#) illustrates that these earlier server versions can synchronize through a NetWare 6.5 server.

---

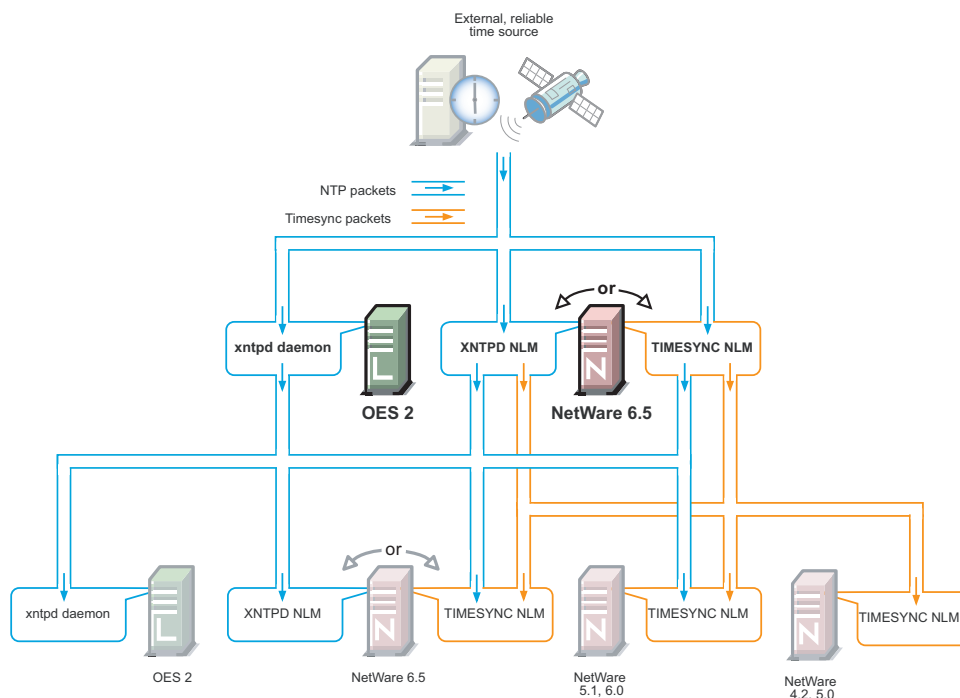
**IMPORTANT:** As shown in [Figure 12-4](#), we recommend that NetWare 4.2 servers not be used as a time source.

---

## 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

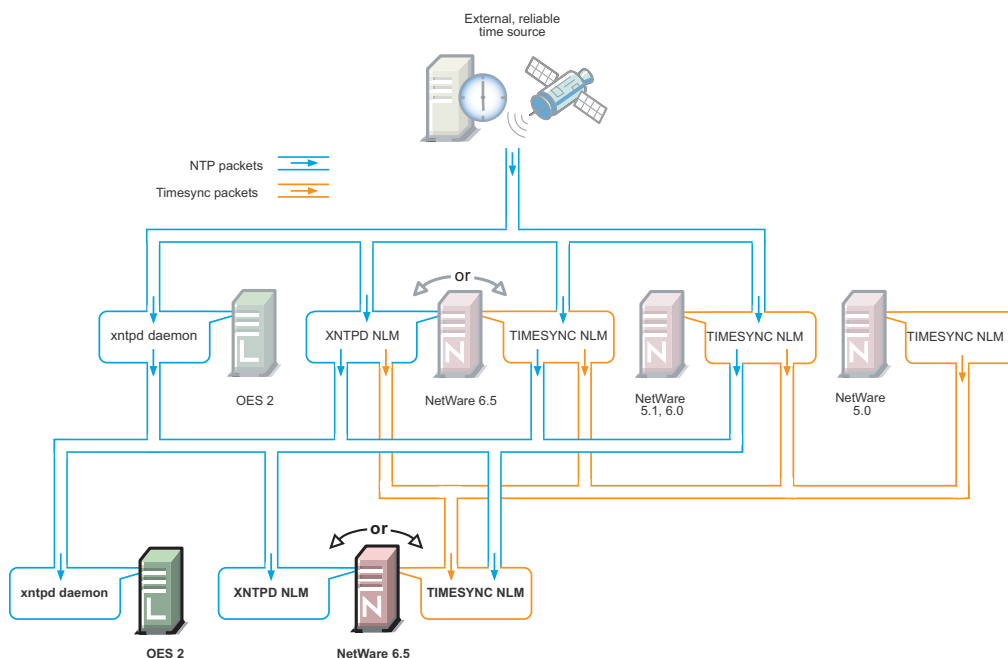
Figure 12-6 shows the time sources that OES 2 servers can use for synchronizing server time.

---

**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 105
- ♦ “Choose Timesync for Virtualized NetWare Only” on page 106
- ♦ “Planning a Time Synchronization Hierarchy before Installing OES” on page 107

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

- ♦ “How Timesync Works” in the *NW 6.5 SP8: Network Time Synchronization Administration Guide*
- ♦ “Network Time Protocol” in the *NW 6.5 SP8: NTP 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 106

- ♦ [“Time Synchronization for Trees with More Than Thirty Servers” on page 106](#)
- ♦ [“Time Synchronization across Geographical Boundaries” on page 106](#)

### 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 107.](#))

All other servers should 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 107.](#)

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

- ♦ [“Configuring Timesync on Servers”](#) in the *NW 6.5 SP8: Network Time Synchronization Administration Guide*
- ♦ [“Modes of Time Synchronization”](#) in the *NW 6.5 SP8: NTP Administration Guide*
- ♦ NTP information on the [Web \(http://www.cis.udel.edu/~mills/ntp.html\)](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 *NW 6.5 SP8: NTP Administration Guide*.

### Choose Timesync for Virtualized NetWare Only

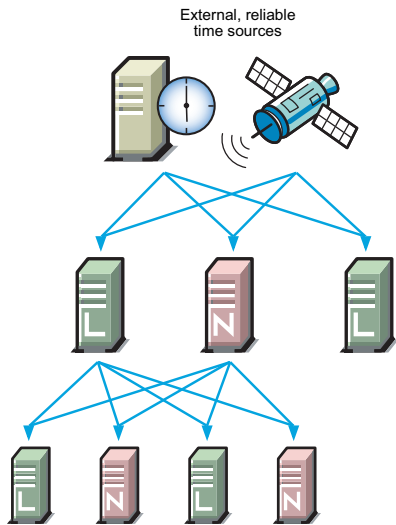
When you install a virtualized NetWare 6.5 server, you should always use Timesync and configure it to communicate using NTP. For more information, see [“You Must Use Timesync for Time Synchronization”](#) in the *OES 2 SP2: Installation Guide*.

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 *NW65 SP8: 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 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 103.)
- 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 *NW 6.5 SP8: NTP Administration Guide*.

For more planning information, see the following documentation:

- ♦ *NW 6.5 SP8: Network Time Synchronization Administration Guide*
- ♦ *NW 6.5 SP8: NTP Administration Guide*
- ♦ NTP information found on the OES 2 server in /usr/share/doc/packages/xntp and on the [Web](http://www.cis.udel.edu/~mills/ntp.html) (<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 can be introduced into an existing network environment without disrupting any of the products and services that are in place.

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

- ♦ “[Coexistence](#)” on page 108
- ♦ “[Upgrading from NetWare to OES 2](#)” on page 109

#### 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 108
- ♦ “[Coexistence Issues](#)” on page 109

#### 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 104](#) and [Figure 12-6 on page 105](#).

**Table 12-3** *Time Synchronization Compatibility*

| Module                 | Compatibility                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TIMESYNC NLM (NetWare) | <p>Can consume time from</p> <ul style="list-style-type: none"><li>♦ All previous versions of Timesync. However, the NetWare 4.2 TIMESYNC NLM should not be used as a time source.</li><li>♦ Any TIMESYNC or NTP daemon.</li></ul> <p>Can provide time to</p> <ul style="list-style-type: none"><li>♦ All previous versions of Timesync.</li><li>♦ Any TIMESYNC or NTP daemon.</li></ul> |
| XNTPD NLM (NetWare)    | <p>Can consume time from</p> <ul style="list-style-type: none"><li>♦ Any NTP daemon.</li></ul> <p>Can provide time to</p> <ul style="list-style-type: none"><li>♦ All previous versions of Timesync.</li><li>♦ Any NTP daemon.</li></ul>                                                                                                                                                 |
| xntpd daemon (SLES 10) | <p>Can consume time from</p> <ul style="list-style-type: none"><li>♦ Any NTP daemon.</li></ul> <p>Can provide time to</p> <ul style="list-style-type: none"><li>♦ Any NTP daemon.</li></ul>                                                                                                                                                                                              |
| 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 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 103](#).

## Upgrading from NetWare to OES 2

The OES 2 SP21 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 Linux”](#) in the *OES 2 SP2: Migration Tool Administration Guide*.

## 12.3.4 Implementing Time Synchronization

As you plan to implement your time synchronization hierarchy, you should know how the NetWare and OES 2 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 110
- ♦ “Existing Tree” on page 111

### New Tree

By default, both the OES 2 and the NetWare 6.5 SP8 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” on page 110
- ♦ “NetWare 6.5 SP8” on page 110

### OES 2

When you configure your eDirectory installation, the OES 2 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.

---

### NetWare 6.5 SP8

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 “[Choose Timesync for Virtualized NetWare Only](#)” on page 106 and as fully explained in “[Setting the Server Time Zone and Time Synchronization Method](#)” in the *NW65 SP8: Installation Guide*.

## Existing Tree

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

- ♦ [“OES 2” on page 111](#)
- ♦ [“NetWare 6.5 SP8” on page 111](#)

## OES 2

If you are installing into an existing tree, the OES 2 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.
- ♦ 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 107](#).

The OES 2 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 112](#).

## NetWare 6.5 SP8

If you are installing into an existing tree, the NetWare 6.5 SP8 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 *NW65 SP8: 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 107](#)) 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 112](#)
- ♦ [“Changing Time Synchronization Settings on a NetWare Server” on page 112](#)

## 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: *NW 6.5 SP8: Network Time Synchronization Administration Guide*
- ♦ NTP: *NW 6.5 SP8: NTP 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

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

- ♦ DNS/DHCP
- ♦ Directory services
- ♦ Local host configuration files
- ♦ Service Location Protocol (SLP services)
- ♦ 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 112](#)
- ♦ [Section 12.4.2, “WinSock and Discovery Is NetWare only,” on page 113](#)
- ♦ [Section 12.4.3, “UDDI and Discovery,” on page 113](#)
- ♦ [Section 12.4.4, “CIMOM and Discovery,” on page 113](#)

### 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 113](#).

## 12.4.2 WinSock and Discovery Is NetWare only

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

## 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 NetWare 6.5 SP3, the UDDI server component was removed from the list of products that could be installed.

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

The OpenSLP services on OES 2 are compatible with NetWare SLP services.

This section discusses the following topics:

- ♦ [Section 12.5.1, “Why SLP Is Needed,” on page 113](#)
- ♦ [Section 12.5.2, “Comparing Novell SLP and OpenSLP,” on page 114](#)
- ♦ [Section 12.5.3, “Setting Up OpenSLP on OES 2 Networks,” on page 115](#)
- ♦ [Section 12.5.4, “Using Novell SLP on OES 2 Networks,” on page 119](#)

## 12.5.1 Why SLP Is Needed

**NetWare:** Although many other applications and server types rely on SLP for service discovery, NetWare services 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:** On the other hand, for OES 2 services to work, 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 installation or manually.

## 12.5.2 Comparing Novell SLP and OpenSLP

**Table 12-4** *SLP Solutions*

| Platform           | NetWare                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | OES 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 NetWare 6.5 SP8 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, 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 server is the fourth or later server added to a tree and doesn't have an eDirectory replica automatically installed.</p> |
| 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><b>NOTE:</b> 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>                                                                                                                                                                                                                                                 |

| Platform      | NetWare                                                                                                                 | OES 2                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| 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 | <a href="#">“Implementing the Service Location Protocol”</a> in the <i>Novell eDirectory 8.8 Administration Guide</i> . | <a href="#">“Configuring OpenSLP for eDirectory”</a> 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 SP3 (the underlying OES 2 SP2 platform). On NetWare the Novell SLP service is configured to automatically work with eDirectory and other services. On OES 2, the OpenSLP service must be manually configured to work with eDirectory and other services.

- ♦ [“When Is OpenSLP Required?”](#) on page 115
- ♦ [“Setting Up an OpenSLP DA Server”](#) on page 115
- ♦ [“Configuring OES 2 Servers to Access the OpenSLP DA”](#) on page 116
- ♦ [“Configuring NetWare Servers to Use the OpenSLP Service”](#) on page 118

#### When Is OpenSLP Required?

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

- ♦ You plan to install more than three servers into a new tree or a new eDirectory partition being created on an OES 2 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, it is most convenient if you do it before you install the fourth server in your tree or partition. That way you can point to the SLP service during the installation. Setting up SLP services on every OES 2 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 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 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 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 Servers to Access the OpenSLP DA \(page 116\)](#)
- ♦ [Configuring NetWare Servers to Use the OpenSLP Service \(page 118\)](#)

## Configuring OES 2 Servers to Access the OpenSLP DA

If you created the OpenSLP DA on an OES 2 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 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 Installation” on page 117](#)
- ♦ [“Configuring for DA Access Before or After Installing the OES 2 Server” on page 117](#)

### Configuring for DA Access During the OES 2 Installation

As you install OES 2 by using the instructions in the [“Novell eDirectory Services”](#) section of the *OES 2 SP2: 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 116](#). 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 115](#). You can also list additional DA addresses, separated by commas.
- 4 Return to the [“Novell eDirectory Services”](#) instructions in the *OES 2 SP2: Installation Guide*.

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

Whether you configure DA access before installing OES 2 on a SLES 10 server or after a simultaneous install of SLES 10 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 116](#).

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 115](#).

```
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 118](#)
- ♦ [“Configuring for DA Access After Installing the NetWare Server” on page 118](#)

### 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 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 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 during the upgrade to OES 2 until you are ready to switch to OpenSLP.

This section discusses the following:

- ♦ [“NetWare Is Configured with Novell SLP By Default” on page 119](#)
- ♦ [“Configuring OES 2 Servers to Access the Novell SLP DA” on page 119](#)
- ♦ [“Checking the Status of Novell SLP Services” on page 121](#)

### 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 Servers to Access the Novell SLP DA

For each of the OES 2 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 Installation” on page 119](#)
- ♦ [“Configuring for DA Access Before or After Installing the OES 2 Server” on page 120](#)

#### Configuring for DA Access During the OES 2 Installation

As you install OES 2, in the [“Novell eDirectory Services”](#) section of the *OES 2 SP2: 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 SP2: Installation Guide*.

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

Whether you configure DA access before installing OES 2 on a SLES 10 server or after a simultaneous install of SLES 10 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 a terminal 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, 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 `SLPINFO / ALL` command.



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 123](#)
- ♦ [Section 13.2, “Planning OES File Storage,” on page 128](#)
- ♦ [Section 13.3, “Coexistence and Migration of Storage Services,” on page 135](#)
- ♦ [Section 13.4, “Configuring and Maintaining Storage,” on page 136](#)

Other storage-related topics in this guide:

- ♦ [Chapter 16, “Access Control and Authentication,” on page 163](#)
- ♦ [Section 16.2, “Authentication Services,” on page 174](#)
- ♦ [Appendix D, “Backup Services,” on page 245](#)
- ♦ [Chapter 17, “File Services,” on page 179](#)

## 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 123](#)
- ♦ [Section 13.1.2, “iSCSI,” on page 124](#)
- ♦ [Section 13.1.3, “File System Support in OES,” on page 124](#)
- ♦ [Section 13.1.4, “Storage Basics by Platform,” on page 126](#)
- ♦ [Section 13.1.5, “Storage Options,” on page 126](#)
- ♦ [Section 13.1.6, “NetWare Core Protocol Support \(Novell Client Support\) on Linux,” on page 128](#)

### 13.1.1 Databases

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

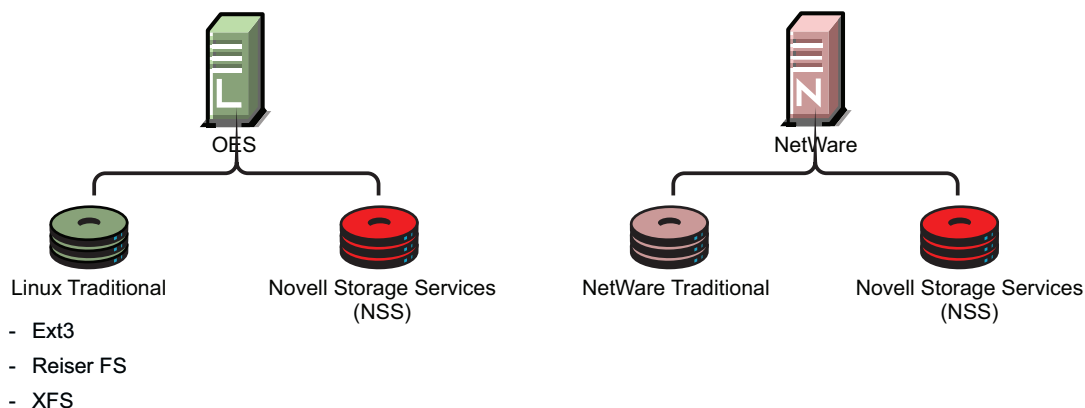
## 13.1.2 iSCSI

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

## 13.1.3 File System Support in OES

As shown in [Figure 13-1](#), both OES 2 and NetWare 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> | For an overview of the supported file systems in OES 2, see “ <a href="#">File Systems Overview</a> ” in the <i>OES 2 SP2: File Systems Management Guide</i> . |
| NetWare® Traditional File System | This is a legacy file system on NetWare servers that supports the Novell file service trustee access control model.                                                         | For more information, see the <i>NW6.5 SP8: Traditional File System Administration Guide</i> .                                                                 |

| 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 “<a href="#">Comparison of NSS on NetWare and NSS on Linux</a>” in the <i>OES 2 SP2: NSS File System Administration Guide</i>.</p> | <p>For an overview of NSS, see “<a href="#">Overview of NSS</a>” in the <i>OES 2 SP2: NSS File System Administration Guide</i>.</p> |

## Novell Storage Services (NSS)

The following sections summarize key points regarding NSS:

- ♦ “[Understanding NSS Nomenclature](#)” on page 125
- ♦ “[Comparing NSS with Other File Systems](#)” on page 125
- ♦ “[NSS and Storage Devices](#)” on page 126

### 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 SP2: 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 SP2: 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 SP2: 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 126
- ♦ “[NetWare Directories](#)” on page 126
- ♦ “[NetWare Storage Devices](#)” on page 126

#### 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 SP2: 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 SP2: 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 *NW6.5 SP8: Server Disks and Storage Devices*.

### 13.1.5 Storage Options

The following sections summarize OES storage options.

- ♦ “[Dynamic Storage Technology](#)” on page 126
- ♦ “[Direct-Attached Storage Options \(NSS and Traditional\)](#)” on page 127
- ♦ “[Advanced Storage Options \(NSS Only\)](#)” on page 127

#### Dynamic Storage Technology

Dynamic Storage Technology for OES 2 lets you present the files and subdirectories on two separate NSS volumes as though they were on a single, unified NSS 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 SP2: Dynamic Storage Technology Administration Guide](#).

### **Direct-Attached Storage Options (NSS and Traditional)**

As shown in [Figure 13-1 on page 124](#), 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 SP2: Storage and File Services Overview](#).

### **Advanced Storage Options (NSS Only)**

NSS volumes support the following advanced storage solutions, as documented in the [OES 2 SP2: 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 [NW 6.5 SP8: iSCSI 1.1.3 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 SP2: NSS File System Administration Guide*.

- ♦ **Software RAID:** NSS supports software RAID 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 SP2: 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 *NW6.5 SP8: Novell Cluster Services 1.8.5 Administration Guide* and the *OES 2 SP2: Novell Cluster Services 1.8.7 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 file storage services.

Novell Storage Services (NSS) volumes are NCP volumes by nature, and 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 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 200.

## 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 128
- ♦ [Section 13.2.2, “File Service Support Considerations,”](#) on page 129
- ♦ [Section 13.2.3, “General Requirements for Data Storage,”](#) on page 129
- ♦ [Section 13.2.4, “OES 2 Storage Planning Considerations,”](#) on page 129
- ♦ [Section 13.2.5, “NSS Planning Considerations,”](#) on page 134

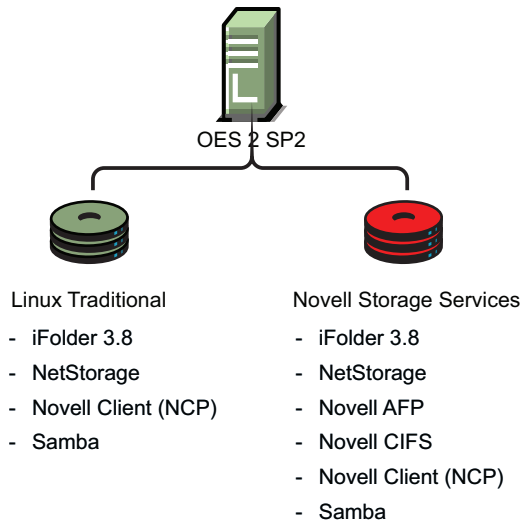
### 13.2.1 Directory Structures

To plan the directory structures you need on OES 2, see “[Understanding Directory Structures in Linux POSIX File Systems](#)” in the *OES 2 SP2: 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 SP2: Storage and File Services Overview*.

## 13.2.4 OES 2 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 servers, and includes the following topics:

- ♦ “[The Workgroup Environment](#)” on page 129
- ♦ “[File System Support](#)” on page 130
- ♦ “[File Access Protocol Support](#)” on page 132
- ♦ “[OES 2 Workloads](#)” on page 133

### The Workgroup Environment

When selecting a file system, it is important to understand the environment in which it operates. For OES 2, 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 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 130](#)
- ♦ [“Ext2” on page 131](#)
- ♦ [“Ext3” on page 131](#)
- ♦ [“ReiserFS” on page 131](#)
- ♦ [“XFS” on page 132](#)

### 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](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](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
- ♦ Journalled (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 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.

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 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 134](#)
- ♦ [“Other NSS Planning Topics” on page 134](#)

### 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 SP2: 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 135](#)
- ♦ [Section 13.3.2, “OES 2 Options,” on page 135](#)
- ♦ [Section 13.3.3, “NetWare 6.5 SP8 Options,” on page 136](#)

### 13.3.1 MySQL

OES 2 includes the open source MySQL database. 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.

---

### 13.3.2 OES 2 Options

OES 2 provides support for Novell Storage Services (NSS) as well as Linux POSIX file systems.

- ♦ [“NSS Volumes” on page 135](#)
- ♦ [“Linux POSIX File Systems” on page 136](#)

#### NSS Volumes

NSS volumes are cross-compatible between NetWare and Linux.

To use NSS on OES 2, 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 with EVMS as the Volume Manager of the System Device”](#) in the *OES 2 SP2: Installation Guide*.

On OES 2, 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 NetWare 6.5 SP4 and OES 2, 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 SP2: 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 SP2: 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 SP2: NCP Server for Linux Administration Guide](#).

Users can access data storage on OES 2 servers through a number of methods. For more information, see [“Overview of File Services” on page 179](#).

### 13.3.3 NetWare 6.5 SP8 Options

NetWare 6.5 SP8 supports both the NetWare Traditional file system and Novell Storage Services (NSS).

- ♦ [“NetWare Traditional File System” on page 136](#)
- ♦ [“NSS Volumes” on page 136](#)

#### NetWare Traditional File System

After upgrading an older NetWare server to NetWare 6.5 SP8, it is possible for a NetWare Traditional file system volume to still reside on that server. Although you can continue to use Traditional volumes with NetWare 6.5 SP8, you will want to consider upgrading them to NSS to support a data migration to OES 2.

#### 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 SP2: NSS File System Administration Guide](#).

## 13.4 Configuring and Maintaining Storage

- ♦ [Section 13.4.1, “Managing Directories and Files,” on page 137](#)
- ♦ [Section 13.4.2, “Managing NSS,” on page 137](#)
- ♦ [Section 13.4.3, “Optimizing Storage Performance,” on page 138](#)

## 13.4.1 Managing Directories and Files

To learn about managing directories and files on an OES 2 server, see “[Understanding Directory Structures in Linux POSIX File Systems](#)” in the *OES 2 SP2: File Systems Management Guide*.

## 13.4.2 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.        | <a href="#">OES 2 SP2: Novell Archive and Version Services 2.1 for Linux Administration Guide</a>                                                  |
| Compression                     | Conserve disk space and increase the amount of data a volume can store.                                                                                        | <a href="#">“Managing Compression on NSS Volumes”</a> in the <a href="#">OES 2 SP2: NSS File System Administration Guide</a>                       |
| Console Commands                | Manage NSS volumes at an NetWare 6.5 SP8 server console, or an OES 2 terminal console via the NSS Console ( <code>nsscon</code> ) utility.                     | <a href="#">“NSS Commands”</a> and <a href="#">“NSS Utilities”</a> in the <a href="#">OES 2 SP2: NSS File System Administration Guide</a>          |
| 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. | <a href="#">OES 2 SP2: Novell Distributed File Services Administration Guide</a>                                                                   |
| Encryption                      | Create and manage encrypted NSS volumes that make data inaccessible to software that circumvents normal access control.                                        | <a href="#">“Managing Encrypted NSS Volumes”</a> in the <a href="#">OES 2 SP2: NSS File System Administration Guide</a>                            |
| 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.                  | <a href="#">“Using EVMS to Manage Devices with NSS Volumes (Linux)”</a> in the <a href="#">OES 2 SP2: NSS File System Administration Guide</a>     |
| Hard Links                      | Create multiple names for a single file in the same or multiple directories in an NSS volume.                                                                  | <a href="#">“Managing Hard Links”</a> in the <a href="#">OES 2 SP2: NSS File System Administration Guide</a>                                       |
| Monitoring                      | Monitor NSS file systems.                                                                                                                                      | <a href="#">“Monitoring the Status of the NSS File System and Services”</a> in the <a href="#">OES 2 SP2: NSS File System Administration Guide</a> |
| Multipath Support (NetWare)     | Manage the dynamic, multiple, redundant connection paths NSS creates between a NetWare server and its external storage devices.                                | <a href="#">“Managing Multipath I/O to Devices (NetWare)”</a> in the <a href="#">OES 2 SP2: NSS File System Administration Guide</a>               |

| Category/Feature                    | Description                                                                                                                                                           | Link                                                                                                                                                                |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Partitions                          | Manage partitions on NSS volumes.                                                                                                                                     | <a href="#">“Managing Partitions” in the OES 2 SP2: NSS File System Administration Guide</a>                                                                        |
| Pools                               | Create and manage NSS pools.                                                                                                                                          | <a href="#">“Managing NSS Pools” in the OES 2 SP2: NSS File System Administration Guide</a>                                                                         |
| Quotas                              | Set space restrictions for users and directories to control storage usage.                                                                                            | <a href="#">“Managing Space Quotas for Volumes, Directories, and Users” in the OES 2 SP2: NSS File System Administration Guide</a>                                  |
| Salvage subsystem                   | Use the salvage subsystem to make deleted files and directories available for undelete or purge actions.                                                              | <a href="#">“Salvaging and Purging Deleted Volumes, Directories, and Files” in the OES 2 SP2: NSS File System Administration Guide</a>                              |
| Tools                               | Learn about the various tools available to manage NSS volumes, the tool capabilities, and how to use them.                                                            | <a href="#">“Management Tools for NSS” in the OES 2 SP2: NSS File System Administration Guide</a>                                                                   |
| Troubleshooting                     | Troubleshoot NSS on OES 2 and NetWare 6.5 SP8.                                                                                                                        | <a href="#">“Troubleshooting the NSS File System” in the OES 2 SP2: NSS File System Administration Guide</a>                                                        |
| 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. | <a href="#">“Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes” in the OES 2 SP2: NSS File System Administration Guide</a> |
| Volumes                             | Create and manage NSS volumes in NSS pools.                                                                                                                           | <a href="#">“Managing NSS Volumes” in the OES 2 SP2: NSS File System Administration Guide</a>                                                                       |

### 13.4.3 Optimizing Storage Performance

See [“Tuning NSS Performance on Linux”](#) in the *OES 2 SP2: NSS File System Administration Guide*.

# eDirectory, LDAP, and Domain Services for Windows

# 14

This section discusses the following topics:

- ♦ [Section 14.1, “Overview of Directory Services,” on page 139](#)
- ♦ [Section 14.2, “eDirectory,” on page 140](#)
- ♦ [Section 14.3, “LDAP \(eDirectory\),” on page 141](#)
- ♦ [Section 14.4, “Domain Services for Windows,” on page 142](#)

## 14.1 Overview of Directory Services

Storing and managing network identities in directory services is a fundamental expectation for networking.

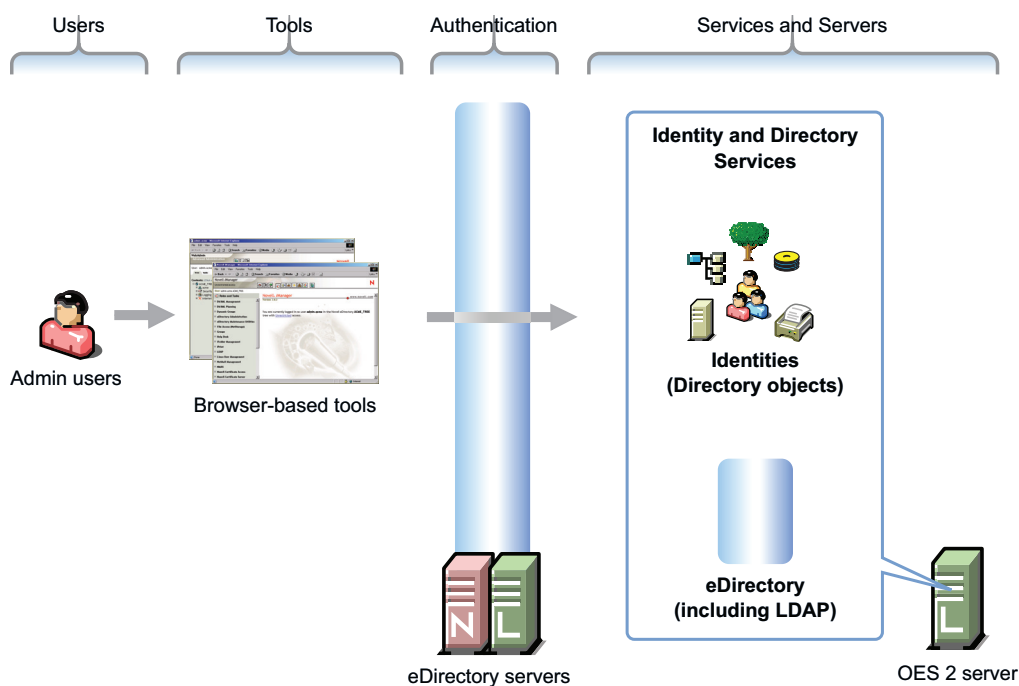
In the simplest terms, Novell® eDirectory™ is a tree structure containing a list of objects (or identities) that represent network resources, such as the following:

- ♦ 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 and NetWare.

For more information, see [Chapter 14, “eDirectory, LDAP, and Domain Services for Windows,” on page 139](#).

**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 140](#)
- ♦ [Section 14.2.2, “Planning Your eDirectory Tree,” on page 141](#)
- ♦ [Section 14.2.3, “eDirectory Coexistence and Migration,” on page 141](#)

### 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 140](#)
- ♦ [“iManager” on page 141](#)

#### OES Installation Programs

OES requires that eDirectory be installed by using the NetWare<sup>®</sup> Install or the YaST-based install for OES.

---

**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 2.7.3 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.

For those who are new to eDirectory, the [OES 2 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 What's 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 includes eDirectory 8.8. For those upgrading an existing 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 SP5](#)” 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 142](#)

- ♦ [Section 14.3.2, “Planning eDirectory LDAP Services,” on page 142](#)
- ♦ [Section 14.3.3, “Migration of eDirectory LDAP Services,” on page 142](#)
- ♦ [Section 14.3.4, “eDirectory LDAP Implementation Suggestions,” on page 142](#)

### 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:

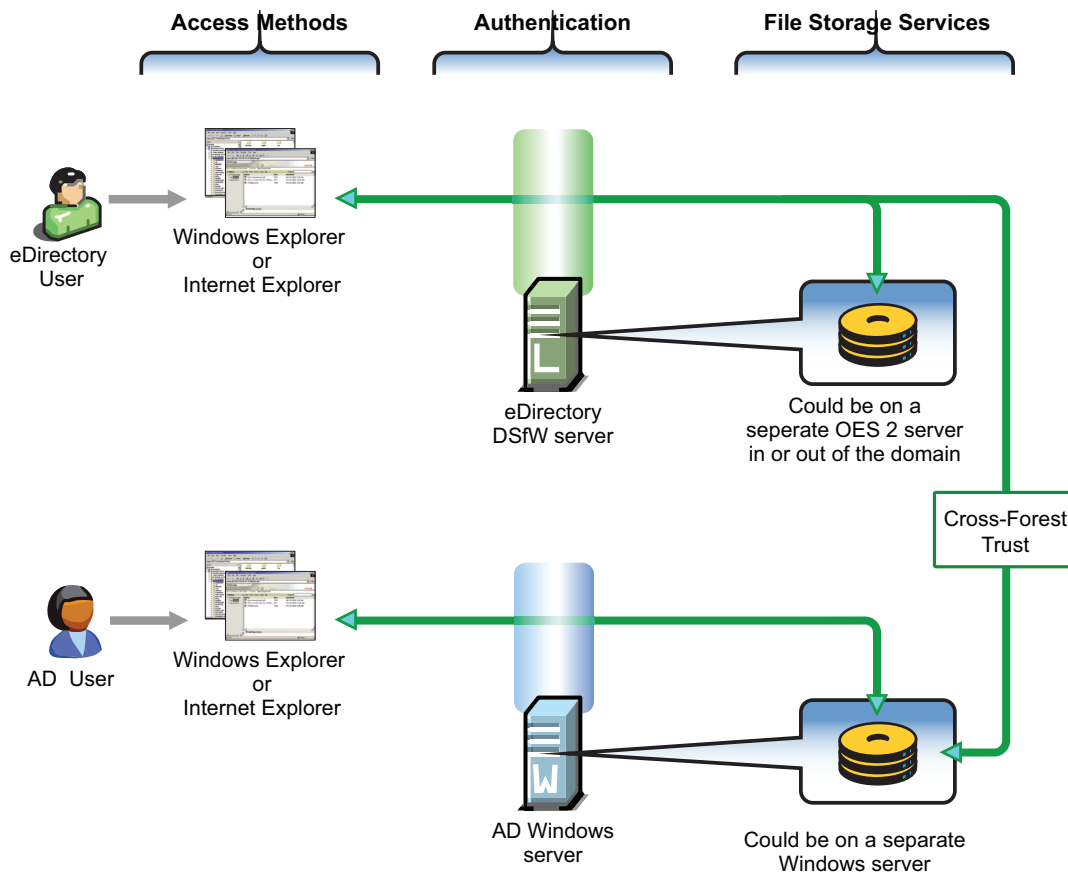
- ♦ [Section 14.4.1, “Graphical Overview of DSfW,” on page 143](#)
- ♦ [Section 14.4.2, “Planning Your DSfW Implementation,” on page 146](#)
- ♦ [Section 14.4.3, “Implementing DSfW on Your Network,” on page 146](#)

## 14.4.1 Graphical Overview of DSfW

- ♦ “File Access” on page 143
- ♦ “User Management” on page 144
- ♦ “Storage Management” on page 145

### File Access

**Figure 14-2** DSfW File Access Overview

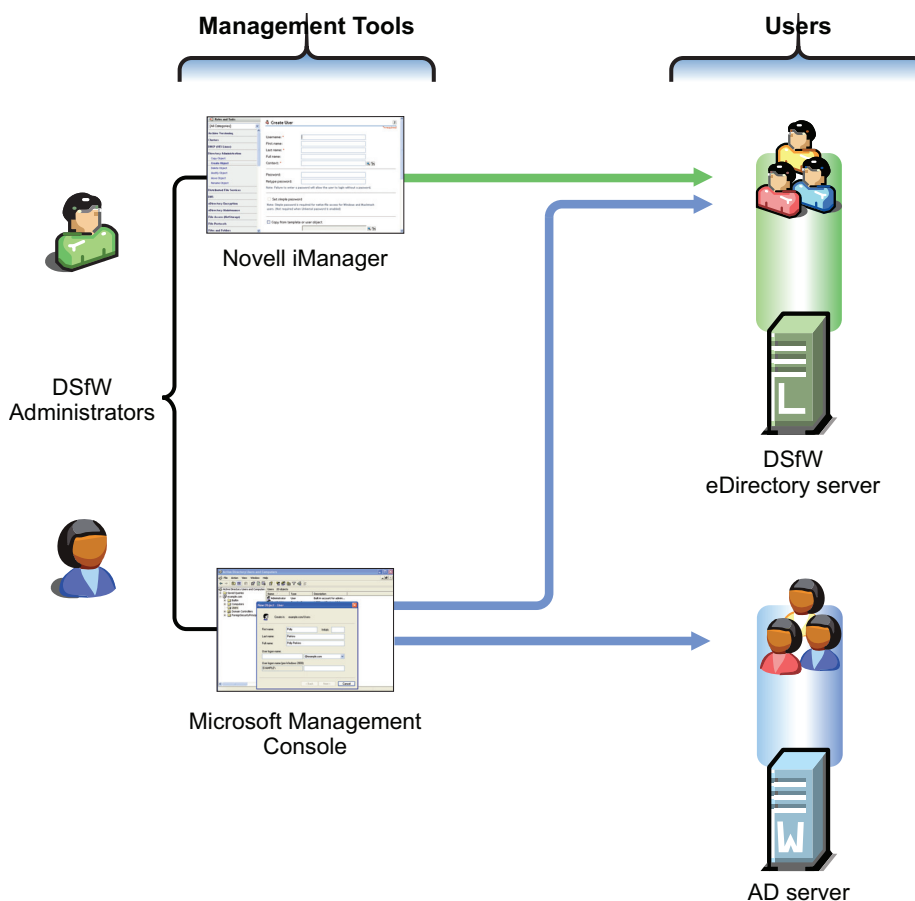


**Table 14-1** *DSfW File Access*

| 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*

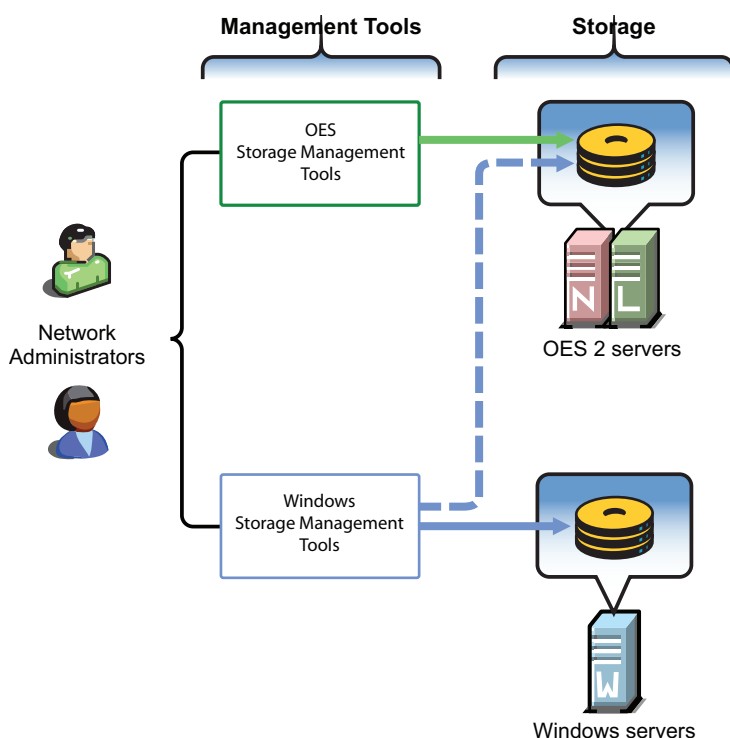


**Table 14-2** *DSfW User Management*

| 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 SP2: 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 SP2: Domain Services for Windows Administration Guide](#), especially the “[Troubleshooting DSfW](#)” section.

- ♦ “[Universal Password in a Name-Mapped Scenario](#)” on page 146
- ♦ “[DSfW Must Be Installed at the Root of an eDirectory Partition](#)” on page 146
- ♦ “[Hierarchical Placement of Users in the eDirectory Tree](#)” on page 147
- ♦ “[OES 2 Service Limitations](#)” on page 147
- ♦ “[Domain and Container Names Must Match](#)” on page 147
- ♦ “[Install DSfW on a New OES 2 Server When Possible](#)” on page 147
- ♦ “[DNS Configuration](#)” on page 147

### 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 SP2: 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 “[Container is Partitioned](#)” in the *OES 2 SP2: Domain Services for Windows Administration Guide*.

## Install DSfW on a New OES 2 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.



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 149](#)
- ♦ [Section 15.2, “Linux User Management: Access to Linux for eDirectory Users,” on page 149](#)
- ♦ [Section 15.3, “Identity Management Services,” on page 158](#)
- ♦ [Section 15.4, “Using the Identity Manager 3.6.1 Bundle Edition,” on page 158](#)

## 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 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 can manage through eDirectory.

The *Lab Guide for OES 2* 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 SP2: 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 150](#)
- ♦ [Section 15.2.2, “Planning,” on page 155](#)
- ♦ [Section 15.2.3, “LUM Implementation Suggestions,” on page 155](#)

## 15.2.1 Overview

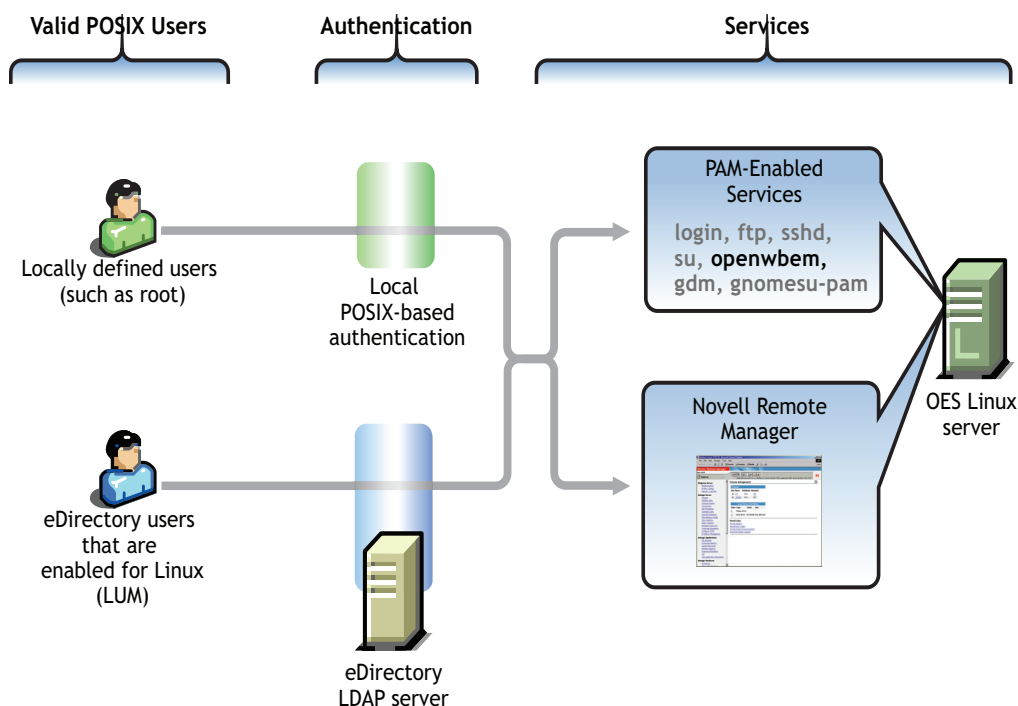
The topics in this section are designed to help you understand when LUM-enabled access is required so that your network services are accessible and work as expected. For more information about Linux User Management, see “Overview” in the *OES 2 SP2: Novell Linux User Management Technology Guide*.

- ♦ “A Graphical Preview of Linux User Management” on page 150
- ♦ “Linux Requires POSIX Users” on page 151
- ♦ “Linux Users Can Be Local or Remote” on page 151
- ♦ “The root User Is Never LUM-Enabled” on page 151
- ♦ “About Service Access on OES 2” on page 152
- ♦ “Services in OES 2 That Require LUM-Enabled Access” on page 152
- ♦ “Services That Do Not Require LUM-Enabled Access But Have Some LUM Requirements” on page 153
- ♦ “Services That Do Not Require LUM-enabled Access” on page 154
- ♦ “LUM-Enabling Does Not Provide Global Access to ALL OES 2 Servers” on page 154

### 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 servers must be accessed by POSIX users.<br><br>eDirectory users can function as POSIX users if they are enabled for Linux access (LUM). | 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.<br><br>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 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 6.2, “Avoiding POSIX and eDirectory Duplications,” on page 62](#).

- 
- ♦ **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 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

Novell Linux User Management (LUM) lets you use eDirectory to centrally manage remote users for access to one or more OES 2 servers.

In other words, LUM lets eDirectory users function as local (POSIX) users on an OES 2 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 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 155](#).

## Services in OES 2 That Require LUM-Enabled Access

Some services on an OES 2 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 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 Limitations,” on page 221](#).

---

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"><li>♦ OES 2 server</li><li>♦ SSH session with OES 2 server</li></ul> | 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"> <li>♦ Local host</li> <li>♦ Remote host</li> </ul>                     | 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"> <li>♦ OES 2 server</li> <li>♦ SSH session with OES 2 server</li> </ul> | <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 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 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 SP2," on page 257](#).

- ♦ **NSS:** eDirectory users that access NSS volumes directly through NCP (the Novell Client™) are not required to be LUM-enabled.

However, because Novell Samba accesses NSS through the virtual file system layer that makes NSS appear to be a POSIX-compliant file system, Samba users must be LUM-enabled to access an NSS volume.

### **Services That Do Not Require LUM-enabled Access**

The following end user services do not require LUM-enabled access:

- ♦ iFolder 3.8
- ♦ iPrint
- ♦ NCP Client to an NCP Volume
- ♦ NCP Client to an NSS Volume
- ♦ Novell AFP
- ♦ Novell CIFS
- ♦ QuickFinder™

### **LUM-Enabling Does Not Provide Global Access to ALL OES 2 Servers**

As you plan to LUM-enable users for access to the services that require it, keep in mind that each OES 2 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 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 Servers" on page 156](#).

For more information on LUM, see the [OES 2 SP2: 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 155](#)
- ♦ [“Planning Which Users to Enable for Access” on page 155](#)
- ♦ [“Be Aware of System-Created Users and Groups” on page 155](#)

### eDirectory Admin User Is Automatically Enabled for Linux Access

When you install Linux User Management on an OES 2 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 servers that require LUM-enabled users.

This can be easily determined by doing the following:

1. Review the information in [“Services in OES 2 That Require LUM-Enabled Access” on page 152](#).
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 SP2,” on page 257](#).

## 15.2.3 LUM Implementation Suggestions

The following sections summarize LUM implementation considerations.

- ♦ [“About Enabling eDirectory Users for Linux Access” on page 155](#)
- ♦ [““UNIX Workstation” and “Linux Workstation” Are the Same Thing” on page 156](#)
- ♦ [“Enabling Users to Access Multiple OES 2 Servers” on page 156](#)
- ♦ [“Enabling eDirectory Groups for Linux Access” on page 156](#)
- ♦ [“Enabling eDirectory Users for Linux Access” on page 157](#)

### 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 servers or Linux workstations. For more information, see [“Enabling Users to Access Multiple OES 2 Servers” on page 156](#).

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 SP2: Novell Linux User Management Technology Guide*.

## “UNIX Workstation” and “Linux Workstation” Are the Same Thing

When you use iManager to manage OES 2 access, you might notice some inconsistencies in naming.

When OES 2 servers are created, a “UNIX Workstation - *server\_name*” object is created in eDirectory, where *server\_name* is the DNS name of the OES 2 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 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 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 156](#)
- ♦ [“Using LUM Utilities at the Command Prompt” on page 157](#)

### 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 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 SP2: 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 SP2: 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 157
- ♦ “[Using LUM Utilities at the Command Prompt](#)” on page 157

### 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 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 SP2: 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 SP2: 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 servers by using the NCP server for Linux and iPrint services. For more information, see [Section 17.6, “NCP Implementation and Maintenance,”](#) on page 200 and [Chapter 19, “Print Services,”](#) on page 209.
- ♦ If you want eDirectory users to have access to OES 2 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 149.
- ♦ 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 3.6.1 Bundle Edition,”](#) on page 158.

## 15.4 Using the Identity Manager 3.6.1 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 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 159
- ♦ [Section 15.4.2, “System Requirements,”](#) on page 159
- ♦ [Section 15.4.3, “Installation Considerations,”](#) on page 159
- ♦ [Section 15.4.4, “Getting Started,”](#) on page 159
- ♦ [Section 15.4.5, “Activating the Bundle Edition,”](#) on page 160

## 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

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 would like 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 160.

## 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 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](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) (<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](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*.

## Frequently Asked Questions about Activation

### 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 DirXML 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.

### 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 \(http://www.novell.com/documentation/idm35/install/data/agftax.html\)](http://www.novell.com/documentation/idm35/install/data/agftax.html).

# Access Control and Authentication

# 16

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 163](#)
- ♦ [Section 16.2, “Authentication Services,” on page 174](#)

## 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 163](#)
- ♦ [Section 16.1.2, “Planning for Service Access,” on page 169](#)
- ♦ [Section 16.1.3, “Coexistence and Migration of Access Services,” on page 172](#)
- ♦ [Section 16.1.4, “Access Implementation Suggestions,” on page 172](#)
- ♦ [Section 16.1.5, “Configuring and Administering Access to Services,” on page 172](#)

### 16.1.1 Overview of Access Control

The following sections present overviews of methods for accessing Open Enterprise Server 2 services.

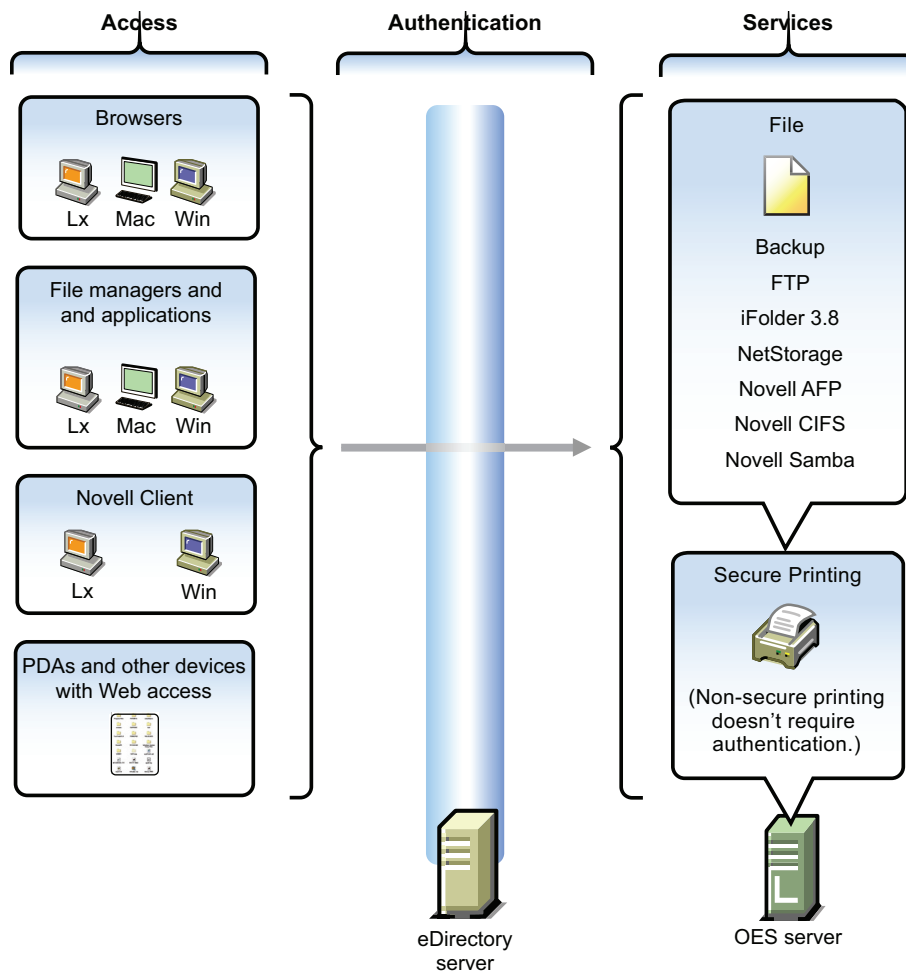
- ♦ [“Access to OES 2 Services” on page 164](#)
- ♦ [“Access Control Options in OES 2” on page 165](#)
- ♦ [“The Traditional Novell Access Control Model” on page 166](#)
- ♦ [“NSS Access Control on OES” on page 167](#)

- ♦ “Novell Client (NCP File Services) Access” on page 168
- ♦ “eDirectory User Access to OES 2 Servers” on page 169

## 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 171](#).

## 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. | <a href="http://www.novell.com/documentation/sles10/sles_admin/data/cha_acls.html">“Access Control Lists in Linux” (http://www.novell.com/documentation/sles10/sles_admin/data/cha_acls.html)</a> in the <i>SLES 10 SP3: Installation and Administration Guide</i> ( <a href="http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html">http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html</a> ) |
| Aligning NCP and POSIX access rights                    | How to approximate the NCP (or NetWare) access control model on POSIX file systems.                                                                                                      | <a href="#">“Section 17.4, “Aligning NCP and POSIX File Access Rights,” on page 195”</a>                                                                                                                                                                                                                                                                                                                                                   |
| Directory and file attributes                           | Directory and file attributes on NSS volumes.                                                                                                                                            | <a href="#">“Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes”</a> in the <i>OES 2 SP2: File Systems Management Guide</i>                                                                                                                                                                                                                                                                                      |
| File system trustee rights                              | File system trustee rights on NetWare (NSS and traditional volumes), including how effective file system trustee rights are determined.                                                  | <a href="#">“File-System Trustee Rights ”</a> in the <i>OES 2 SP2: File Systems Management Guide</i>                                                                                                                                                                                                                                                                                                                                       |
| Novell trustee rights and directory and file attributes | How to control who can see which files and what they can do with them.                                                                                                                   | <a href="#">“Understanding File System Access Control Using Trustees”</a> in the <i>OES 2 SP2: File Systems Management Guide</i>                                                                                                                                                                                                                                                                                                           |
| POSIX file system rights and attributes on Linux        | How to configure file system attributes on OES 2 servers.                                                                                                                                | <a href="http://www.novell.com/documentation/sles10/sles_admin/data/cha_acls.html">“Access Control Lists in Linux” (http://www.novell.com/documentation/sles10/sles_admin/data/cha_acls.html)</a> in the <i>SLES 10 SP3: Installation and Administration Guide</i> ( <a href="http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html">http://www.novell.com/documentation/sles10/sles_admin/data/sles_admin.html</a> ) |

| Feature                            | To Understand                                      | See                                                                                                                  |
|------------------------------------|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Security Equivalence in eDirectory | The concept of Security Equivalence in eDirectory. | <a href="#">“eDirectory Objects and Security Equivalence”</a> in the <i>OES 2 SP2: File Systems Management Guide</i> |

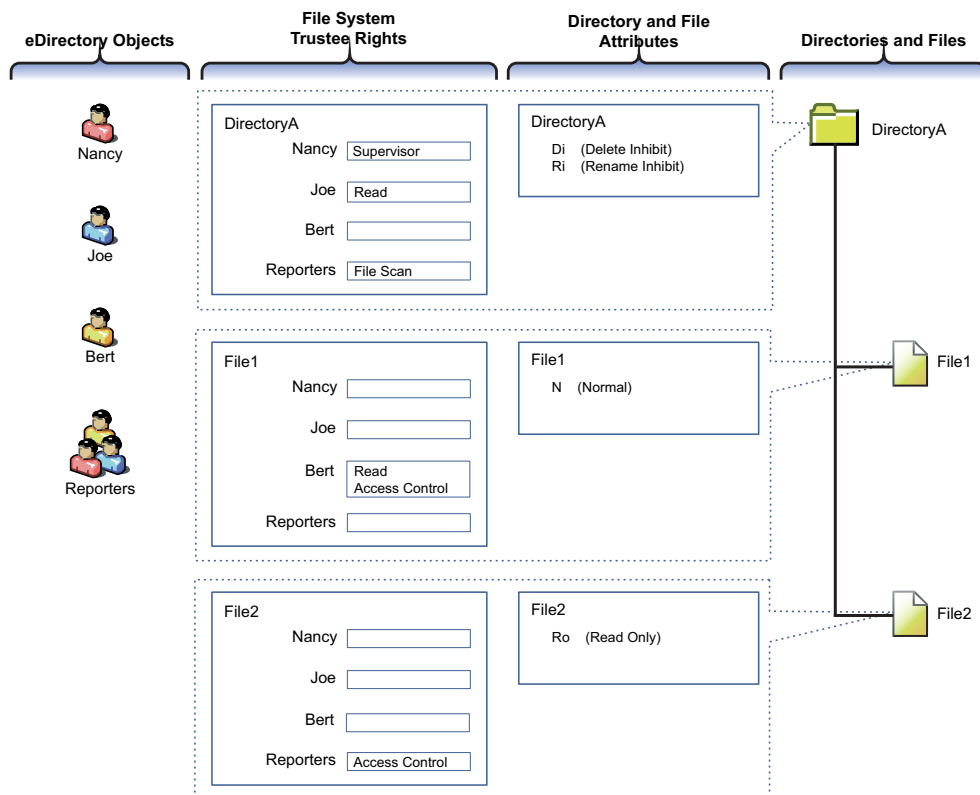
## The Traditional Novell Access Control Model

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 Novell 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"> <li>♦ 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.</li> </ul> <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"> <li>♦ 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.</li> </ul> <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"> <li>♦ 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.</li> </ul> <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"> <li>♦ Because all three users are members of the Reporters group, they can grant any eDirectory user access to File2.</li> </ul> <p>Of course, for Nancy this is redundant because she has the Supervisor right at the directory level.</p> |

## NSS Access Control on OES

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<br><br>This applies only to OES servers, not NetWare.                                                                                    | The difference between Independent Mode access and NetWare Mode access.                               | <a href="#">“Access Control for NSS on Linux”</a> in the <i>OES 2 SP2: File Systems Management Guide</i>                                             |
| POSIX directory and file attributes on NSS volumes on OES 2<br><br>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. | <a href="#">“Displaying Key NSS Directory and File Attributes as Linux POSIX Permissions”</a> in the <i>OES 2 SP2: 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 168
- ♦ [“Is the Novell Client Right for Your Network?”](#) on page 168
- ♦ [“Differences between Linux and Windows”](#) on page 169

### About the Novell Client

The Novell Client extends the capabilities of Windows and Linux desktops with access to NetWare and OES 2 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<sup>®</sup> 3.8, 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 you or 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 SP3 for Linux Administration Guide*.

## eDirectory User Access to OES 2 Servers

Some services that run on OES 2 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 149.

## 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 169
- ♦ “[Planning Print Service Access](#)” on page 170
- ♦ “[Matching Protocols and Services to Check Access Requirements](#)” on page 171

### 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 169
- ♦ “[Feature Support](#)” on page 170

### 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         |
|--------------|------------------------------|------------------------------|
| AFP          | No                           | Yes-Novell AFP               |
| CIFS         | Yes-Novell CIFS Novell Samba | Yes-Novell CIFS Novell Samba |

| File Service                | Linux POSIX Volumes | NSS Volumes on Linux |
|-----------------------------|---------------------|----------------------|
| NetStorage                  | Yes                 | Yes                  |
| NetWare Core Protocol (NCP) | Yes                 | Yes                  |
| NFS                         | Yes                 | Yes-NFSv3            |
| Novell iFolder 2.1x         | No                  | No                   |
| Novell iFolder 3.8          | Yes                 | Yes                  |

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 171](#).

## Feature Support

**Table 16-5** *Features Supported on Each Volume Type*

| Feature                              | Linux POSIX Volumes                    | NSS Volumes on Linux |
|--------------------------------------|----------------------------------------|----------------------|
| Directory quotas                     | No                                     | Yes                  |
| Login scripts                        | Yes (if also defined as an NCP volume) | Yes                  |
| Mapped drives                        | Yes (if also defined as an NCP volume) | Yes                  |
| Novell directory and file attributes | No                                     | Yes                  |
| Purge/Salvage                        | No                                     | Yes                  |
| Trustee rights                       | Yes (if also defined as an NCP volume) | Yes                  |
| User space quotas                    | No                                     | 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 [“Setting Access Control for Your Print System”](#) in the *OES 2 SP2: iPrint for Linux Administration Guide*

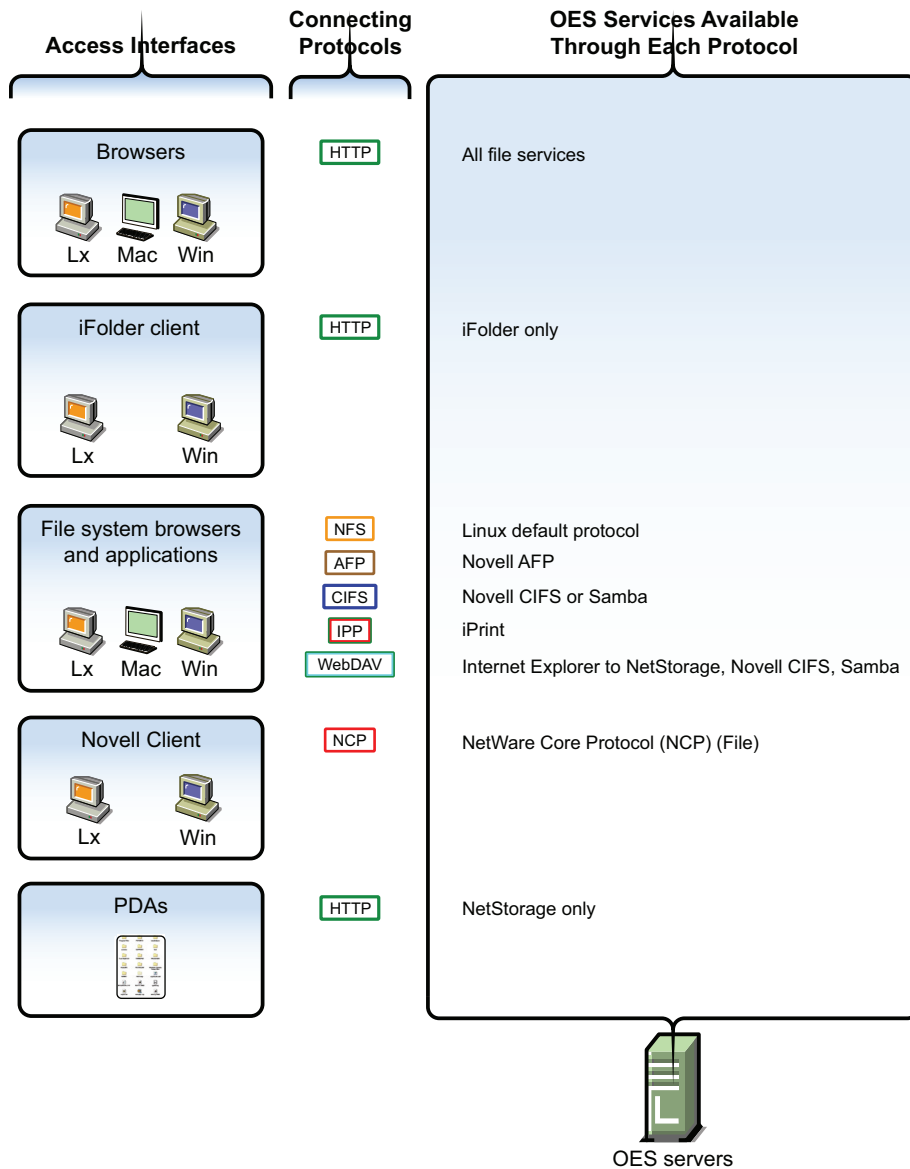
## Matching Protocols and Services to Check Access Requirements

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 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 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. 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 SP2: 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 247.

### 16.1.5 Configuring and Administering Access to Services

The following sections discuss administering access to services.

- ♦ [“Password Management”](#) on page 172
- ♦ [“Linux \(POSIX\) File System Access Rights”](#) on page 172
- ♦ [“NSS File and Directory Trustee Management”](#) on page 173

#### 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 SP2: File Systems Management Guide*.

## NSS File and Directory Trustee Management

The *OES 2 SP2: 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 173
- “[Using the Novell Client to Change File and Directory Attributes and Trustee Rights](#)” on page 173
- “[Using iManager 2.7 to Change File and Directory Attributes and Trustee Rights](#)” on page 173
- “[Using the Linux Command Prompt to Change File Attributes](#)” on page 173
- “[Using the Linux Command Prompt to Change Trustee Rights](#)” on page 174

### 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.

### 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 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 SP3 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 SP2: 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 SP2: 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 174](#)
- [Section 16.2.2, “Planning for Authentication,” on page 177](#)
- [Section 16.2.3, “Authentication Coexistence and Migration,” on page 177](#)
- [Section 16.2.4, “Configuring and Administering Authentication,” on page 177](#)

### 16.2.1 Overview of Authentication Services

This section provides specific overview information for the following key OES components:

- [“NetIdentity Agent” on page 174](#)
- [“Novell Modular Authentication Services \(NMAS\)” on page 175](#)
- [“Password Support in OES 2” on page 176](#)

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 eDirectory authentication to NetStorage through a secure identity “wallet” on the workstation.

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<sup>®</sup> 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](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 “ <a href="#">Creating a Universal Password Policy to Support Both AFP and CIFS</a> ” in the <i>OES 2 SP2: Lab Guide for Linux and Virtualized NetWare</i> . More information about password policy planning is available in <a href="#">Appendix K, “Coordinating Password Policies Among Multiple File Services,”</a> on page 279.                                                                                                                                                                                                                                                                                                                                                                    |
| 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 “<a href="#">Samba Passwords</a>” in the <i>OES2 SP2: Samba Administration Guide</i>.</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 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 “<a href="#">Deploying Universal Password</a>” 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 217](#) and [Chapter 22, “Certificate Management,” on page 225](#)” 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.



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 179](#)
- ♦ [Section 17.2, “Planning for File Services,” on page 189](#)
- ♦ [Section 17.3, “Coexistence and Migration of File Services,” on page 193](#)
- ♦ [Section 17.4, “Aligning NCP and POSIX File Access Rights,” on page 195](#)
- ♦ [Section 17.5, “PureFTP Remote Access Implementation,” on page 198](#)
- ♦ [Section 17.6, “NCP Implementation and Maintenance,” on page 200](#)
- ♦ [Section 17.7, “NetStorage Implementation and Maintenance,” on page 202](#)
- ♦ [Section 17.8, “Novell AFP Implementation and Maintenance,” on page 204](#)
- ♦ [Section 17.9, “Novell CIFS Implementation and Maintenance,” on page 204](#)
- ♦ [Section 17.10, “Novell iFolder 3.8 Implementation and Maintenance,” on page 205](#)
- ♦ [Section 17.11, “Samba Implementation and Maintenance,” on page 206](#)

## 17.1 Overview of File Services

The file service components in OES include the following:

- ♦ [FTP Services \(page 180\)](#): Lets users securely transfer files to and from OES 2 servers.
- ♦ [NetWare Core Protocol \(page 180\)](#): Provides NetWare Core Protocol™ (NCP™) access to NCP volumes (including NSS volumes) that you define on OES 2 server partitions.
- ♦ [NetStorage \(page 181\)](#): Provides network and Web access to various file services through common file service protocols, such as CIFS.  

The NetStorage server doesn't actually store files and folders. Rather, it provides access to other file services that support the native TCP/IP protocol.
- ♦ [Novell AFP \(page 184\)](#): Provides native Macintosh access to files stored on an NSS volume on an OES 2 server.
- ♦ [Novell CIFS \(page 185\)](#): Provides native Windows (CIFS and HTTP-WebDAV) access to files stored on an NSS volume on an OES 2 server.
- ♦ [Novell iFolder 3.8 \(page 186\)](#): 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 \(page 188\)](#): Provides Windows (CIFS and HTTP-WebDAV) access to files stored on an OES 2 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 189](#).

### 17.1.2 FTP Services

OES 2 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 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.

For migration instructions and a brief FAQ, see “[Migrating FTP from NetWare to OES 2 Linux](#)” in the *OES 2 SP2: 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).

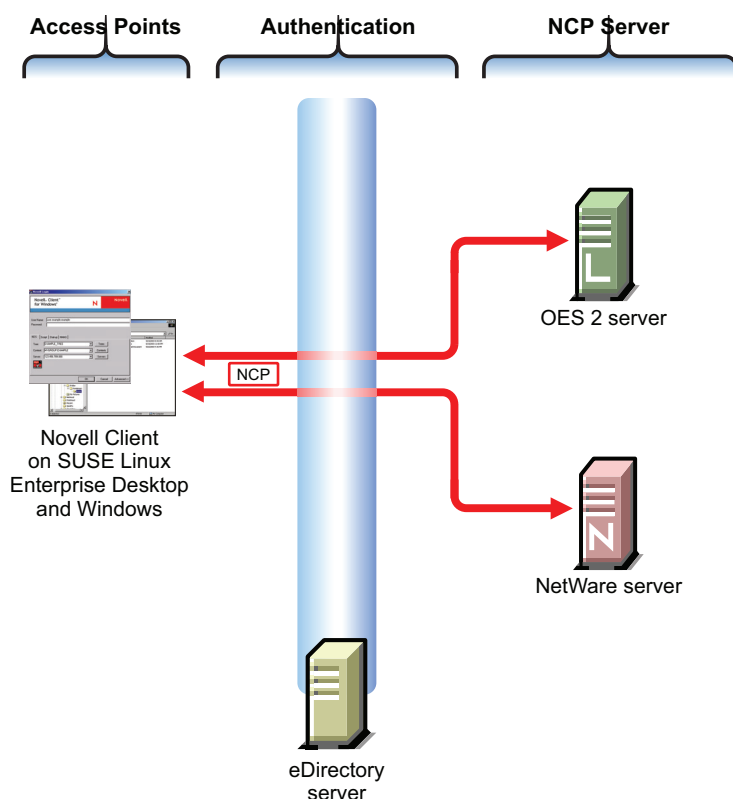
### 17.1.3 NetWare Core Protocol

NetWare Core Protocol (NCP) is the technology beneath many of the network services for which NetWare is famous.

In OES, 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 17-1](#) 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 163.

**Figure 17-1** NCP Services for Linux and NetWare



The following table explains the information illustrated in [Figure 17-1](#).

**Table 17-1** 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.<br><br>The same core set of NetWare file attributes are available on both Linux and NetWare. |

## 17.1.4 NetStorage

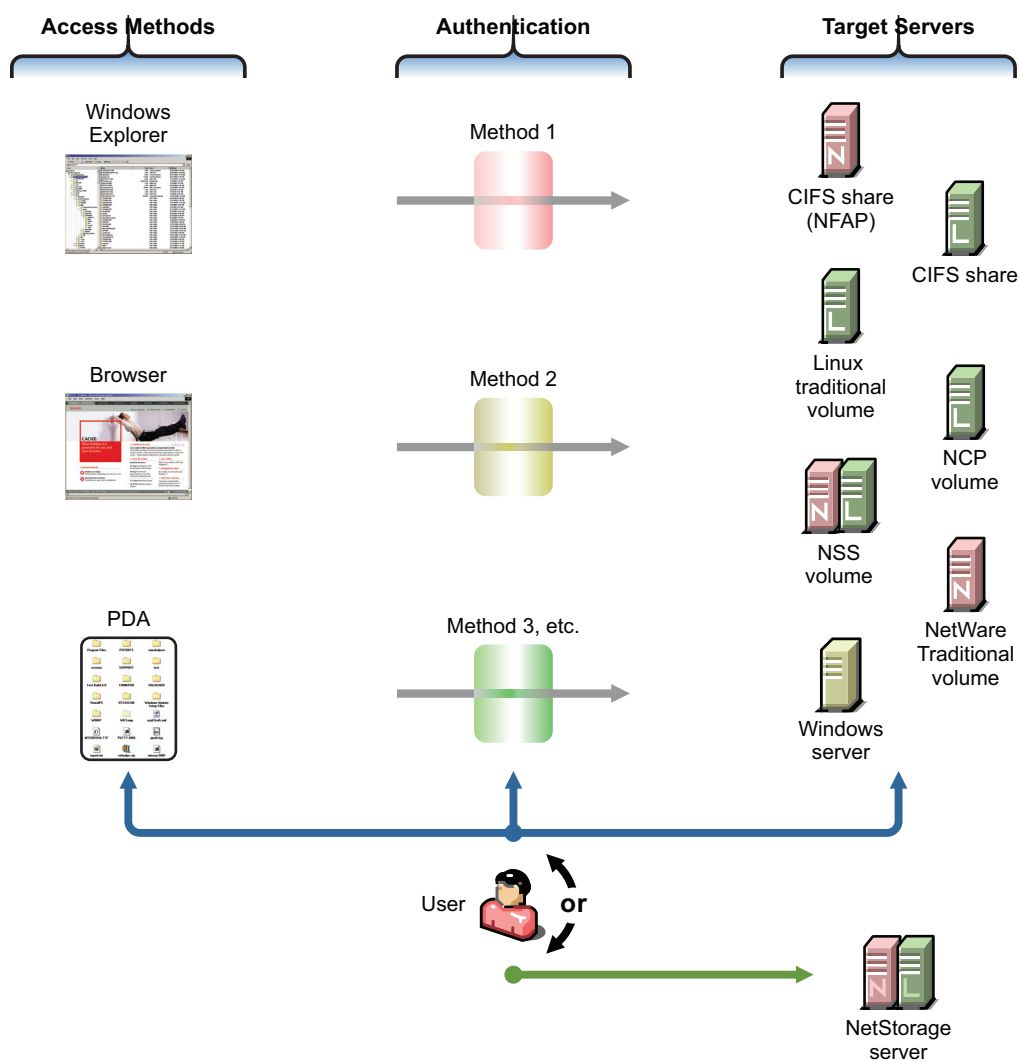
- ♦ [“Common Network File Storage Problems” on page 181](#)
- ♦ [“Novell NetStorage on Linux” on page 182](#)

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 17-2](#).

**Figure 17-2** Common Network File Storage Problems



The following table explains the information illustrated in [Figure 17-2](#).

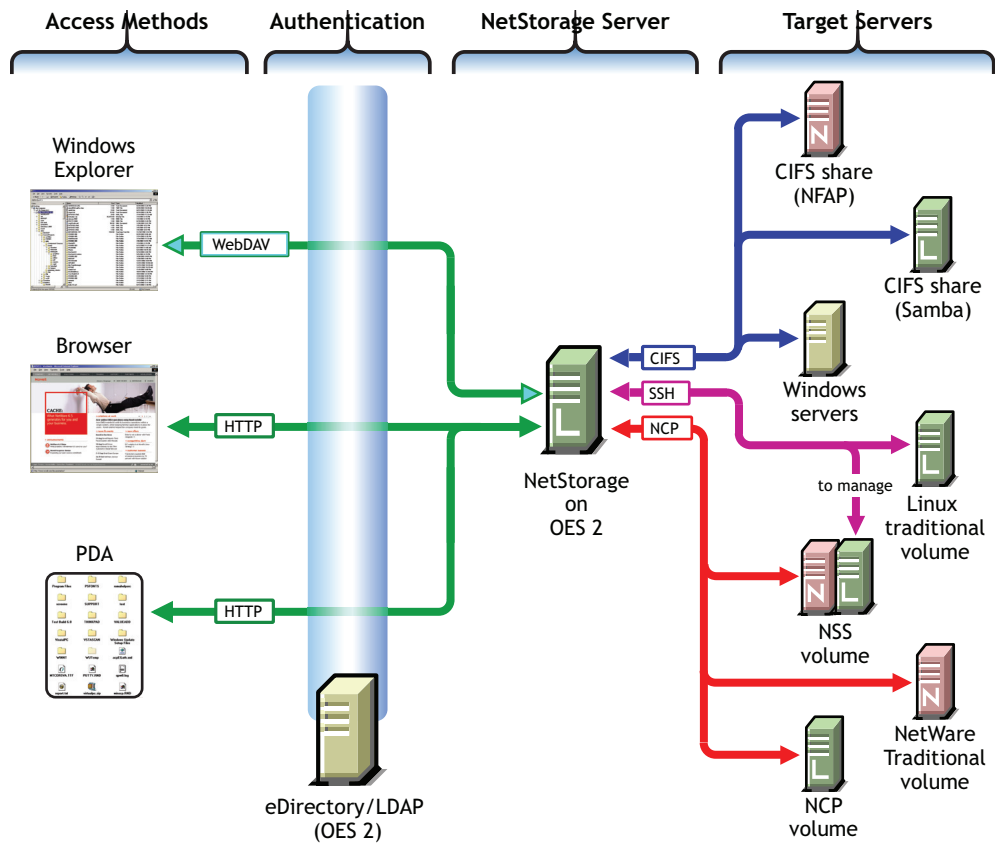
**Table 17-2** NetStorage Access Solutions

| 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 17-3](#)).

**Figure 17-3** *How NetStorage Works on OES 2*



The following table explains the information illustrated in [Figure 17-3](#).

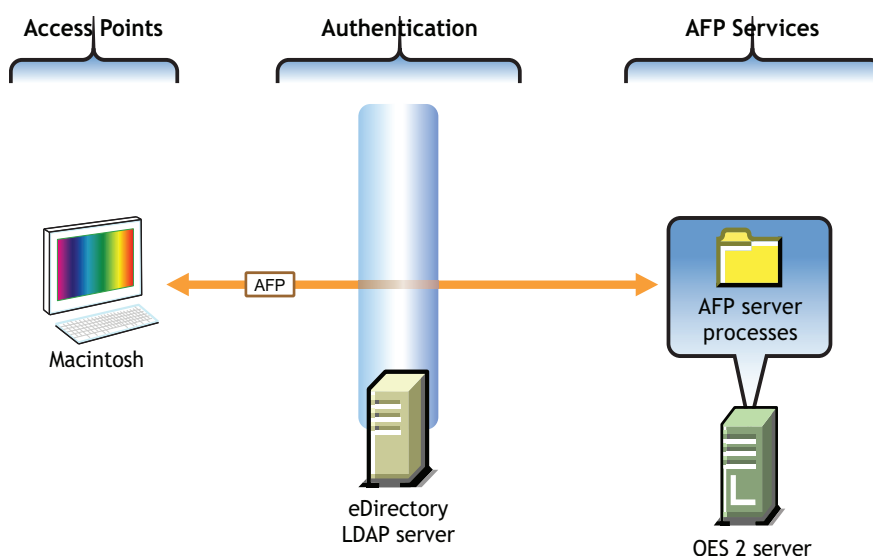
**Table 17-3** *NetStorage on Linux*

| Access Methods                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Authentication                                                                                                                                                                               | NetStorage Server                                                                                                                         | Target Servers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Users have read and write access to files from</p> <ul style="list-style-type: none"> <li>♦ <b>Windows Explorer:</b> Enabled by the HTTP protocol with WebDAV extensions.</li> <li>♦ <b>Browsers:</b> Users can access files directly by connecting to the NetStorage server.</li> <li>♦ <b>PDA:</b> PDA users with network connections can access their files as well.</li> </ul> <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"> <li>♦ Windows workgroup shares (CIFS or Samba shares)</li> <li>♦ Linux POSIX volumes through an SSH connection.</li> </ul> <p>Linux volumes can also be made available as NCP volumes.</p> <p>Management of NSS volumes on OES 2 through NetStorage requires SSH access to the server. See <a href="#">“When Is SSH Access Required?”</a> on page 94.</p> |

## 17.1.5 Novell AFP

The Novell AFP service lets users on Macintosh workstations access and store files on OES 2 servers with NSS volumes without installing any additional software, such as the Novell Client™ (see [Figure 17-4](#)).

**Figure 17-4** *How Novell AFP Works*



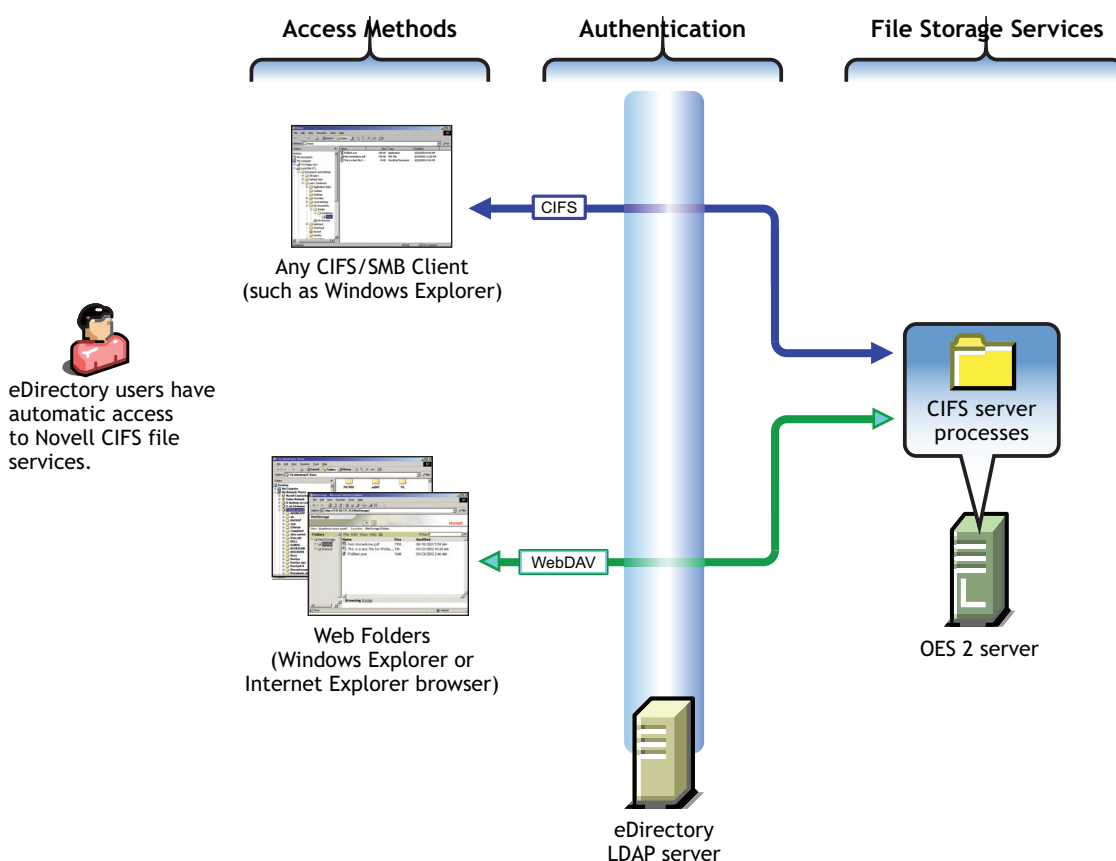
**Table 17-4** *AFP Access*

| 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.<br><br>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. |

## 17.1.6 Novell CIFS

The Novell CIFS service lets users on Windows workstations access and store files on OES 2 servers with NSS volumes without installing any additional software, such as the Novell Client (see [Figure 17-4](#)).

**Figure 17-5** *How Novell CIFS Works*



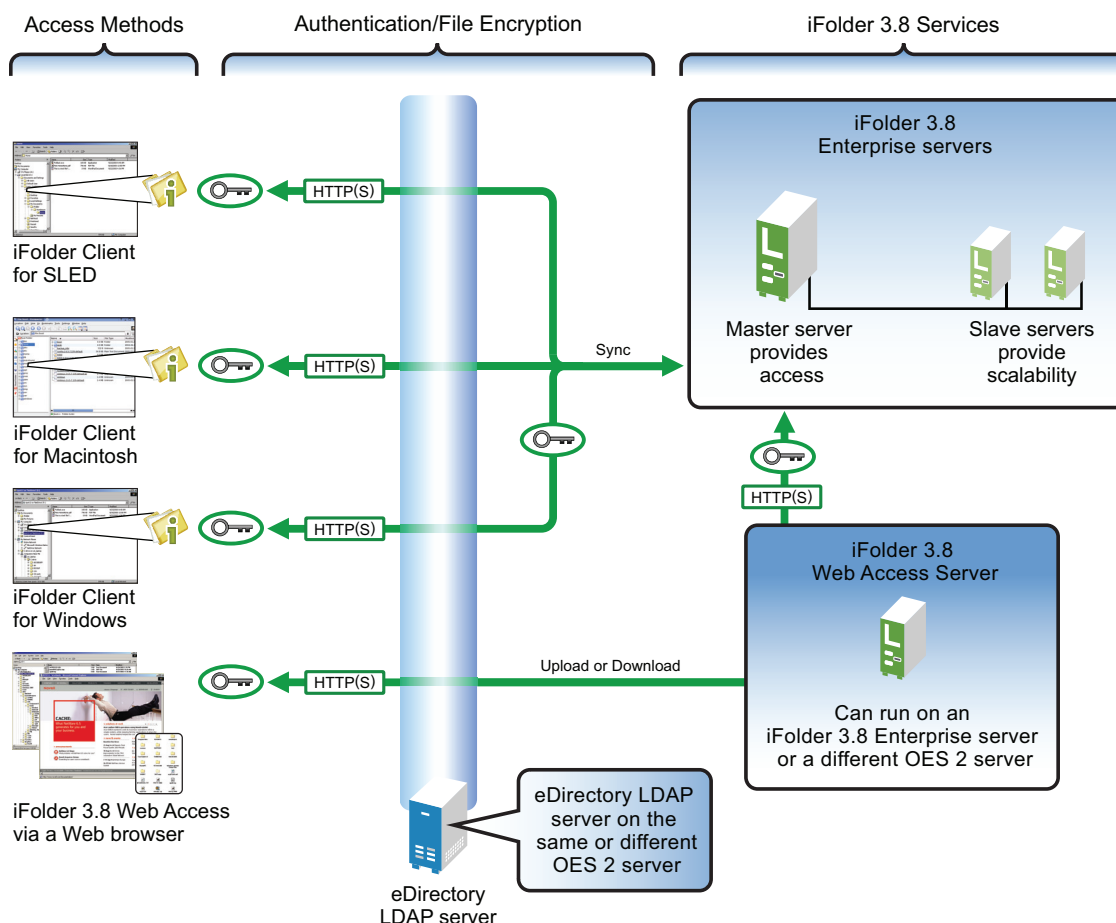
**Table 17-5** *CIFS Access*

| 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"> <li>♦ <b>CIFS Client Access:</b> Windows Explorer users can access and modify files on the OES 2 server just as they would on any workgroup server share.</li> <li>♦ <b>Web Folder:</b> Users can create Web Folders in Windows Explorer or Internet Explorer.</li> </ul> <p>Files on the OES 2 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> |

### 17.1.7 Novell iFolder 3.8

Novell iFolder 3.8 supports multiple iFolders per user, user-controlled sharing, and a centralized network server for file storage and secure distribution (see [Figure 17-6](#)).

**Figure 17-6** *How Novell iFolder Works*



The following table explains the information illustrated in [Figure 17-6](#).

**Table 17-6** *iFolder Access*

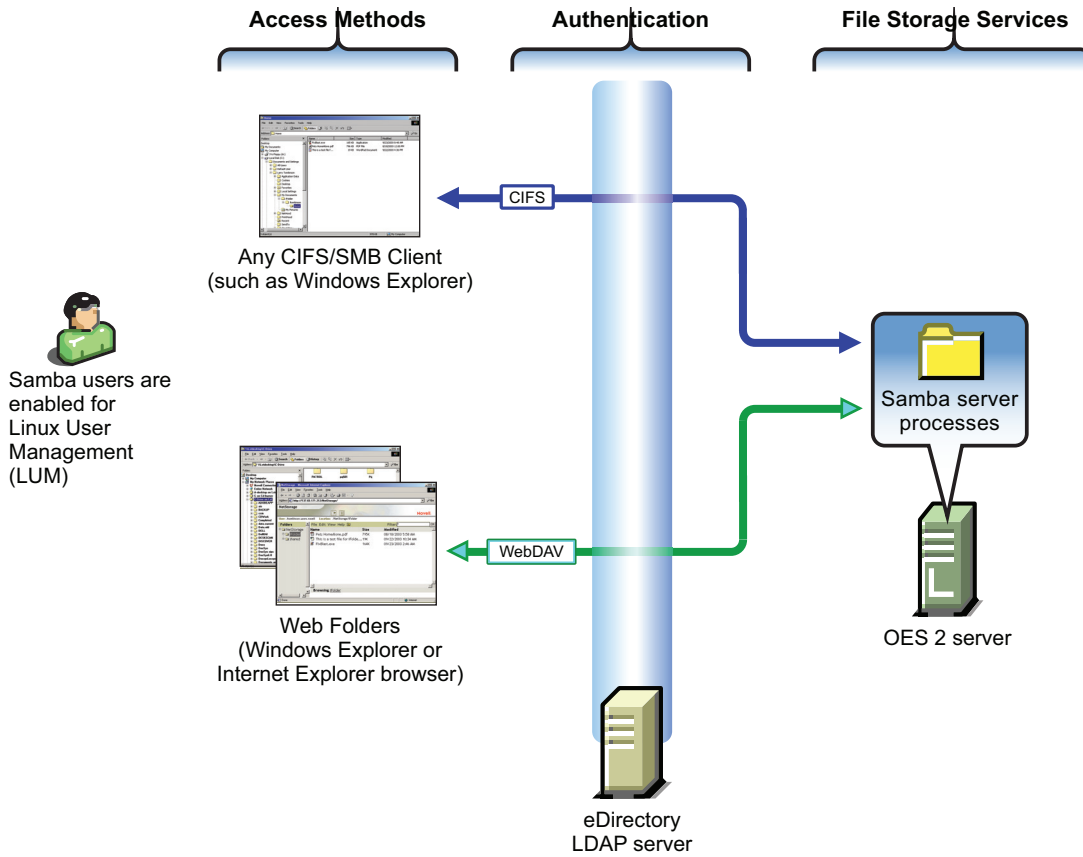
| Access Methods                                                                                                                                                                                                                               | Authentication/File Encryption                                                                                                                           | Novell iFolder 3.8 Services                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Linux, Mac, 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 3.8 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 Web interface lets users access their files from any computer with an active network or Internet connection.                                                                                                                               | Although shown separately, eDirectory could be installed on the OES 2 server.<br><br>Files can be encrypted for transport using SSL connections (HTTPS). | Local and network copies of each file are automatically synchronized by the Novell iFolder Client and Server pieces.       |

Additional overview information is available in “[Overview of Novell iFolder 3.7 and Later Versions](#)” in the *Novell iFolder 3.8 Administration Guide*.

## 17.1.8 Novell Samba

Samba on an OES 2 server provides Windows (CIFS and HTTP-WebDAV) access to files stored on the OES 2 server (see [Figure 17-7](#)).

**Figure 17-7** *How Samba on OES Works*



The following table explains the information illustrated in [Figure 17-7](#).

**Table 17-7** *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"> <li>♦ <b>CIFS Client Access:</b> Windows Explorer users can access and modify files on the Samba server just as they would on any workgroup server share.</li> <li>♦ <b>Web Folder:</b> Users can create Web Folders in Windows Explorer or Internet Explorer.</li> </ul> <p>Files on the OES 2 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 179.

- ♦ [Section 17.2.1, "Deciding Which Components Match Your Needs,"](#) on page 189
- ♦ [Section 17.2.2, "Comparing Your CIFS File Service Options,"](#) on page 190
- ♦ [Section 17.2.3, "Planning Your File Services,"](#) on page 192

### 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 17-8](#) to your network's file service requirements.

**Table 17-8** *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"> <li>♦ Any Linux volumes (including NSS) that are defined as NCP volumes</li> <li>♦ NetWare volumes</li> </ul> | <ul style="list-style-type: none"> <li>♦ eDirectory Authentication</li> </ul> |

| Service            | Access Method Features                                                                                                                                                                                                                                                            | Back-End Storage Features                                                                                                                                                                              | Security Features                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| NetStorage         | <ul style="list-style-type: none"> <li>Any <a href="#">supported browsers</a></li> <li>Personal Digital Assistant (PDA)</li> <li>Remote (browser-based)</li> <li>Web Folders (on either an Internet Explorer browser or in Windows Explorer)</li> <li>Windows Explorer</li> </ul> | <ul style="list-style-type: none"> <li>Linux POSIX volumes</li> <li>NetWare volumes</li> <li>NCP volumes</li> <li>NSS volumes</li> <li>Samba (CIFS) servers</li> <li>Windows (CIFS) servers</li> </ul> | <ul style="list-style-type: none"> <li>Secure LDAP Authentication</li> </ul>                                                                    |
| Novell AFP         | <ul style="list-style-type: none"> <li>Macintosh Chooser</li> </ul>                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>NSS volumes</li> </ul>                                                                                                                                          | <ul style="list-style-type: none"> <li>Secure LDAP Authentication</li> </ul>                                                                    |
| Novell CIFS        | <ul style="list-style-type: none"> <li>Any CIFS client</li> <li>Remote access (Web Folders in the Internet Explorer browser)</li> <li>Windows Explorer</li> </ul>                                                                                                                 | <ul style="list-style-type: none"> <li>NSS volumes</li> </ul>                                                                                                                                          | <ul style="list-style-type: none"> <li>Secure LDAP Authentication</li> </ul>                                                                    |
| Novell iFolder 3.8 | <ul style="list-style-type: none"> <li>Linux File Managers</li> <li>Macintosh Chooser</li> <li>Offline access with file synchronization (between local and network copies) on reconnect</li> <li>Web browsers</li> <li>Windows Explorer</li> </ul>                                | <ul style="list-style-type: none"> <li>Novell iFolder 3.8 Enterprise server file repository on OES 2 server</li> </ul>                                                                                 | <ul style="list-style-type: none"> <li>Files can be encrypted for transport through SSL (HTTPS).</li> <li>Secure LDAP Authentication</li> </ul> |
| Novell Samba       | <ul style="list-style-type: none"> <li>Any CIFS client</li> <li>Remote access (Web Folders in the Internet Explorer browser)</li> <li>Windows Explorer</li> </ul>                                                                                                                 | <ul style="list-style-type: none"> <li>Linux POSIX file system on OES 2 server</li> <li>NSS volumes</li> </ul>                                                                                         | <ul style="list-style-type: none"> <li>Secure LDAP Authentication</li> </ul>                                                                    |

## 17.2.2 Comparing Your CIFS File Service Options

OES 2 SP2 offers three file services that use the CIFS protocol: Novell CIFS, Novell Samba, and Samba in Domain Services for Windows (DSfW).

**Table 17-9** 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 server. For instructions on how to set up an NSS volume, see <a href="#">“Managing NSS Volumes”</a> in the <i>OES 2 SP2: 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 <a href="#">“Creating Users”</a> in the <i>OES 2 SP2: 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> |
| 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).
  - ♦ **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 3.8:** Suggestions for calculating the additional RAM you need are contained in “[Server Workload Considerations](#)” in the *Novell iFolder 3.8 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).
  - ♦ **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 3.8:** Suggestions for calculating the additional disk space you need are contained in “[Server Workload Considerations](#)” in the *Novell iFolder 3.8 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                                                       |
|----------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| NCP                  | “ <a href="#">Novell NCP Server / Dynamic Storage Technology</a> ” in the <i>OES 2 SP2: Installation Guide</i> | Installed by default. No additional planning required.                            |
| NetStorage           | “ <a href="#">Novell NetStorage</a> ” in the <i>OES 2 SP2: Installation Guide</i>                              | “ <a href="#">NetStorage Install</a> ” in the <i>NW65 SP8: Installation Guide</i> |
| Novell AFP           | “ <a href="#">Novell AFP Services</a> ” in the <i>OES 2 SP2: Installation Guide</i>                            | N/A                                                                               |
| Novell CIFS          | “ <a href="#">Novell CIFS for Linux</a> ” in the <i>OES 2 SP2: Installation Guide</i>                          | N/A                                                                               |

| File Service Product | Linux Planning References                                             | NetWare Planning References |
|----------------------|-----------------------------------------------------------------------|-----------------------------|
| Novell iFolder 3.8   | <a href="#">“Novell iFolder” in the OES 2 SP2: Installation Guide</a> | N/A                         |
| Samba                | <a href="#">“Novell Samba” in the OES 2 SP2: Installation Guide</a>   | 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 193](#)
- ♦ [Section 17.3.2, “NetStorage,” on page 194](#)
- ♦ [Section 17.3.3, “Novell AFP,” on page 194](#)
- ♦ [Section 17.3.4, “Novell CIFS,” on page 194](#)
- ♦ [Section 17.3.5, “Novell iFolder 3.8,” on page 194](#)
- ♦ [Section 17.3.6, “Samba,” on page 194](#)

### 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 SP3 for Linux Administration Guide](#).

Because NCP is now available on Linux, Novell Client users can attach to OES 2 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 servers, and other services commonly associated with Novell Client access.

For more information on NCP Server for Linux, see the [OES 2 SP2: NCP Server for Linux Administration Guide](#).

## 17.3.2 NetStorage

NetStorage provides Web access to the files and directories on OES 2 servers from browsers and Web-enabled devices such as PDAs.

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 [NW 6.5 SP8: NetStorage Administration Guide](#) or the [OES 2 SP2: NetStorage for Linux Administration Guide](#).

## 17.3.3 Novell AFP

Novell AFP provides native AFP protocol access from Macintosh workstations to data on OES 2 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, see “[Migrating AFP from NetWare to OES 2 SP2 Linux](#)” in the [OES 2 SP2: Migration Tool Administration Guide](#).

## 17.3.4 Novell CIFS

Novell CIFS provides native CIFS protocol access from Windows workstations to data on OES 2 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, see “[Migrating CIFS from NetWare to OES 2 SP2 Linux](#)” in the [OES 2 SP2: Migration Tool Administration Guide](#).

## 17.3.5 Novell iFolder 3.8

iFolder 3.8 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 3.8 is available only on OES 2.

For information on migrating from iFolder 2 to iFolder 3.8, see “[Migrating iFolder 2.x](#)” in the [OES 2 SP2: Migration Tool Administration Guide](#).

## 17.3.6 Samba

OES 2 includes Samba software to provide Microsoft CIFS and HTTP-WebDAV access to files on the server. Like Novell CIFS, this is 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 SP2: 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 Novell Trustee File Security Models,”](#) on page 219) 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 195
- ♦ [Section 17.4.2, “Providing a Private Work Directory,”](#) on page 196
- ♦ [Section 17.4.3, “Providing a Group Work Area,”](#) on page 197
- ♦ [Section 17.4.4, “Providing a Public Work Area,”](#) on page 197
- ♦ [Section 17.4.5, “Setting Up Rights Inheritance,”](#) on page 198

### 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 SP3: Installation and Administration Guide* ([http://www.novell.com/documentation/sles10/sles\\_admin/data/sles\\_admin.html](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 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 rwx 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 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 195.”](#)

### 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.)

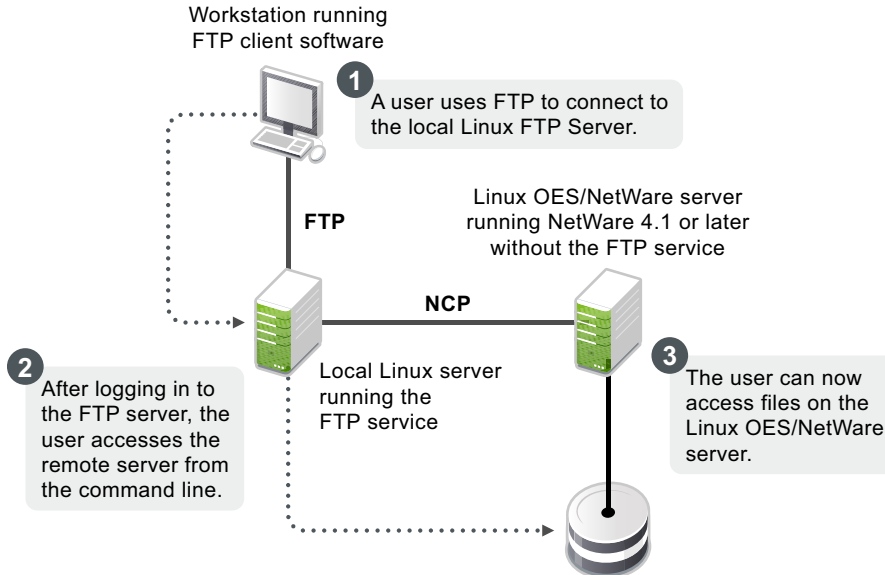
Use the `chmod` command to adjust this where necessary by specifying the number 5 for the other permission. For more information, see “[Managing Access Rights](#)” at the beginning of this section.

## 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 SP2: NCP Server for Linux Administration Guide*.

## 17.5 PureFTP Remote Access Implementation

After logging in to the eDirectory tree, users can access files and directories on a remote Linux server whether or not the server is running Linux FTP Server software. The remote server can be another Linux OES server or an IBM server if they are in the same tree.



The NCP protocol lets you transfer files and navigate to and from remote eDirectory servers.

To navigate to remote servers, use the following command:

```
cd //remote server name/volume/directory pathname
```

File operations such as `get`, `put`, and `delete` can be used on the remote server, even without changing the directory path to that server.

For example:

```
get //remote_server_name/volume/directory path/filename
```

The double slash (//) indicates that the user wants to access a remote server. After the double slash, the first entry must be the name of the remote server.

## 17.5.1 Configuring FTP

**Configuration file:** /etc/pure-ftpd/pure-ftpd.conf

The configuration parameters for remote server navigation are as follows:

| Entry                    | Value | Function                                                   |
|--------------------------|-------|------------------------------------------------------------|
| remote_server            | yes   | Enables remote server navigation for the Pure-FTPd server. |
| disallow_list_oes_server | yes   | Disables SITE SLIST command for listing OES machines.      |
| edir_ldap_port           | 389   | eDirectory LDAP port                                       |

The following configuration parameters needs to be set for remote server navigation:

| Entry          | Value | Reason Why                                                                                                                            |
|----------------|-------|---------------------------------------------------------------------------------------------------------------------------------------|
| ChrootEveryone | no    | Option yes restricts users to login only to his home directory and cannot navigate to other directories including remote OES servers. |
| ChrootEveryone | no    | Option yes restricts users to login only to his home directory and cannot navigate to other directories including remote OES servers. |
| AnonymousOnly  | no    | Option yes allows only anonymous logins.                                                                                              |

## 17.5.2 Path Formats

**Table 17-10** Linux FTP Server path formats

| Task                                          | Command Format                           |
|-----------------------------------------------|------------------------------------------|
| Specifying the volume and directory path name | //server_name/volume_name/directory_path |
| Navigating to different volumes               | cd //server_name/volume_name             |
| Switching back to the home directory          | cd ~                                     |
| Switching to home directory of any user       | cd ~user_name                            |

| Task                                | Command Format |
|-------------------------------------|----------------|
| Switching to the root of the server | cd /           |

**NOTE:** The Linux FTP Server does not support wildcards at the root of the server.

### 17.5.3 SITE Command

The `SITE` command enables FTP clients to access features specific to the Linux FTP Server.

**NOTE:** The `SITE` command is not case sensitive if entered from an FTP client.

The `SITE` command has the following syntax:

```
SITE [SLIST]
```

**NOTE:** The settings done through `SITE` commands are valid only for the current session.

This command is unique to the Linux FTP service and are not standard FTP commands.

[Table 17-11](#) provides the `SITE` command along with the description:

**Table 17-11** *Linux FTP SITE command*

| Command | Description                                           |
|---------|-------------------------------------------------------|
| SLIST   | Lists all the OES servers within the eDirectory tree. |

**NOTE:** All the FTP users needs to be LUM-enabled on the FTP server.

## 17.6 NCP Implementation and Maintenance

If you have installed the NCP server for OES, eDirectory/Novell Client users can access files on the OES 2 server with no additional configuration.

The implementation information in the following sections can help you get started with NCP on OES 2 servers.

- ♦ [Section 17.6.1, “The Default NCP Volume,” on page 201](#)
- ♦ [Section 17.6.2, “Creating NCP Home and Data Volume Pointers,” on page 201](#)
- ♦ [Section 17.6.3, “Assigning File Trustee Rights,” on page 201](#)
- ♦ [Section 17.6.4, “NCP Caveats,” on page 201](#)
- ♦ [Section 17.6.5, “NCP Maintenance,” on page 202](#)

## 17.6.1 The Default NCP Volume

The NCP Server for OES enables NCP access to NCP and NSS volumes defined on the OES 2 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 OES server.

This NCP volume contains `LOGIN` and `PUBLIC` directories that, in turn, contain a small subset of the files traditionally found on a NetWare server in the directories with the same names.

## 17.6.2 Creating NCP 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 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 terminal 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 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 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 SP2: 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 Caveats

Starting with OES 2 SP2, cross-protocol file locking (CPL) is enabled by default on all new servers with NCP installed. For more information, see [Section 1.3.5, “Cross-Protocol File Locking Change,”](#) on page 20.

## 17.6.5 NCP Maintenance

Because NCP provides Novell Client access to files on NetWare and OES 2 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 SP2: NetStorage for Linux Administration Guide*.

- ♦ [Section 17.7.1, “About Automatic Access and Storage Locations,” on page 202](#)
- ♦ [Section 17.7.2, “About SSH Storage Locations,” on page 202](#)
- ♦ [Section 17.7.3, “Assigning User and Group Access Rights,” on page 202](#)
- ♦ [Section 17.7.4, “Authenticating to Access Other Target Systems,” on page 203](#)
- ♦ [Section 17.7.5, “NetStorage Authentication Is Not Persistent by Default,” on page 203](#)
- ♦ [Section 17.7.6, “NetStorage Maintenance,” on page 204](#)

### 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.

In summary, NetStorage provides automatic access to:

- ♦ 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)

To provide access to file systems not listed above, you must create Storage Location objects in eDirectory. For instructions on creating Storage Locations, see [“Creating a Storage Location Object”](#) in the *OES 2 SP2: NetStorage for Linux 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,” on page 93](#).

### 17.7.3 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:

- ♦ eDirectory users must exist in the eDirectory tree where the OES server resides and have access rights to the files and directories on the OES 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 server, they must be enabled for LUM and Samba access on the OES 2 server. For more information, see [“Services in OES 2 That Require LUM-Enabled Access” on page 152](#).

---

**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.

---

## 17.7.4 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 legacy 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 non-primary authentication domain.

When defining a non-primary authentication domain, you must

- ♦ Ensure that the username and password in the non-primary 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 non-primary authentication domains.

For more information about managing NetStorage authentication domains, see [“Authentication Domains”](#) in the *OES 2 SP2: NetStorage for Linux Administration Guide*.

## 17.7.5 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 SP2: NetStorage for Linux Administration Guide*.

## 17.7.6 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 [OES 2 SP2: NetStorage for Linux Administration Guide](#).

## 17.8 Novell AFP Implementation and Maintenance

To use the Novell implementation of AFP file services on your OES 2 server, you must install the service by using the instructions in the [OES 2 SP2: Installation Guide](#) (for a new installation) or install it after the initial OES installation, as explained in “Installing AFP after the OES 2 SP 2 Installation” in the [OES 2 SP2: Novell AFP For Linux Administration Guide](#).

- ♦ [Section 17.8.1, “Implementing Novell AFP File Services,” on page 204](#)
- ♦ [Section 17.8.2, “Maintaining Novell AFP File Services,” on page 204](#)

### 17.8.1 Implementing Novell AFP File Services

---

**NOTE:** If you are new to OES, we recommend the [OES 2 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 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 SP2: 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 server, you must install the service by using the instructions in the [OES 2 SP2: 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 SP2: Novell CIFS for Linux Administration Guide](#).

- ♦ [Section 17.9.1, “Implementing Novell CIFS File Services,” on page 204](#)
- ♦ [Section 17.9.2, “Maintaining Novell CIFS File Services,” on page 205](#)

### 17.9.1 Implementing Novell CIFS File Services

---

**NOTE:** If you are new to OES, we recommend the [OES 2 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 server as they would any Windows workgroup server.

For instructions on implementing Novell CIFS, see “[Planning and Implementing CIFS](#)” in the *OES 2 SP2: 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 SP2: Novell CIFS for Linux Administration Guide*.

## 17.10 Novell iFolder 3.8 Implementation and Maintenance

The following implementation pointers are provided only as introductory information. To begin using Novell iFolder, see the *Novell iFolder 3.8 Administration Guide*.

- ♦ [Section 17.10.1, “Managing Novell iFolder 3.8,” on page 205](#)
- ♦ [Section 17.10.2, “Configuring Novell iFolder 3.8 Servers,” on page 205](#)
- ♦ [Section 17.10.3, “Creating and Enabling Novell iFolder 3.8 Users,” on page 205](#)
- ♦ [Section 17.10.4, “Novell iFolder 3.8 Maintenance,” on page 206](#)

### 17.10.1 Managing Novell iFolder 3.8

You manage Novell iFolder through the iFolder Management Console, which you can access directly or through iManager. For more information, see “[Installing and Configuring iFolder Services](#)” in the *Novell iFolder 3.8 Administration Guide*.

### 17.10.2 Configuring Novell iFolder 3.8 Servers

Before you let users log in to the Novell iFolder 3.8 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 *Novell iFolder 3.8 Administration Guide*.

### 17.10.3 Creating and Enabling Novell iFolder 3.8 Users

To provide user access to Novell iFolder 3.8:

1. Provision eDirectory User objects for iFolder 3.8.
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 *Novell iFolder 3.8 Administration Guide*.

## 17.10.4 Novell iFolder 3.8 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 *Novell iFolder 3.8 Administration Guide*. For a list of other common iFolder maintenance topics, see [iFolder 3.8](#) 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 SP2: 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 SP2: Samba Administration Guide*.

- ♦ [Section 17.11.1, “Implementing Samba File Services,”](#) on page 206
- ♦ [Section 17.11.2, “Maintaining Samba File Services,”](#) on page 206

### 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 SP2: Samba Administration Guide*.

### 17.11.2 Maintaining Samba File Services

Information on maintaining your Samba installation is found in the *OES2 SP2: Samba Administration Guide*.

# Search Engine (QuickFinder)

# 18

Open Enterprise Server 2 includes the Novell® QuickFinder™ Server. QuickFinder lets you add search 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 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](#)*.



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 19.1, “Overview of Print Services,” on page 209](#)
- ♦ [Section 19.2, “Planning for Print Services,” on page 211](#)
- ♦ [Section 19.3, “Coexistence and Migration of Print Services,” on page 212](#)
- ♦ [Section 19.4, “Print Services Implementation Suggestions,” on page 212](#)
- ♦ [Section 19.5, “Print Services Maintenance Suggestions,” on page 214](#)

## 19.1 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 19.1.1, “Using This Overview,” on page 209](#)
- ♦ [Section 19.1.2, “iPrint Components,” on page 210](#)
- ♦ [Section 19.1.3, “iPrint Functionality,” on page 210](#)

### 19.1.1 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 19.2, “Planning for Print Services,” on page 211](#).

If you want to learn more about iPrint, continue with this overview section.

## 19.1.2 iPrint Components

A Novell iPrint installation consists of various components, most of which are represented by objects in your eDirectory™ tree:

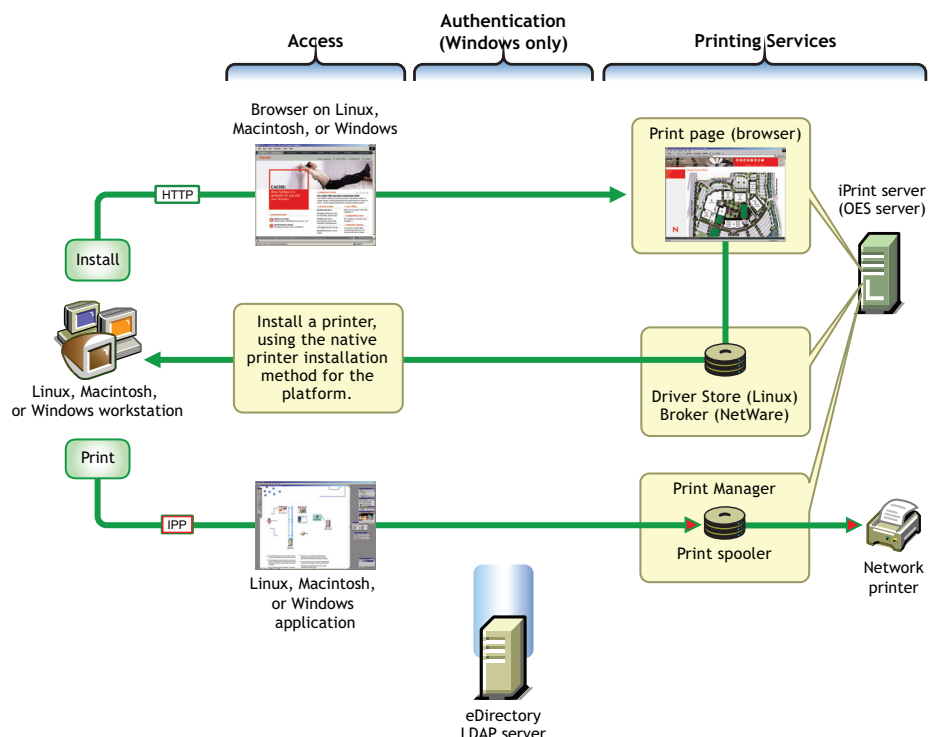
- ♦ **Print Driver Store (Linux):** This is a repository that stores the drivers on an OES 2 server for your network printers. It is the first component you configure and is represented by an eDirectory object that you create.
- ♦ **Print Broker (NetWare):** This is a repository that stores the drivers on an NetWare 6.5 SP8® 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 or an NLM™ that runs on the NetWare 6.5 SP8 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.

## 19.1.3 iPrint Functionality

[Figure 19-1](#) describes how iPrint functions from a user workstation perspective.

**Figure 19-1** *How iPrint Works*



The following table explains the information illustrated in [Figure 19-1](#).

**Table 19-1** *iPrint Functionality*

| Access                                                                                                                                                                                                                                                                                                                                                                                                                  | Authentication                                                                                                                                                                                                                               | Printing Services                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>The iPrint Client must be installed on each workstation accessing iPrint services.</p> <p>A user needing to use a printer for the first time accesses the organization's print page on the Web.</p> <p>When the user selects the target printer, its platform-specific driver is automatically installed and configured.</p> <p>After printer installation, users can print to the printer from any application.</p> | <p>You can require authentication for Windows users if needed. The option to require authentication is not available for Linux and Macintosh users.</p> <p>Although shown separately, eDirectory could be installed on the OES 2 server.</p> | <p>Users with the iPrint Client installed and access to the OES 2 server can install printer drivers and print to iPrint printers.</p> <p>By default, iPrint generates a printer list for the printers hosted on the server.</p> <p>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.</p> |

## 19.2 Planning for Print Services

Consider the following information as you plan your iPrint installation:

- We recommend that you record your decisions in planning notes 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 servers. On NetWare servers, you designate the location when creating the Print Manager object.

- ♦ To finish planning your iPrint installation, refer to the information in “[Novell iPrint](#)” in the *OES 2 SP2: Installation Guide*

## 19.3 Coexistence and Migration of Print Services

If you select iPrint during the OES 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 *NW 6.5 SP8: iPrint Administration Guide*.

For more information on configuring iPrint on OES, see “[Installing and Setting Up iPrint on Your Server](#)” in the *OES 2 SP2: iPrint for Linux Administration Guide*.

In OES SP2, migrating iPrint services from a NetWare server to an OES 2 server is supported by the OES 2 Migration Tool. For more information, see “[Migrating iPrint from NetWare to OES 2 Linux](#)” in the *OES 2 SP2: Migration Tool Administration Guide*.

## 19.4 Print Services Implementation Suggestions

This section provides only summary implementation information. For complete iPrint documentation, see the *OES 2 SP2: iPrint for Linux Administration Guide*.

- ♦ [Section 19.4.1, “Initial Setup,” on page 212](#)
- ♦ [Section 19.4.2, “Implementation Caveats,” on page 213](#)
- ♦ [Section 19.4.3, “Other Implementation Tasks,” on page 213](#)

### 19.4.1 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 or a Broker on NetWare 6.5 SP8 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 “[Creating a Driver Store](#)” in the *OES 2 SP2: iPrint for Linux Administration Guide*

- 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 [“Updating Printer Drivers”](#) in the *OES 2 SP2: iPrint for Linux Administration Guide*

- 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 [“Creating a Print Manager”](#) in the *OES 2 SP2: iPrint for Linux Administration Guide*

- 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 [“Creating a Printer”](#) in the *OES 2 SP2: iPrint for Linux Administration Guide*

- 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 [“Setting Up Location-Based Printing”](#) in the *OES 2 SP2: iPrint for Linux Administration Guide*

- 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.

## 19.4.2 Implementation Caveats

There are a few implementation caveats relating to iPrint on Linux. See [“iPrint” on page 66](#).

## 19.4.3 Other Implementation Tasks

In addition to the tasks described in [Section 19.4.1, “Initial Setup,” on page 212](#), 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.

## 19.5 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 “[Using the Print Manager Health Monitor](#)” in the *OES 2 SP2: iPrint for Linux Administration Guide*

For more information on iPrint and its functionality within OES, see the “[Print Services](#)” links in the online documentation.

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.

## **Apache**

Apache Web Server 2.0 is the most popular Web server on the Internet.

For additional information, see [Apache.org Web site \(http://www.apache.org\)](http://www.apache.org).

## **Tomcat**

Tomcat is used to run basic Java servlet and JavaServer Pages (JSP) applications.

For information, see 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).



This section contains the following topics:

- ♦ [Section 21.1, “Overview of OES Security Services,” on page 217](#)
- ♦ [Section 21.2, “Planning for Security,” on page 219](#)
- ♦ [Section 21.3, “Configuring and Administering Security,” on page 221](#)
- ♦ [Section 21.4, “Links to Product Security Considerations,” on page 221](#)
- ♦ [Section 21.5, “Links to Anti-Virus Partners,” on page 223](#)

## 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 217](#)
- ♦ [Section 21.1.2, “NSS Auditing Engine,” on page 217](#)
- ♦ [Section 21.1.3, “Encryption \(NICI\),” on page 218](#)
- ♦ [Section 21.1.4, “General Security Issues,” on page 219](#)

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 NSS Auditing Engine

OES 2 SP2 includes the NSS Auditing Engine, which is installed by default with NSS.

The auditing engine provides an interface for auditing client applications, such as Novell Sentinel and various third-party products to access. Information about the auditing engine SDK is available on the [Novell Web site \(http://developer.novell.com/wiki/index.php/NSS\\_Auditing\\_SDK\)](http://developer.novell.com/wiki/index.php/NSS_Auditing_SDK).

Using the SDK, client applications can be developed to audit various NSS file system operations on files and directories, including:

- ♦ delete
- ♦ create
- ♦ open
- ♦ close

- ♦ rename
- ♦ link
- ♦ metadata modified
- ♦ trustee add/delete
- ♦ inherited rights modified

### **Novell Sentinel Log Manager 90-Day Free Trial**

Novell Sentinel Log Manager runs on a 64-bit SLES 11 host. You can download the suite from the [Novell Download Web site \(http://download.novell.com/Download?buildid=o8BgsbCidWg~\)](http://download.novell.com/Download?buildid=o8BgsbCidWg~). For installation and usage instructions, see the Novell Log Management Readme and Release Notes included as a link on the download page.

### **Third-Party Partner Applications**

The following Novell partners are currently developing applications for use with the NSS Auditing Engine:

- ♦ Blue Lance
- ♦ NetVision
- ♦ Symantec

## **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) 2.7.5 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 Novell Trustee File Security Models,” on page 219](#)
- ♦ [Section 21.2.2, “User Restrictions: Some OES 2 Limitations,” on page 221](#)

### 21.2.1 Comparing the Linux and the Novell Trustee File Security Models

The Novell Trustee 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                                                                                                                                                                                                                                                                                                                                                                                                                                    | Novell Trustee Model on OES 2                                                                                                                   |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <a href="#">Section 17.4.2, “Providing a Private Work Directory,” on page 196</a>.</p> | <p>Trustee assignments are made to directories and files and flow down from directories to everything below unless specifically reassigned.</p> |

| Feature                                              | POSIX / Linux                                                                                                                                                                                                                                                                                                                                                                              | Novell Trustee Model on OES 2                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <a href="#">Section 17.4.2, “Providing a Private Work Directory,” on page 196</a>.</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>                                                                                                             |
| Privacy                                              | <p>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.</p>                                                                                                                                                                                                                     | <p>Directories and files are private by default.</p>                                                                                                                                                                                                                                                                        |
| 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>         | <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.</p>                                                               |

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 SP2: NCP Server for Linux Administration Guide](#), particularly the “NCP on Linux Security” section.

## 21.2.2 User Restrictions: Some OES 2 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,” on page 93](#).

For more information on Linux User Management, see [“Linux User Management: Access to Linux for eDirectory Users” on page 149](#). For more information on the services that can be PAM-enabled, see [Table 15-2 on page 152](#).

## 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                                                                                                                                                                                                                     |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AppArmor           | <a href="http://www.novell.com/documentation/apparmor/apparmor201_sp10_admin/data/book_apparmor_admin.html">Novell AppArmor Administration Guide (http://www.novell.com/documentation/apparmor/apparmor201_sp10_admin/data/book_apparmor_admin.html)</a> |

| <b>Product/Technology</b>       | <b>Security Considerations Section Link</b>                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Archive and Version Services    | <a href="#">“Security Considerations for Archive and Version Services” in the <i>OES 2 SP2: Novell Archive and Version Services 2.1 for Linux Administration Guide</i></a>                                                                                                                                                                                                      |
| Domain Services for Windows     | <a href="#">OES 2: Novell Domain Services for Windows Security Guide</a>                                                                                                                                                                                                                                                                                                        |
| Dynamic Storage Technology      | <a href="#">“Security Considerations” in the <i>OES 2 SP2: Dynamic Storage Technology Administration Guide</i></a>                                                                                                                                                                                                                                                              |
| eDirectory                      | <a href="#">“Security Considerations” in the <i>Novell eDirectory 8.8 Administration Guide</i></a>                                                                                                                                                                                                                                                                              |
| File Systems                    | <a href="#">OES 2 SP2: File Systems Management Guide (information throughout the guide)</a>                                                                                                                                                                                                                                                                                     |
| Identity Manager 3.6            | <a href="#">“Security Best Practices (<a href="http://www.novell.com/documentation/idm36/idm_security/data/front.html">http://www.novell.com/documentation/idm36/idm_security/data/front.html</a>)” in the Identity Manager 3.6 Documentation (<a href="http://www.novell.com/documentation/caribou/index.html">http://www.novell.com/documentation/caribou/index.html</a>)</a> |
| iPrint for OES 2                | <a href="#">“Setting Up a Secure Printing Environment” in the <i>OES 2 SP2: iPrint for Linux Administration Guide</i></a>                                                                                                                                                                                                                                                       |
| Linux User Management           | <a href="#">“Security Considerations” in the <i>OES 2 SP2: Novell Linux User Management Technology Guide</i></a>                                                                                                                                                                                                                                                                |
| Novell AFP                      | <a href="#">“Security Guidelines for AFP” in the <i>OES 2 SP2: Novell AFP For Linux Administration Guide</i></a>                                                                                                                                                                                                                                                                |
| Novell CIFS                     | <a href="#">“Security Guidelines for CIFS” in the <i>OES 2 SP2: Novell CIFS for Linux Administration Guide</i>.</a>                                                                                                                                                                                                                                                             |
| Novell Client™ for Windows      | <a href="#">“Managing File Security and Passwords” in the <i>Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide</i></a>                                                                                                                                                                                                                           |
| Novell Client for Linux         | <a href="#">“Managing File Security” in the <i>Novell Client 2.0 SP3 for Linux Administration Guide</i></a>                                                                                                                                                                                                                                                                     |
| Novell Remote Manager for OES 2 | <a href="#">“Security Considerations” in the <i>OES 2 SP2: Novell Remote Manager for Linux Administration Guide</i></a>                                                                                                                                                                                                                                                         |
| Novell Storage Services         | <a href="#">“Securing Access to NSS Volumes, Directories, and Files” and “Security Considerations” in the <i>OES 2 SP2: NSS File System Administration Guide</i></a>                                                                                                                                                                                                            |
| Novell iFolder® 3.8             | <a href="#">Novell iFolder 3.8 Security Administration Guide</a>                                                                                                                                                                                                                                                                                                                |
| OES 2 Installation              | <a href="#">“Security Considerations” in the <i>OES 2 SP2: Installation Guide</i></a>                                                                                                                                                                                                                                                                                           |
| OES 2 Migration Tools           | <a href="#">“Security Considerations for Data Migration” in the <i>OES 2 SP2: Migration Tool Administration Guide</i></a>                                                                                                                                                                                                                                                       |
| OpenWBEM                        | <a href="#">“Ensuring Secure Access” in the <i>OES 2 SP2: OpenWBEM Services Administration Guide</i></a>                                                                                                                                                                                                                                                                        |
| QuickFinder™                    | <a href="#">“Security Considerations for QuickFinder Server” in the <i>QuickFinder Server 5.0 Administration Guide</i></a>                                                                                                                                                                                                                                                      |

| Product/Technology | Security Considerations Section Link                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SuSEfirewall2      | "Masquerading and Firewalls" ( <a href="http://www.novell.com/documentation/sles10/book_sle_reference/data/cha_fire.html">http://www.novell.com/documentation/sles10/book_sle_reference/data/cha_fire.html</a> ) in the <i>SLES 10 SP3 Installation and Administration</i> guide ( <a href="http://www.novell.com/documentation/sles10/book_sle_reference/data/book_sle_reference.html">http://www.novell.com/documentation/sles10/book_sle_reference/data/book_sle_reference.html</a> ) |

## 21.5 Links to Anti-Virus Partners

See the [Partners and Communities](http://www.novell.com/products/openenterpriseserver/partners_communities.html) page on Novell.com ([http://www.novell.com/products/openenterpriseserver/partners\\_communities.html](http://www.novell.com/products/openenterpriseserver/partners_communities.html)).



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 225](#)
- ♦ [Section 22.2, “Setting Up Certificate Management,” on page 228](#)
- ♦ [Section 22.3, “If You Don’t Want to Use eDirectory Certificates,” on page 230](#)

## 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 225](#)
- ♦ [Section 22.1.2, “OES 2 Certificate Management,” on page 226](#)
- ♦ [Section 22.1.3, “Multiple Trees Sharing a Common Root,” on page 228](#)

### 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 226](#)
- ♦ [“What Is Installed Where” on page 226](#)
- ♦ [“Novell Certificate Server” on page 227](#)
- ♦ [“Server Self-Provisioning” on page 227](#)
- ♦ [“PKI Health Check” on page 227](#)

### 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 3.3.2 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 3.3.2 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 3.3.2 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 3.3.2 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 228](#)
- ♦ [Section 22.2.2, “Eliminating Browser Certificate Errors,” on page 228](#)

### 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 227.

---

**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 229](#)
- ♦ [“Importing the CA Certificate into Mozilla Firefox on Linux” on page 229](#)
- ♦ [“Importing the CA Certificate into Mozilla Firefox on Windows” on page 229](#)
- ♦ [“Importing the CA Certificate into Internet Explorer 6 and 7 on Windows” on page 230](#)

### **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 229](#) 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 229](#) 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 229](#), 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 or OES 2 SP1   | The same option is used as when OES 2 was installed | HTTPS service settings are retained.                                            | No effect.<br><br>Once the option to use eDirectory certificates has been used, the behavior can only be changed in eDirectory through iManager. |



# Adding Services to OES 2 Servers



You can add services to Open Enterprise Server 2 servers after they are installed.

OES 2 is a set of services that can be either added to an existing server or installed at the same time as SUSE<sup>®</sup> Linux Enterprise Server 10 SP1. After OES 2 services are added, we refer to the server as an OES 2 server.

To add OES 2 services to an OES 2 server, follow the instructions in “[Installing or Configuring OES 2 SP2 on an Existing Server](#)” in the *OES 2 SP2: Installation Guide*.



# Changing an OES 2 Server's IP Address

# B

The instructions in this section let you change the IP address assigned to an OES 2 SP2 server and the services it hosts.

- ♦ [Section B.1, “Caveats and Disclaimers,” on page 235](#)
- ♦ [Section B.2, “Prerequisites,” on page 235](#)
- ♦ [Section B.3, “Changing the Server's Address Configuration,” on page 236](#)
- ♦ [Section B.4, “Reconfiguring the OES Services,” on page 236](#)
- ♦ [Section B.5, “Repairing the eDirectory Certificates,” on page 237](#)
- ♦ [Section B.6, “Completing the Server Reconfiguration,” on page 237](#)
- ♦ [Section B.7, “Modifying a Cluster,” on page 241](#)
- ♦ [Section B.8, “Reconfiguring Services on Other Servers That Point to This Server,” on page 241](#)

## 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 235](#)
- ♦ [Section B.2.2, “iPrint,” on page 236](#)
- ♦ [Section B.2.3, “Clustering,” on page 236](#)

### 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 SP2: 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 SP2: Novell Cluster Services 1.8.7 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 `ipchangesp2.sh` script file (<http://www.novell.com/documentation/oes2/scripts/ipchangesp2.sh>) to the `root (/)` partition of the server you are reconfiguring.
- 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 235](#) 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 235](#), 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 236](#).

## 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 ipchangesp2.sh
./ipchangesp2.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 238](#)
- ♦ [Section B.6.2, “DHCP,” on page 238](#)
- ♦ [Section B.6.3, “DSfW,” on page 238](#)
- ♦ [Section B.6.4, “iPrint,” on page 240](#)
- ♦ [Section B.6.5, “NetStorage,” on page 241](#)

## 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

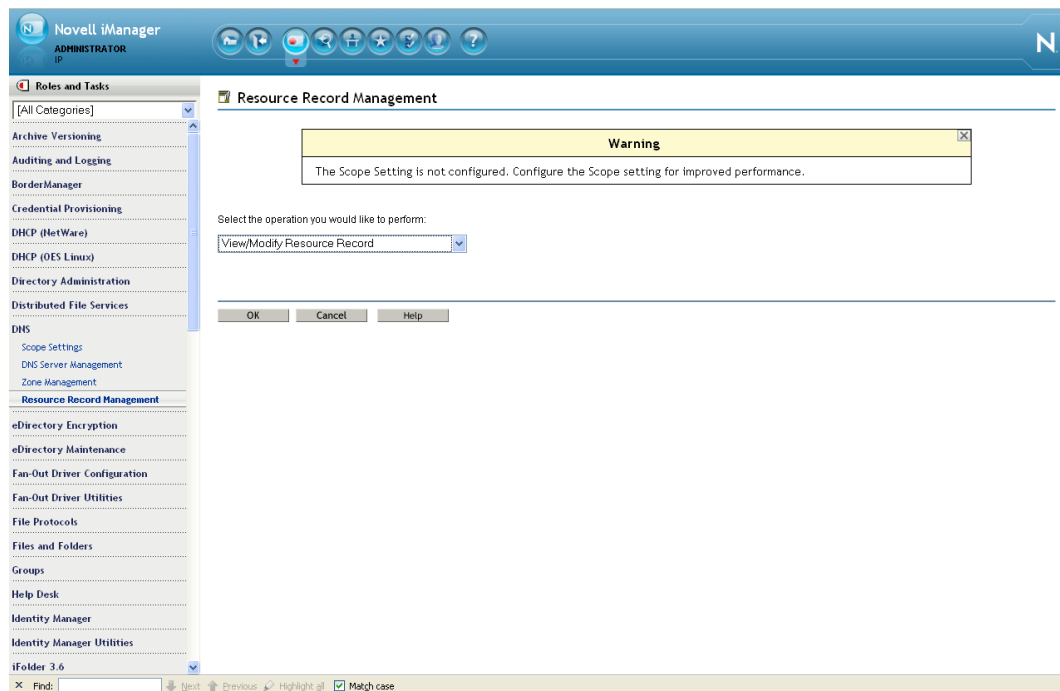
- 1 Make sure the DHCP configuration in eDirectory has a subnet declared for the new IP address.

For instructions, see “[Administering and Managing DHCP](#)” in the *OES 2 SP2: Novell DNS/DHCP Administration Guide for Linux*.

## B.6.3 DSfW

After the IP address is changed, execute the following instructions:

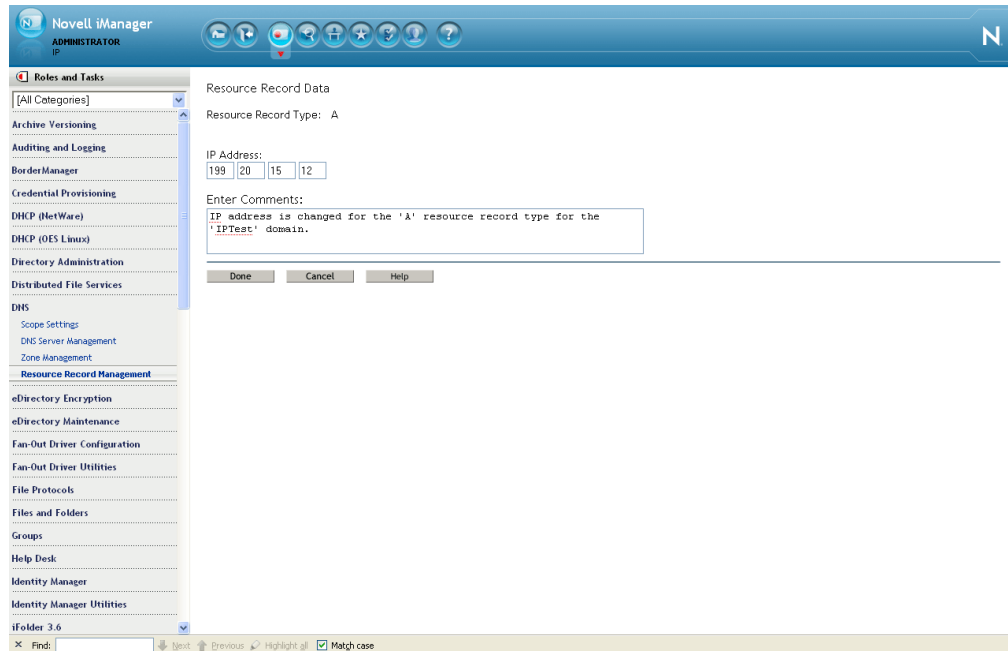
- 1 Open *iManager* > *DNS* > *Resource Record Management*. Select *View and Modify Resource Record* from the drop-down list, then click *OK* to open the Modify Resource Record window.



- 2 Select the domain name from the drop-down list, then click *Search*. This is the domain name whose IP address is to be changed (In this example, it is the 'A' record).

The screenshot shows the Novell iManager Administrator interface. On the left is a navigation pane with categories like Roles and Tasks, DNS, and Resource Record Management. The 'Resource Record Management' section is expanded, showing 'Modify RR Set - Resource Record'. The main area contains a form with the following fields: 'Select Domain Name' (dropdown menu showing 'ip1est.com'), 'Select a Host Name' (text field with '@'), 'Select RR Data' (text field with '199.100.9.1'), and 'Resource Record type' (dropdown menu showing 'A'). At the bottom of the form are four buttons: 'Modify', 'Done', 'Cancel', and 'Help'. The status bar at the bottom shows 'iFolder 3.6' and search options like 'Find', 'Next', 'Previous', 'Highlight all', and 'Match case'.

- 2a Specify the *Host Name* using the search feature.
- 2b Select the '@' record and click *Modify* to change the IP address with the new IP address.  
Select the hostname A record and click *Modify* to change the IP address with the new IP address.



- 2c Click *Done*. A message indicates that the A record has been successfully modified.
- 3 Execute the following steps to rename and move the Reverse Lookup object:
  - 3a Click *iManager > Directory Administration > Rename Object*. Search and select the Reverse Lookup object from eDirectory.
  - 3b In the New Object Name field, specify the name of the Reverse Lookup object with the new IP address.  
 For example: If the object name is `135_103_92_100_in-addr_arp.a.OESSystemObjects.nmfrd`, rename it with the new IP address. So if the new IP address is `100.92.103.136`, the new name of the Reverse Lookup object will be `136_103_92_100_in-addr_arp.a.OESSystemObjects.nmfrd`.
  - 3c Click *iManager > Directory Administration > Modify Object*. Search and select the Reverse Lookup object from eDirectory.
  - 3d From the *Other* tab, select the valued attribute named `dnip:zonedomainname` and change the value to new name of the Reverse Lookup object. Click *Save*.
- 4 Restart the DNS server.
- 5 Change the following:
  - 5a Update the `/etc/resolve.conf` file if the server was acting as the DNS server for the domain.

---

**NOTE:** If you are performing the IP address change on the Forest Root Domain that is hosting the DNS server, make sure you update the `/etc/resolve.conf` file for all the servers referencing this domain controller.

---

## B.6.4 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 SP2: iPrint for Linux Administration Guide*.

---

## B.6.5 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-xsrvd 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 *OES 2 SP2: Novell Cluster Services 1.8.7 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.



# Updating/Patching OES 2 Servers

# C

One of a network administrator's biggest challenges is keeping installed software up-to-date on all servers and workstations.

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 server and running the patch process, see “[Updating \(Patching\) an OES 2 SP2 Server](#)” in the *OES 2 SP2: Installation Guide*.



# Backup Services

# D

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 245](#)
- ♦ [Section D.2, “System-Wide Services,” on page 245](#)

## 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 3.8:** By implementing Novell® iFolder® 3.8, 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. Files 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, “Links to Backup Partners,” on page 245](#)
- ♦ [Section D.2.2, “Novell Storage Management Services \(SMS\),” on page 245](#)
- ♦ [Section D.2.3, “SLES 10 Backup Services,” on page 246](#)

### D.2.1 Links to Backup Partners

See the [Partners and Communities page on Novell.com](http://www.novell.com/products/openenterpriseserver/partners_communities.html) ([http://www.novell.com/products/openenterpriseserver/partners\\_communities.html](http://www.novell.com/products/openenterpriseserver/partners_communities.html)).

### D.2.2 Novell Storage Management Services (SMS)

- ♦ [“Understanding SMS” on page 246](#)
- ♦ [“SMS Coexistence and Migration Issues” on page 246](#)

## 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 NetWare 6.5 SP8® and OES 2 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 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 SP2: Storage Management Services Administration Guide*.

## D.2.3 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](http://www.novell.com/documentation/sles10/stor_evms/data/drdb.html)) in the *SLES 10 SP3: Storage Administration Guide* ([http://www.novell.com/documentation/sles10/stor\\_evms/data/bookinfo.html](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](http://www.novell.com/documentation/sles10/sles_admin/data/sec_net_sync_rsync.html)) in the *SLES 10 SP3: Installation and Administration Guide* ([http://www.novell.com/documentation/sles10/sles\\_admin/data/sles\\_admin.html](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                                | <a href="http://server_ip_address_or_dns_name/ipp">http://server_ip_address_or_dns_name/ipp</a><br><a href="https://server_ip_address_or_dns_name:443/ipp">https://server_ip_address_or_dns_name:443/ipp</a>                                                                                                                                                                   |                                                                                 |
| NetStorage                            | For browser access, use:<br><a href="http://server_ip_or_dns/netstorage">http:</a> or <a href="https://server_ip_or_dns/netstorage">https://server_ip_or_dns/netstorage</a><br>For WebDAV access, use:<br><a href="http://server_ip_or_dns/oneNet/NetStorage">http:</a> or <a href="https://server_ip_or_dns/oneNet/NetStorage">https://server_ip_or_dns/oneNet/NetStorage</a> | The WebDAV URL is case sensitive.                                               |
| Novell Client™                        | 1. Install the Novell Client on a supported Windows workstation.<br>2. Log in to eDirectory™.<br>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.<br>Create a Web Folder in Internet Explorer.                                                                                                                                                                                                                                                                                          |                                                                                 |
| Novell iFolder® 3.x Web Access server | <a href="https://server_ip_address_or_dns_name/ifolder">https://server_ip_address_or_dns_name/ifolder</a>                                                                                                                                                                                                                                                                      | “ifolder” is the default name, but this can be customized by the administrator. |
| Novell Remote Manager                 | <a href="http://server_ip_address_or_dns_name:8008">http://server_ip_address_or_dns_name:8008</a>                                                                                                                                                                                                                                                                              | Any LUM-enabled user can see their directories and files on OES 2 servers.      |
| Samba                                 | Map a network drive in Windows Explorer.<br>Create a Web Folder in Internet Explorer.                                                                                                                                                                                                                                                                                          |                                                                                 |



# OES 2 SP2 Browser Support

F

As a general rule, Open Enterprise Server 2 SP2 management tools support the following browsers as they are available on the workstation platforms listed in [“Client/Workstation OS Support” on page 251](#):

- ♦ 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"> <li>♦ <a href="#">“Using a Supported Web Browser”</a> in the <a href="#">Novell iManager 2.7.3 Administration Guide</a></li> </ul> <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> <p>Also, iManager plug-ins might not work properly if the highest priority Language setting for your Web browser is set to a language other than one of iManager’s support languages.</p> <p>To avoid problems, set the first language preference to a supported language.</p> |
| iMonitor                       | <ul style="list-style-type: none"> <li>♦ <a href="#">“System Requirements”</a> in <a href="#">“Using Novell iMonitor 2.4”</a> in the <a href="#">Novell eDirectory 8.8 Administration Guide</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| IP Address Manager (NetWare®)  | Same as Novell Remote Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| iPrint                         | <ul style="list-style-type: none"> <li>♦ <a href="#">“Supported Browsers for iPrint”</a> in the <a href="#">OES 2 SP2: iPrint for Linux Administration Guide</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Novell iFolder® 3.8            | <ul style="list-style-type: none"> <li>♦ <a href="#">“Web Browser”</a> in the <a href="#">Novell iFolder 3.8 Administration Guide</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Novell Remote Manager          | <ul style="list-style-type: none"> <li>♦ <a href="#">“System Requirements”</a> in the <a href="#">OES 2 SP2: Novell Remote Manager for Linux Administration Guide</a></li> <li>♦ <a href="#">“System Requirements”</a> in the <a href="#">NW 6.5 SP8: Novell Remote Manager Administration Guide</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                          |
| OpenSSH Manager (NetWare)      | <ul style="list-style-type: none"> <li>♦ <a href="#">“Added Functionality”</a> in the <a href="#">NW 6.5 SP8: OpenSSH Administration Guide</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| QuickFinder™ Server Manager    | <ul style="list-style-type: none"> <li>♦ <a href="#">“Managing QuickFinder Server”</a> in the <a href="#">OES 2: Novell QuickFinder Server 5.0 Administration Guide</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| TCP/IP Configuration (NetWare) | Same as Novell Remote Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Management Tool | Supported Browser Information Link                                                                                   |
|-----------------|----------------------------------------------------------------------------------------------------------------------|
| Tomcat Manager  | ♦ <a href="#">“Managing Tomcat with Tomcat Admin”</a> in the <a href="#">NW 6.5 SP8: Tomcat Administration Guide</a> |

# 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 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 83](#). 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 <code>init</code> 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 <code>shadowfs</code> daemon and the kernel module <code>fuse</code> .                                                                                                       |
| 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.<br><br>The namcd daemon caches user and group names and IDs from eDirectory, speeding subsequent lookups of cached users and groups.<br><br>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.<br><br>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.<br><br>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.<br><br>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-httpstkd | <p>This script runs by default on every OES 2 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 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 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-smdrd    | 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 SP2

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 SP2,” on page 277](#).

- ♦ [Section I.1, “About System Users and Groups,” on page 257](#)
- ♦ [Section I.2, “Understanding Proxy Users,” on page 259](#)
- ♦ [Section I.3, “Planning Your Proxy Users,” on page 264](#)
- ♦ [Section I.4, “Implementing Your Proxy User Plan,” on page 271](#)
- ♦ [Section I.5, “Proxy Users and Domain Services for Windows,” on page 272](#)
- ♦ [Section I.6, “System Users,” on page 272](#)
- ♦ [Section I.7, “System Groups,” on page 274](#)
- ♦ [Section I.8, “Auditing System Users,” on page 275](#)

## 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 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 257](#)
- ♦ [Section I.1.2, “OES System Users and Groups by Name,” on page 258](#)

### 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"> <li>♦ Retrieving passwords and service attributes</li> <li>♦ Writing Service information in eDirectory.</li> <li>♦ Providing a user ID (uid) that the associated service daemon uses to run.</li> </ul> | <ul style="list-style-type: none"> <li>♦ <code>afpProxyUser-servename</code></li> <li>♦ <code>cifsProxyUser-servename</code></li> <li>♦ <code>LUM_Proxy_user</code></li> </ul> |
| System Group              | <ul style="list-style-type: none"> <li>♦ Facilitate the management of system users</li> <li>♦ Provide access rights to service data on the server or in the eDirectory tree.</li> </ul>                                                                                                             | <ul style="list-style-type: none"> <li>♦ DHCP</li> <li>♦ DNSDHCP</li> </ul>                                                                                                    |
| System User               | The daemons associated with the respective services run as these users.                                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>♦ <code>wwwrun</code></li> <li>♦ <code>iprint</code></li> </ul>                                                                         |

## 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              |
|---------------------------------------|--------------|---------------------------------|
| <code>AfpProxyUser-servename</code>   | Proxy User   | AFP                             |
| (Archive Versioning Proxy)            | Proxy User   | Archive and Versioning Services |
| The install admin is always assigned. |              |                                 |
| <code>arkuser</code>                  | System User  | Archive and Versioning Services |
| <code>CifsProxyUser-servename</code>  | Proxy User   | CIFS                            |
| <i>DHCP LDAP Proxy</i>                | Proxy User   | DHCP                            |
| <code>dhcpcd</code>                   | System User  | DHCP                            |
| DHCPGroup                             | System Group | DHCP                            |
| <i>DNS Proxy</i>                      | Proxy User   | DNS                             |
| DNSDHCP-GROUP                         | System Group | DNS                             |
| <code>hacluster</code>                | System User  | Heartbeat                       |
| <code>iFolderProxy</code>             | Proxy User   | iFolder 3                       |
| <code>iprint</code>                   | System User  | iPrint                          |

| System User or Group                 | Object Type  | Associated Service              |
|--------------------------------------|--------------|---------------------------------|
| lprint (POSIX)                       | System Group | iPrint                          |
| lprintgrp (eDirectory)               |              |                                 |
| <i>LUM proxy</i><br>(optional)       | Proxy User   | Linux User Management           |
| named                                | System User  | DNS                             |
| ncsclient                            | System User  | NCS                             |
| ncsgroup                             | System Group | NCS                             |
| <i>NetStorage Proxy</i>              | Proxy User   | NetStorage                      |
| novell_nobody                        | System User  | CIMOM                           |
| novell_nogroup                       | System Group | CIMOM                           |
| novlxregd                            | System User  | XTier                           |
| novlxsrvd                            | System User  | XTier                           |
| novlxtier                            | System Group | XTier                           |
| <i>server_name</i> -SambaProxy       | Proxy User   | Samba (Novell)                  |
| <i>server_name</i> -W-SambaUserGroup | System Group | Samba (Novell)                  |
| <i>server_name</i> admin             | Proxy User   | NSS                             |
| www                                  | System Group | Apache<br>Tomcat<br>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 260](#)
- ♦ [Section I.2.2, “Why Are Proxy Users Needed on OES?,” on page 260](#)
- ♦ [Section I.2.3, “Which Services Require Proxy Users and Why?,” on page 260](#)
- ♦ [Section I.2.4, “What Rights Do Proxy Users Have?,” on page 261](#)

## 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 260](#)). 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?

OES 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 Services:** eDirectory also runs very well on OES, 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<br><br>The install admin is always specified. | The service runs as this user.      |
| CIFS               | CifsProxyUser- <i>servername</i>                    | Retrieves passwords for CIFS users. |

| Associated Service    | Example Proxy User Name                                                                                                                             | Services That the User Provides                                                                                                                                                                                                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                                                                                                                                                 |
| 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"> <li>♦ modifytimestamp</li> <li>♦ cn</li> <li>♦ mail</li> <li>♦ sn</li> <li>♦ GUID</li> <li>♦ givenName</li> <li>♦ member</li> </ul>                         |
| Linux User Management | <i>LUM_proxy</i>                                                                                                                                    | Searches the tree for LUM users.                                                                                                                                                                                                                                                                        |
| NetStorage            | <i>NetStorage_Proxy</i><br><br>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_name</i> admin                                                                                                                            | <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</i> -SambaProxy                                                                                                                      | 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-servername  | ♦ The Universal Password policy associated with the AFP users grants this proxy user the right to retrieve AFP user passwords.         |
| Archive Versioning | Archive Versioning Proxy | ♦ This user has Read and Write rights to the archived volume.                                                                          |
| CIFS               | CifsProxyUser-servername | ♦ 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"> <li>♦ Additional eDirectory rights include:</li> </ul> <p><b>[Entry Rights]</b></p> <p>Browse</p> <p>LDAP ACL representation:</p> <p>1#subtree#iFolderProxy#</p> <p><b>[All Attributes Rights]</b></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"> <li>♦ If created, this proxy user has Search rights on Unix Config &amp; Unix Workstation Objects.</li> </ul>                                                                                                                                                                                                                                                                                                                                            |
| NetStorage            | NetStorage_Proxy        | <ul style="list-style-type: none"> <li>♦ Additional eDirectory rights:</li> </ul> <p><b>[Entry Rights]</b></p> <p>Browse</p> <p>LDAP ACL representation:</p> <p>1#subtree#NetStorage_Proxy#</p> <p><b>[All Attributes Rights]</b></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"> <li>♦ Additional eDirectory rights:</li> </ul> <p>Supervisor right to the container it was created in.</p>                                                                                                                                                                                                                                                                                                                                               |
| Samba (Novell)        | server_name-SambaProxy  | <ul style="list-style-type: none"> <li>♦ The Universal Password policy associated with the Samba users grants this proxy user the right to retrieve user passwords.</li> <li>♦ Additional eDirectory rights: <ul style="list-style-type: none"> <li>Rights to itself – Supervisor attribute right</li> <li>Rights to the OU where it is located</li> <li>All Attribute rights – Read Write</li> <li>Entry rights – Browse Create</li> <li>samba* – Create Read Write</li> </ul> </li> </ul> |

## 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 264](#)
- ♦ [Section I.3.2, “Proxy User Impacts on User Connection Licenses,” on page 267](#)
- ♦ [Section I.3.3, “Limiting the Number of Proxy Users in Your Tree,” on page 267](#)
- ♦ [Section I.3.4, “Proxy Users and Passwords,” on page 269](#)

### 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 264](#)
- ♦ [“Do Not Manually Configure Proxy Users” on page 266](#)
- ♦ [“Avoid Assigning an Admin User As a Proxy User” on page 266](#)

#### 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-<br>servername | <p>By default, the AFP YaST install automatically</p> <ul style="list-style-type: none"><li>♦ Creates a proxy user named <code>afpProxyUser-servername</code> in the same context as the server.</li><li>♦ Creates a Universal Password Policy that you can assign to AFP users after the install.</li><li>♦ Generates a password and stores it in either CASA or in an encrypted file on the server, depending on which option you select.</li></ul> <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-<br><i>servername</i> | <p>By default, the CIFS YaST install automatically</p> <ul style="list-style-type: none"> <li>Creates a proxy user named <i>cifsProxyUser-servername</i> in the same context as the server.</li> <li>Creates a Universal Password Policy that you can assign to CIFS users after the install.</li> <li>Generates a password, and stores it in either CASA or in an encrypted file on the server, depending on which option you select.</li> </ul> <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 | <i>LUM_proxy</i> (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                   | <i>server_name</i> admin            | <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)     | <i>server_name-SambaProxy</i> | <p>By default, the Samba proxy user is created in the container specified as the Base Context for Samba Users and is named <i>servername-sambaProxyUser</i>.</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"> <li>♦ 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.</li> <li>♦ 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.</li> <li>♦ If you specify an existing eDirectory user but enter a new password, you are prompted to change the password for that user.</li> </ul> |

## 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 267](#).

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 | <p>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.</p> <p>For LUM there is no option to have a system-generated password.</p> <p>For DNS, DHCP, and NetStorage, the install admin's credentials are used by default. This has separate security implications as outlined in <a href="#">"Avoid Assigning an Admin User As a Proxy User" on page 266</a>.</p> | <p>This approach requires no proxy user planning.</p> <p>Services are installed at the same time as the OES server.</p> <p>This is a good option for small organizations or installations where only a few services are used.</p> <p>This is not a good option if security policies dictate that all passwords must be reset periodically.</p> |

| 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"> <li>♦ Centralized eDirectory administration</li> <li>♦ 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.</li> </ul> <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 269](#)
- ♦ [“Passwords Are Stored on the Server” on page 269](#)
- ♦ [“Avoid Password Expiration Problems” on page 270](#)

#### 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 CASACli 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 CASACli 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 CASACli 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 266](#).

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 264](#)). 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 267](#).

## **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 Kerberos 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.<br><br>arkuser is that low-privileged user.                                                                                                                                                                       |
| dhcpd                     | DHCP                            | DHCP accesses local resources through this or an alternatively specified user.<br><br>If the DHCP lease and configuration files are stored on NSS, the user must be moved to eDirectory and LUM enabled.<br><br>dhcpd 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.<br><br>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.<br><br>In case of clusters, DNS data is on NSS volume, and so the user has to be created in eDirectory as well.<br><br>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.                                                                                                                                                                                                                                                               |
| novlxregd                 | XTier                           | The XTier Registry Daemon (novell-xregd) runs as this user.<br><br>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. |
| novlxrsvd                 | XTier                           | The XTier Server Daemon (novell-xrsvd) runs as this user.<br><br>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             | The Apache daemon runs as this user.<br><br>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. |

## 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                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lprint (POSIX)<br>lprintgrp (eDirectory)  | iPrint             | The iPrint daemons use the group ID (gid) of this group to run.<br><br>If iPrint is moved to NSS, the lprintgrp group is created in eDirectory.                                                                                                                                                                                                                                                          |
| 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              | The XTier daemons use the group id (gid) of this group to run.<br><br>Apache (wwwrun) is a group member because it needs XTier socket access.<br><br>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. |
| <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 <a href="#">"The Samba connection:" on page 94</a> .                                                                                                                                                                                                   |
| shadow                                    | QuickFinder        | Used by QuickFinder and other Web services.                                                                                                                                                                                                                                                                                                                                                              |

| System User or Group Name | Associated Service | Purpose                                                                                                                                                                                                                                             |
|---------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| www                       | Apache             | Apache (wwwrun) and tomcat (novlwww) 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 novlxsrvd 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. |

## I.8 Auditing System Users

It is the nature of the Linux operating system and the POSIX security model that the `root` user has access to all system information stored on the local server. Due to this fact, some organizations choose to monitor the activities of privileged users.

If you are interested in monitoring such activities, two Novell products can assist you.

- ♦ **Novell Sentinel:** Universal Password events can be monitored using Novell Sentinel. You enable this by modifying the NMAS Login Policy Object. For instructions, see [Auditing NMAS Events \(http://www.novell.com/documentation/nmas33/admin/data/bwmt40o.html\)](http://www.novell.com/documentation/nmas33/admin/data/bwmt40o.html). Then refer to the [Novell Sentinel Documentation \(http://www.novell.com/documentation/sentinel6/\)](http://www.novell.com/documentation/sentinel6/) for further instructions.
- ♦ **Privileged User Manager:** This product lets you monitor root user activities on the OES server by collecting data, analyzing keystrokes, and creating indelible audit trails. For more information, see the [Novell Privileged User Manager Documentation \(http://www.novell.com/documentation/privilegedusermanager22/index.html\)](http://www.novell.com/documentation/privilegedusermanager22/index.html).



# Administrative Users in OES 2 SP2

J

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.<br><br>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.<br><br>The default is the Tree Admin.                                                                                                                                                |



# Coordinating Password Policies Among Multiple File Services



- ♦ [Section K.1, “Overview,” on page 279](#)
- ♦ [Section K.2, “Concepts and Prerequisites,” on page 279](#)
- ♦ [Section K.3, “Examples,” on page 281](#)
- ♦ [Section K.4, “Deployment Guidelines for Different Servers and Deployment Scenarios,” on page 283](#)

## K.1 Overview

OES 2 SP2 includes native file services for Windows and Macintosh\* workstations:

| Macintosh Workstations                                       | Windows Workstations                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>♦ Novell AFP</li></ul> | <ul style="list-style-type: none"><li>♦ Novell CIFS</li><li>♦ Novell Samba</li><li>♦ Domain Services for Windows (DSfW)</li></ul> <p>DSfW is not classified as a file service, but it includes a customized version of Samba that is different from Novell Samba.</p> |

Each of these services requires that users who access them have Password policies that meet specific requirements. Users can be governed by only one Password policy at a time, so if any of your network users require access to more than one of the file services, you need to coordinate the Password policies that govern the users to ensure that they can access the different file services.

## K.2 Concepts and Prerequisites

Prerequisites for AFP, CIFS, and Samba access are explained in the following sections:

- ♦ [Section K.2.1, “Prerequisites for File Service Access,” on page 279](#)
- ♦ [Section K.2.2, “eDirectory contexts,” on page 280](#)
- ♦ [Section K.2.3, “Password Policies and Assignments,” on page 280](#)

### K.2.1 Prerequisites for File Service Access

The following are the prerequisites for user access to AFP, CIFS, and Samba services:

- ♦ The eDirectory context under which users are searched for must be configured during service configuration.
- ♦ The users need to be governed by Password policies that enable Universal Password for them.

- ♦ The Password policies governing the users who need access to these services must be selected during service configuration. The services auto-create default password policies for themselves, but the Password policies to use here must be the actual policies governing users who need access to these services.
- ♦ There must be at least one writable replica of NMAST™ version 3.2 or later having the user object trying to access the AFP or CIFS server. NMAST 3.2 is already present on OES 2 and OES 2 SP2 servers, as well as on servers with eDirectory 8.8.2 installed. On OES 1 and NetWare® servers with a lone writable replica of a AFP or CIFS user, NMAST should be upgraded by upgrading to the Novell® Security Services 2.0.6 on eDirectory 8.7.3 SP10 or eDirectory 8.8.2.
- ♦ The file access services will provide access/visibility to the users as per the trustee rights they have on the volumes and files.

In addition, Samba (on both DSFW and non-DSFW servers) has the following additional requirements:

- ♦ The users must be LUM-enabled on the server.
- ♦ The users must be members of a LUM-enabled group on the server holding the volumes.
- ♦ Samba users must be created in a container or partition that has a <Samba-qualified password policy> assigned to it.

## K.2.2 eDirectory contexts

- ♦ **AFP:** Requires that user contexts be specified during the YaST configuration. These are the contexts under which the user objects will be searched for during an authentication. In a name-mapped (existing tree) install, if the context resides in a DSfW domain, the context can be specified either in the domain name format (Active Directory format) or in the X.509 format.
- ♦ **CIFS:** The eDirectory contexts of users can be specified either in the domain name format (Active Directory format) or in the X.509 format.
- ♦ **Samba:** Depends on LUM to search for the user in eDirectory and therefore doesn't require an eDirectory context.

## K.2.3 Password Policies and Assignments

- ♦ **AFP:** Creates a default Password policy as part of the AFP configuration. This policy is created in the security container as an example. It is not automatically attached to any user objects.

AFP requires the Password policies governing the AFP users to be specified as part of AFP configuration. For this purpose, AFP displays all Password policies in the tree and requires the OES admin to select the relevant policies. The Default AFP Policy is implicitly selected in the configuration process.

- ♦ **CIFS:** Similar in behavior to AFP with respect to password policies, it creates the Default CIFS Policy under the security container.
- ♦ **Samba:** Creates a default password policy, but does not attach this policy to any user.
- ♦ **DSFW:** The password policy in a DSfW environment is modeled after Active Directory Password policies. There is a single Password policy at the domain level, and it is configured during provisioning. eDirectory allows you to set policies at the user or container level. However, this is not recommended in a DSfW environment.

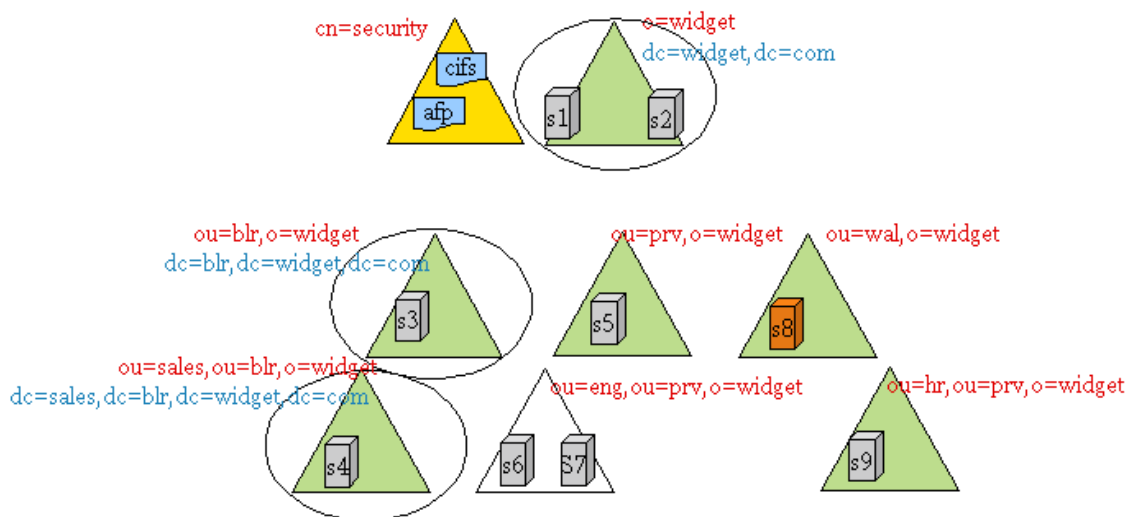
## K.3 Examples

- ♦ Section K.3.1, “Example 1: Complex Mixed Tree with a Mix of File Access Services and Users from across the Tree,” on page 281
- ♦ Section K.3.2, “Example 2: Mutually Exclusive Users,” on page 282

### K.3.1 Example 1: Complex Mixed Tree with a Mix of File Access Services and Users from across the Tree

- ♦ “Tree Setup” on page 281
- ♦ “OES/NetWare Servers” on page 281
- ♦ “File Services” on page 282
- ♦ “User Access to Services” on page 282
- ♦ “Rights Required for Installation and Administration” on page 282

**Figure K-1** Example 1



#### Tree Setup

The WIDGETS\_INC tree has the following configuration:

- ♦ o=widget, ou=blr, o=widget, and ou=sales, ou=blr, o=widget are eDir partitions as well as name mapped domains.
- ♦ ou=prv, o=widget, ou=wal, o=widget, ou=hr, ou=prv, o=widget are partitions (but not domains)
- ♦ ou=end, ou=prv, o=widget refers to the top of a subtree but not a partition. It is a container under the ou=prv, o=widget partition.

#### OES/NetWare Servers

- ♦ S1-S6 and S9 are OES servers
- ♦ S7 and S8 are NetWare<sup>®</sup> servers

## File Services

- ♦ S1, S2, S3, and S4 are DSfW servers and serve volumes over Samba and NCP™
- ♦ S5 serves its volumes over AFP and NCP
- ♦ S6 serves its volumes over CIFS and NCP
- ♦ S7 serves its volumes over AFP, CIFS, and NCP
- ♦ S8 serves its volumes over NetWare CIFS, NetWare AFP, and NCP
- ♦ S9 serves its volumes over AFP, Samba, and NCP

---

**NOTE:** Although Novell CIFS and Samba can both be installed on the same machine, they cannot run together because of a port conflict. The administrator can configure either Samba or Novell CIFS on a single machine, but not both.

---

## User Access to Services

Users from all over the tree can access services running on S1-S9. In order for users to be able to access AFP/CIFS services, the search contexts (eDirectory contexts) for these services should be configured to the subtrees under which those users can be found.

## Rights Required for Installation and Administration

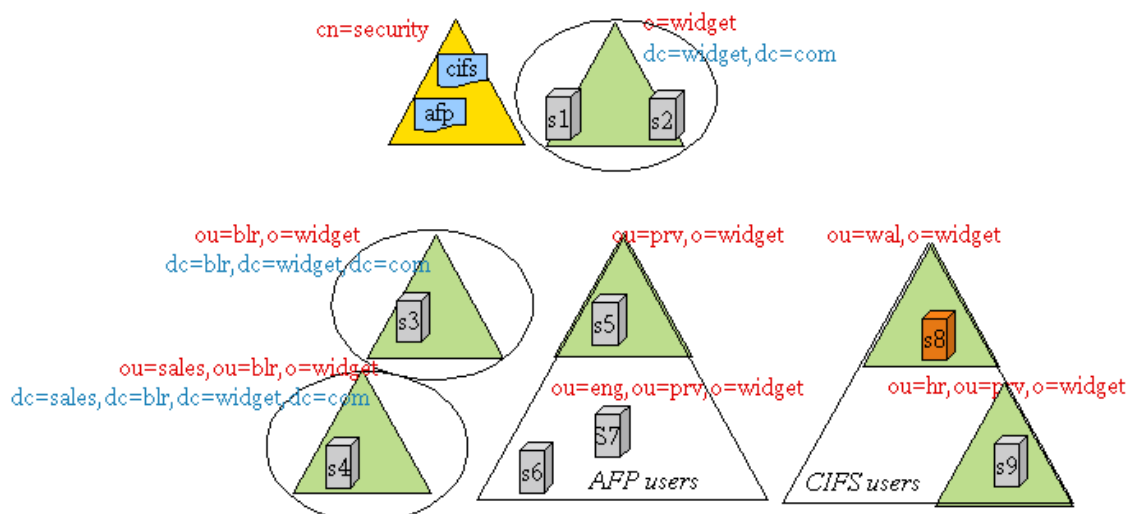
Installation and configuration in iManager must be done by an OES administrator. This is typically a container administrator in eDirectory who has supervisory privileges over the container where the server is being installed. This need not be the tree administrator.

## K.3.2 Example 2: Mutually Exclusive Users

- ♦ [“File Services” on page 283](#)
- ♦ [“Users” on page 283](#)

In this scenario, the setup of the tree and file services is similar to that in [Example 1](#), but the users are local to the context where a particular service is installed.

**Figure K-2** Example 2



## File Services

- S1, S2, S3, and S4 are DSfW servers and serve their volumes over Samba and NCP
- S5, S6, and S7 serve their volumes over AFP and NCP
- S8 and S9 serve their volumes over CIFS and NCP

## Users

For example, u1 is a user under the container ou=prv,o=widget and is expected to access AFP services on S5, S6, and S7. Similarly, u2 is a user under the container ou=wal,o=widget and is expected to access CIFS services on S8 and S9.

## K.4 Deployment Guidelines for Different Servers and Deployment Scenarios

- [Section K.4.1, “Deployment Scenario 1: Complex Mixed Scenario with a Mix of File Access Services,” on page 284](#)
- [Section K.4.2, “Deployment Scenario 2: Mutually /Exclusive Users,” on page 286](#)
- [Section K.4.3, “Deployment Scenario 3: Simple deployments,” on page 286](#)
- [Section K.4.4, “Modifying User Password Policies after AFP/CIFS/Samba/DSfW Is Installed,” on page 286](#)
- [Section K.4.5, “Adding New User eDirectory Contexts to AFP/CIFS after AFP/CIFS/Samba/DSfW Is Installed.,” on page 287](#)
- [Section K.4.6, “Enabling File Access for DSfW Servers Across Domains,” on page 287](#)

## K.4.1 Deployment Scenario 1: Complex Mixed Scenario with a Mix of File Access Services

- ♦ [“First Server in a New Tree \(Example1\)” on page 284](#)
- ♦ [“Subsequent Servers in a Tree \(Example 1\)” on page 284](#)

### First Server in a New Tree (Example1)

- ♦ [“Not recommended—non-name-mapped \(new tree\) S1 \(DSfW\) server” on page 284](#)
- ♦ [“Non-DSFW Server” on page 284](#)

#### Not recommended—non-name-mapped (new tree) S1 (DSfW) server

Installation is the same as for the Forest Root Domain (FRD). The tree is named as per domain naming standards. Samba is installed as part of DSFW installation. Neither AFP nor Novell CIFS can be installed/configured on this server because they are not compatible with the DSFW server.

In order for users to access NSS volumes on this server through Samba, the users need to fit the following constraints:

- ♦ They must be LUM-enabled
- ♦ Cross domain access is necessary for users from outside of the DSFW domain corresponding to this server to access the volumes on this server. This can be achieved by adding those contexts to the LUM context for the LUM workstation object that represents the domain controller.
- ♦ Winbind translates user principles to UIDs for non-NSS volumes. LUM enabling is not required for non-NSS volume access.

#### Non-DSFW Server

If the first server in the tree is a non-DSFW server, then any combination of AFP, Novell CIFS, or Samba can be installed on this server. Because the tree is being newly created, the users, the proxy users (system users), and the Password policies will not be present. Use the following procedure for installation:

- 1 Install and configure the server with eDirectory, NSS, and other core services, but without selecting file access services.
- 2 Use iManager to create the Password policies to be assigned to the users.
- 3 Use iManager to create a system user (proxy user) to be used for the OES services.
- 4 Use the Yast install to configure the Novell AFP and Novell CIFS services as follows:
  - 4a Specify the proxy user and password that were created.
  - 4b Select the appropriate Password policies for the AFP or CIFS users.
  - 4c Specify the contexts under which to search for the AFP or CIFS users.
- 5 If the AFP/CIFS/Samba user objects are present on NetWare servers, upgrade Novell Security Services version 2.0.6 in order to upgrade to NMAS 3.2 on NetWare.

### Subsequent Servers in a Tree (Example 1)

- ♦ [“S2, S3, S4” on page 285](#)
- ♦ [“S5” on page 285](#)

- ♦ “S6” on page 285
- ♦ “S7” on page 285
- ♦ “S8” on page 285
- ♦ “S9” on page 285

## S2, S3, S4

Administrators need to decide whether these servers should be installed on a new domain or as additional domain controllers during capacity planning and deployment design. Follow the [\*OES 2 SP2: Domain Services for Windows Administration Guide\*](#) to deploy S3 and S4 in the tree.

## S5

- 1 Type the common proxy user/password that was used as part of the first server in the tree, or allow the AFP service to auto-create the proxy user in the server context.
- 2 Select the Password policies that govern the users that should be given access to AFP.
- 3 Do not use the AFP default Password policy as the Password policy for the users unless the AFP users are distinct from the CIFS/Samba users.

## S6

Use the same procedure as for S5. Do not use the CIFS default Password policy as the password policy for the users unless the CIFS users are distinct from the AFP/Samba users.

## S7

Use the same procedure as for S5 and S6. To avoid confusion, do not use the AFP or CIFS default policy as the Password policy for your common AFP/CIFS users. If the users are distinct, the default policies can be used.

## S8

- ♦ AFP and CIFS on NetWare don’t require proxy users or password policies for service access.
- ♦ NMAS needs to be upgraded to 3.2+, if this server hosts the only writable replica for a partition with AFP or CIFS users.
- ♦ If this NetWare box is migrated to OES2 SP2, the AFP and CIFS users are enabled for Universal Password. They need to either use a plain text authentication method, or log in through NCP (Novell Client) to synchronize their NDS<sup>®</sup> passwords to the Universal Password. AFP can auto-synchronize the Universal Password if the default DHX authentication method is used.

## S9

- ♦ Use the same procedure as for S5.
- ♦ Either use a common proxy user for all the services (AFP), or allow auto-generation of the proxy user/password for each AFP.
- ♦ To avoid confusion, do not use the AFP default password policy or the Samba default password policy for the common AFP and Samba users to avoid confusion. If the users are distinct, the default policies can be used.

## K.4.2 Deployment Scenario 2: Mutually /Exclusive Users

In some trees, AFP, CIFS, and Samba might be employed, but the users are partitioned in such a way that each user has access to AFP, to CIFS or to Samba, but not to all of them.

### S1, S2, S3, S4

DSfW servers with Samba. All the users are under `dc=blr,dc=widgets,dc=com`.

- ♦ You can use the default Password policy provided by Domain Services for Windows for all the users in this subtree.
- ♦ You can create and use a single proxy user/password under `dc=blr,dc=widgets,dc=com` for all the servers providing Samba.

### S5, S6, S7

Servers with AFP. All the users are under `ou=prv,o=widgets`.

- ♦ You can use the default password policy provided by AFP for all the users in this subtree.
- ♦ You can create and use a single proxy user/password under `ou=prv,o=widgets` for all the services providing AFP.

### S8, S9

Servers with CIFS. All the users are under `ou=wal,o=widgets`.

- ♦ You can use the default password policy provided by CIFS for all the users in this subtree.
- ♦ You can create and use a single proxy user/password under `ou=prv,o=widgets` for all the services providing CIFS.

## K.4.3 Deployment Scenario 3: Simple deployments

Simple deployments require very little planning.

- ♦ Auto-generated proxy users by each service might be a good idea. This does not require that you plan the proxy user context.
- ♦ Use the default password policies if one of the following cases is true:
  - ♦ Case A: All users can access all file services. Use one of the default policies and assign it to all the users, and select the same policy for all the services.
  - ♦ Case B: Only one type of file service is deployed throughout the tree. If only AFP or CIFS or Samba is deployed, set the password policies for all the users to the default Password policy created by the particular service, and choose that default policy as part of the YaST configuration for the service.

## K.4.4 Modifying User Password Policies after AFP/CIFS/Samba/DSfW Is Installed

After a new password policy is assigned to an AFP/CIFS/Samba or DSfW user, rerun the YaST-based configuration and select the new Password policies.

## **K.4.5 Adding New User eDirectory Contexts to AFP/CIFS after AFP/CIFS/Samba/DSfW Is Installed.**

After a new user context is created, rerun the YaST-based configuration and select the new eDirectory context.

## **K.4.6 Enabling File Access for DSfW Servers Across Domains**

DSfW requires that users be LUM-enabled to access NSS file services through Samba. For a user to access a DSfW server in a different domain, the user needs to be a LUM-enabled user on the other server. DSfW provisioning establishes shortcut trust between domains. Users from other domains in the forest can access non-NSS volumes as long as they have rights on the resources.

To achieve this, the context of the partition root for the user object should be added as a search context for LUM. This needs to be done in addition to the trustee rights provided to the user (or the user's group) as part of file system rights.



# Documentation Updates



This section summarizes the changes made to this manual since the initial release of Novell® Open Enterprise Server 2.

## July 15, 2010

| Chapter or Section Changed                                                                                       | Summary of Changes                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Section 1.5.1, "Dynamic Storage Technology," on page 23</a> and <a href="#">Table 3-1 on page 27</a> | These sections incorrectly stated that Dynamic Storage Technology (DST) is supported on NCP and POSIX volumes. Although that functionality was initially planned, and Novell hopes to add support for additional volume and file system types in a future release, DST is currently supported on only Novell Storage Services (NSS) volumes. |

## November 2009

| Chapter or Section Changed | Summary of Changes                         |
|----------------------------|--------------------------------------------|
| Various                    | The guide was updated to include OES 2 SP2 |

## July 31, 2009

| Chapter or Section Changed                                                   | Summary of Changes                        |
|------------------------------------------------------------------------------|-------------------------------------------|
| <a href="#">"System User and Group Management in OES 2 SP2" on page 257.</a> | Completely reworked and expanded Section. |
| <a href="#">"Administrative Users in OES 2 SP2" on page 277.</a>             | New Section.                              |

## June 22, 2009

| Chapter or Section Changed                                      | Summary of Changes |
|-----------------------------------------------------------------|--------------------|
| <a href="#">"Avoid Uninstalling eDirectory" on page 65.</a>     | New Section.       |
| <a href="#">"Novell-tomcat Is for OES Use Only" on page 70.</a> | New Section.       |

## May 6, 2009

| Chapter or Section Changed         | Summary of Changes                                                                                                                                                                                                                                                                                                                |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">“SLP” on page 113.</a> | Removed all information and instructions that refer to incompatibilities between Novell SLP and OpenSLP. This information was outdated.<br><br>Although there are differences in the two SLP services (see <a href="#">Table 12-4 on page 114</a> ), they are completely compatible regarding the sharing of service information. |

## May 4, 2009

| Chapter or Section Changed                                                 | Summary of Changes                                         |
|----------------------------------------------------------------------------|------------------------------------------------------------|
| <a href="#">“Changing the Server’s Address Configuration” on page 236.</a> | In response to a user comment, correct link to wrong file. |

## April 23, 2009

| Chapter or Section Changed                          | Summary of Changes                                              |
|-----------------------------------------------------|-----------------------------------------------------------------|
| <a href="#">“What’s New or Changed” on page 17.</a> | 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. |