

Planning and Implementation Guide

Open Enterprise Server 11 SP2

February 26, 2015

Novell®



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 © 2004–2014 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.
1800 South Novell Place
Provo, Utah 84606
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 \(http://www.novell.com/documentation/oes11\)](http://www.novell.com/documentation/oes11).

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	19
1.1 What's New or Changed in OES 11 SP1 January 2014 Patches	19
1.1.1 Novell CIFS	19
1.1.2 NetWare Core Protocol	19
1.2 What's New or Changed in OES 11 SP2	19
1.2.1 Install and Upgrade	20
1.2.2 Archive and Version Services	21
1.2.3 Novell AFP	21
1.2.4 Novell CIFS	21
1.2.5 Novell Cluster Services	22
1.2.6 Distributed File Services	27
1.2.7 Dynamic Storage Technology	28
1.2.8 Domain Services for Windows	28
1.2.9 DNS and DHCP	30
1.2.10 NetIQ eDirectory	30
1.2.11 Novell iFolder	30
1.2.12 Novell iPrint	30
1.2.13 Novell FTP	31
1.2.14 Novell Linux Volume Manager	31
1.2.15 Linux User Management	35
1.2.16 Migration	35
1.2.17 NetWare Core Protocol (NCP)	35
1.2.18 Linux POSIX Volumes	37
1.2.19 NetStorage	40
1.2.20 QuickFinder	40
1.2.21 Novell Remote Manager	40
1.2.22 Novell Storage Services (NSS)	42
1.2.23 Storage Management Services	43
1.2.24 File Systems Management (Storage)	43
1.2.25 NSS Auditing Client Logger (VLOG)	44
1.2.26 Web Services	44
1.3 What's New or Changed in OES 11 SP1	46
1.3.1 AFP	47
1.3.2 Archive and Version Services	47
1.3.3 CIFS	47
1.3.4 Distributed File Services	47
1.3.5 DNS and DHCP	48
1.3.6 Domain Services for Windows	48
1.3.7 Dynamic Storage Technology	49
1.3.8 eDirectory	50
1.3.9 File Systems Management (Storage)	50
1.3.10 Install	50
1.3.11 iPrint	51
1.3.12 Linux POSIX Volume Support	51
1.3.13 Linux User Management	54
1.3.14 Migration Tool	54
1.3.15 NCP Server	55
1.3.16 NetStorage	55
1.3.17 Novell Cluster Services 2.1	55
1.3.18 Novell Linux Volume Manager	59

1.3.19	Novell Remote Manager	61
1.3.20	Novell Samba	61
1.3.21	Novell Storage Services	61
1.3.22	NSS Auditing Client Logger (VLOG)	62
1.3.23	QuickFinder	62
1.3.24	Storage Management Services	62
1.3.25	Web Services	63
1.4	What's New or Changed in OES 11	63
1.4.1	AFP	64
1.4.2	Archive and Version Services	64
1.4.3	CIFS	64
1.4.4	Distributed File Services (DFS)	65
1.4.5	DNS and DHCP	65
1.4.6	Domain Services for Windows	66
1.4.7	Dynamic Storage Technology	66
1.4.8	File Systems and Storage	66
1.4.9	Install	68
1.4.10	iPrint	68
1.4.11	Linux POSIX Volumes	69
1.4.12	Linux User Management	69
1.4.13	Migration Tool	69
1.4.14	NCP Server	70
1.4.15	NetStorage	70
1.4.16	Novell Cluster Services 2.0	70
1.4.17	Novell Linux Volume Manager	73
1.4.18	Novell Remote Manager	74
1.4.19	Novell Samba	77
1.4.20	Novell Storage Services	77
1.4.21	NSS Auditing Client Logger (VLOG) Utility	78
1.4.22	QuickFinder	79
1.4.23	Storage Management Services (SMS)	79
1.4.24	Web Services	79
1.5	Where's NetWare?	79
1.5.1	NetWare References in This Guide and Elsewhere	79
1.5.2	NetWare Documentation	79

2 Welcome to Open Enterprise Server 11 SP2 81

3 Planning Your OES 11 SP2 Implementation 83

3.1	What Services Are Included in OES 11 SP2?	83
3.2	Which Services Do I Need?	90
3.3	Exploring OES 11 SP2 services	90
3.4	Plan for eDirectory	90
3.4.1	Installing Into a New Tree	90
3.4.2	Installing Into an Existing Tree	91
3.5	Prepare Your Existing eDirectory Tree for OES	91
3.6	Identify a Purpose for Each Server	92
3.7	Understand Server Requirements	92
3.8	Understand User Restrictions and Linux User Management	92
3.9	Caveats to Consider Before You Install	92
3.9.1	Adding a Linux Node to a Cluster Ends Adding More NetWare Nodes	93
3.9.2	Always Double-Check Service Configurations Before Installing	93
3.9.3	Back Button Doesn't Reset Configuration Settings	93
3.9.4	Cluster Upgrades Must Be Planned Before Installing OES	94
3.9.5	Common Proxy Password Policy Should Be Assigned	94
3.9.6	Cross-Protocol File Locking Might Need To Be Reconfigured if AFP or CIFS Is Functioning on an NCP Server	94

3.9.7	Do Not Create Local (POSIX) Users	95
3.9.8	Do Not Upgrade to eDirectory 8.8 Separately	95
3.9.9	Follow the Instructions for Your Chosen Platforms	95
3.9.10	If You've Ever Had OES 1 Servers with LUM and NSS Installed	95
3.9.11	iFolder 3.9.2 Considerations	98
3.9.12	Incompatible TLS Configurations Give No Warning	99
3.9.13	Installing into an Existing eDirectory Tree	99
3.9.14	NetStorage Caveats	100
3.9.15	NetWare Caveats	101
3.9.16	Novell Distributed Print Services Cannot Migrate to Linux	101
3.9.17	NSS Caveats	101
3.9.18	Plan eDirectory Before You Install	102
3.9.19	Samba Enabling Disables SSH Access	102
3.9.20	Unsupported Service Combinations	102
3.9.21	VNC Install Fails to Set the IP Address in /etc/hosts	105
3.10	Consider Coexistence and Migration Issues	105
3.11	Understand Your Installation Options	106
3.11.1	OES 11 SP2 Installation Overview	106
3.11.2	About Your Installation Options	107
3.11.3	Use Predefined Server Types (Patterns) When Possible	107
3.11.4	If You Want to Get Acquainted with SP2 First	108

4 Getting and Preparing OES 11 SP2 Software 109

4.1	Do You Have Upgrade Protection?	109
4.2	64-Bit Only	109
4.3	Do You Want to Purchase OES 11 SP2 or Evaluate It?	109
4.4	Evaluating OES 11 SP2 Software	110
4.4.1	Understanding OES 11 SP2 Software Evaluation Basics	110
4.4.2	Evaluating OES 11 SP2	110
4.4.3	Installing OES 11 for Evaluation Purposes	111
4.5	Downloading and Preparing OES Software	111
4.5.1	Downloading OES 11 SP2 Software from the Novell Web Site	111
4.5.2	Preparing the Installation Media	112
4.5.3	Installing Purchased Activation Codes after the Evaluation Period Expires	112
4.6	Licensing	113
4.6.1	The OES 11 SP2 Licensing Model	113
4.6.2	OES Doesn't Support NLS	113

5 Installing OES 11 SP2 115

5.1	Installing OES 11 SP2 on Physical Servers	115
5.1.1	What's Next	115
5.2	Installing OES 11 SP2 Servers in a Xen VM	116
5.3	Installing OES 11 SP2 Servers in a KVM Virtual Machine	116

6 Caveats for Implementing OES 11 SP2 Services 117

6.1	AFP	118
6.1.1	Anti-Virus Solutions and AFP	118
6.2	Avoiding POSIX and eDirectory Duplications	118
6.2.1	The Problem	118
6.2.2	Three Examples	118
6.2.3	Avoiding Duplication	119
6.3	CIFS	120
6.3.1	Changing the Server IP Address	120
6.3.2	Renaming CIFS Share Names on NSS Volumes Results in Two Share Names	120
6.4	CUPS on OES 11 SP2	121

6.5	DSfW: MMC Password Management Limitation	121
6.6	eDirectory	121
6.6.1	Avoid Uninstalling eDirectory When Possible	121
6.6.2	Avoid Renaming Trees and Containers	122
6.6.3	Default Static Cache Limit Might Be Inadequate	122
6.6.4	eDirectory Not Restarting Automatically	122
6.6.5	One Instance Only	122
6.6.6	Special Characters in Usernames and Passwords	122
6.7	iFolder 3.9.22	123
6.8	iPrint	123
6.8.1	Advanced Printing Options	123
6.8.2	Authentication Dialog Not Displaying for Secure Printers from Terminal Servers	123
6.8.3	Cluster Failover Between Mixed Platforms Not Supported	123
6.8.4	iManager Plug-Ins Are Platform-Specific	124
6.8.5	iPrint Client for Linux Doesn't Install Automatically	124
6.8.6	iPrint Disables CUPS Printing on the OES Server	124
6.8.7	Linux and Macintosh Client Printer Installation Fails When Communicating via Proxy	124
6.8.8	Printer Driver Uploading on OES 11 SP2 Might Require a CUPS Administrator Credential	124
6.8.9	Printer Driver Uploading Support	124
6.9	LDAP—Preventing “Bad XML” Errors	125
6.10	LUM Cache Refresh No Longer Persistent	125
6.11	Management	125
6.11.1	iManager RBS Configuration with OES 11	126
6.11.2	Storage Error in iManager When Accessing a Virtual Server	126
6.11.3	Truncated DOS-Compatible Short Filenames Are Not Supported at a Terminal Prompt	127
6.11.4	LUM-Enabling Required for Full Administrative Access	127
6.12	McAfee Antivirus Requires Additional Configuration	127
6.13	NCP	127
6.13.1	NCP Doesn't Equal NSS File Attribute Support	128
6.13.2	Opening MS Office Files Using Novell Client for Windows 7	128
6.14	Novell-tomcat Is for OES Use Only	128
6.15	NSS	128
6.15.1	For GroupWise, Change the Default Name Space to UNIX	129
6.15.2	Junction Target Support	129
6.16	OpenLDAP on OES	129
6.17	Samba	129
6.18	SLP Registrations Are Not Retrieved from a Novell SLP DA	129
6.19	Synchronizing NMAS Login Methods Is Required to Avoid Login Failures	129
6.20	Using NLVM with Linux Software RAIDs	130
6.20.1	Linux Software RAIDs	130
6.20.2	Linux Software RAIDs Are Not Cluster Aware	130
6.20.3	Linux Software RAIDs Are Not Recommended for the System Device	131
6.21	Virtualization	131
6.21.1	Always Close Virtual Machine Manager When Not in Use	131
6.21.2	Always Use Timesync Rather Than NTP	131
6.21.3	Backing Up a Xen Virtual Machine	131
6.21.4	Time Synchronization and Virtualized OES	132
6.21.5	NSS Considerations	132

7 Upgrading to OES 11 SP2

133

7.1	Caveats to Consider Before Upgrading	133
7.1.1	About Previously Installed Packages (RPMs)	133
7.1.2	Only One eDirectory Instance Is Supported on OES Servers	133
7.1.3	Before Upgrading to OES 11 SP2 You Must Update Sentinel	133

7.2	OES 11 SP2 Upgrade Paths	134
7.3	NetWare 6.5 SP8 Upgrade Paths	134
8	Migrating Existing Servers and Data	135
8.1	Supported OES 11 SP2 Migration Paths	135
8.2	Migration Tools and Purposes	135
9	Virtualization in OES 11 SP2	137
9.1	Graphical Overview of Virtualization in OES 11 SP2	137
9.2	Why Install OES Services on Your VM Host?	138
9.3	Services Supported on VM Hosts and Guests	139
9.4	Xen VMs Need Ext2 for the System /Boot Volume	140
10	Clustering and High Availability	141
11	Managing OES 11 SP2	143
11.1	Overview of Management Interfaces and Services	143
11.2	Using OES 11 SP2 Welcome Pages	144
11.2.1	The Welcome Site Requires JavaScript, Apache, and Tomcat	144
11.2.2	Accessing the Welcome Web Site	145
11.2.3	The Welcome Web Site Is Available to All Users	145
11.2.4	Administrative Access from the Welcome Web Site	145
11.3	OES Utilities and Tools	145
11.4	iManager Differences on OES	155
11.5	SSH Services on OES 11 SP2	155
11.5.1	Overview	155
11.5.2	Setting Up SSH Access for LUM-enabled eDirectory Users	157
12	Network Services	161
12.1	TCP/IP	161
12.1.1	Coexistence and Migration Issues	161
12.2	DNS and DHCP	162
12.2.1	DNS Differences Between NetWare and OES 11 SP2	162
12.2.2	DHCP Differences Between NetWare and OES 11 SP2	163
12.3	Time Services	164
12.3.1	Overview of Time Synchronization	164
12.3.2	Planning for Time Synchronization	168
12.3.3	Coexistence and Migration of Time Synchronization Services	171
12.3.4	Implementing Time Synchronization	172
12.3.5	Configuring and Administering Time Synchronization	174
12.3.6	Daylight Saving Time	175
12.4	Discovery Services	175
12.4.1	Novell SLP and OpenSLP	175
12.5	SLP	176
12.5.1	Overview	176
12.5.2	Comparing Novell SLP and OpenSLP	178
12.5.3	Setting Up OpenSLP on OES 11 SP2 Networks	179
12.5.4	Using Novell SLP on OES 11 SP2 Networks	184
12.5.5	TIDs and Other Help	188

13 Storage and File Systems	189
13.1 Overview of OES 11 SP2 Storage	189
13.1.1 Databases	189
13.1.2 iSCSI	190
13.1.3 File System Support in OES	190
13.1.4 Storage Basics by Platform	192
13.1.5 Storage Options	192
13.1.6 NetWare Core Protocol Support (Novell Client Support) on Linux	194
13.2 Planning OES File Storage	194
13.2.1 Directory Structures	194
13.2.2 File Service Support Considerations	194
13.2.3 General Requirements for Data Storage	195
13.2.4 OES 11 SP2 Storage Planning Considerations	195
13.2.5 NSS Planning Considerations	201
13.3 Coexistence and Migration of Storage Services	201
13.3.1 Databases	201
13.3.2 NetWare 6.5 SP8	202
13.3.3 OES 11 SP2 File System Options	202
13.4 Configuring and Maintaining Storage	203
13.4.1 Managing Directories and Files	203
13.4.2 Managing NSS	203
13.4.3 Optimizing Storage Performance	205
14 eDirectory, LDAP, and Domain Services for Windows	207
14.1 Overview of Directory Services	207
14.2 eDirectory	208
14.2.1 Installing and Managing eDirectory on OES	208
14.2.2 Planning Your eDirectory Tree	209
14.2.3 eDirectory Coexistence and Migration	209
14.3 LDAP (eDirectory)	209
14.3.1 Overview of eDirectory LDAP Services	210
14.3.2 Planning eDirectory LDAP Services	210
14.3.3 Migration of eDirectory LDAP Services	210
14.3.4 eDirectory LDAP Implementation Suggestions	210
14.4 Domain Services for Windows	210
14.4.1 Graphical Overview of DSfW	211
14.4.2 Planning Your DSfW Implementation	214
14.4.3 Implementing DSfW on Your Network	214
15 Users and Groups	217
15.1 Creating Users and Groups	217
15.2 Linux User Management: Access to Linux for eDirectory Users	217
15.2.1 Overview	218
15.2.2 LUM Changes	223
15.2.3 Planning	223
15.2.4 LUM Implementation Suggestions	223
15.3 Identity Management Services	226
15.4 Using the Identity Manager 4.0.2 Bundle Edition	226
15.4.1 What Am I Entitled to Use?	227
15.4.2 System Requirements	227
15.4.3 Installation Considerations	227
15.4.4 Getting Started	227
15.4.5 Activating the Bundle Edition	228

16 Access Control and Authentication	231
16.1 Controlling Access to Services	231
16.1.1 Overview of Access Control.	231
16.1.2 Planning for Service Access	237
16.1.3 Coexistence and Migration of Access Services.	240
16.1.4 Access Implementation Suggestions.	240
16.1.5 Configuring and Administering Access to Services	240
16.2 Authentication Services	242
16.2.1 Overview of Authentication Services	242
16.2.2 Planning for Authentication	245
16.2.3 Authentication Coexistence and Migration	245
16.2.4 Configuring and Administering Authentication.	245
17 Backup Services	247
17.1 Services for End Users	247
17.2 System-Wide Services.	247
17.2.1 Links to Backup Partners.	247
17.2.2 Novell Storage Management Services (SMS)	247
17.2.3 SLES 11 Backup Services.	248
18 File Services	249
18.1 Overview of File Services.	249
18.1.1 Using the File Services Overviews	250
18.1.2 FTP Services	250
18.1.3 NetWare Core Protocol	250
18.1.4 NetStorage.	251
18.1.5 Novell AFP.	254
18.1.6 Novell CIFS	255
18.1.7 Novell iFolder 3.9.22	256
18.1.8 Novell Samba	257
18.2 Planning for File Services	259
18.2.1 Deciding Which Components Match Your Needs	259
18.2.2 Comparing Your CIFS File Service Options.	260
18.2.3 Planning Your File Services.	261
18.3 Coexistence and Migration of File Services	262
18.3.1 Novell Client (NCP)	263
18.3.2 NetStorage.	263
18.3.3 Novell AFP.	263
18.3.4 Novell CIFS	263
18.3.5 Novell iFolder 3.9.2	264
18.3.6 Samba	264
18.4 Aligning NCP and POSIX File Access Rights	264
18.4.1 Managing Access Rights	265
18.4.2 Providing a Private Work Directory	266
18.4.3 Providing a Group Work Area	266
18.4.4 Providing a Public Work Area	267
18.4.5 Setting Up Rights Inheritance	267
18.5 Novell FTP (Pure-FTPd) and OES 11 SP2	268
18.5.1 Planning for Pure-FTPd	268
18.5.2 Installing Pure-FTPd	268
18.5.3 Home Directory Support in Pure-FTPd	268
18.5.4 Configuring Pure-FTPd on an OES 11 SP2 Server.	269
18.5.5 Administering and Managing Pure-FTPd on an OES 11 SP2 Server	270
18.5.6 Cluster Enabling Pure-FTPd in an OES 11 SP2 Environment.	274
18.5.7 Migrating Pure-FTPd From NetWare to Linux	275
18.5.8 Troubleshooting Pure-FTPd from Novell	276

18.6	NCP Implementation and Maintenance	276
18.6.1	The Default NCP Volume.	276
18.6.2	Creating NCP Home and Data Volume Pointers	276
18.6.3	Assigning File Trustee Rights	277
18.6.4	NCP Caveats	277
18.6.5	NCP Maintenance	277
18.7	NetStorage Implementation and Maintenance	277
18.7.1	About Automatic Access and Storage Locations	278
18.7.2	About SSH Storage Locations	278
18.7.3	Assigning User and Group Access Rights	278
18.7.4	Authenticating to Access Other Target Systems	279
18.7.5	NetStorage Authentication Is Not Persistent by Default	279
18.7.6	NetStorage Maintenance	279
18.8	Novell AFP Implementation and Maintenance	279
18.8.1	Implementing Novell AFP File Services	280
18.8.2	Maintaining Novell AFP File Services	280
18.9	Novell CIFS Implementation and Maintenance	280
18.9.1	Implementing Novell CIFS File Services	280
18.9.2	Maintaining Novell CIFS File Services	280
18.10	Novell iFolder 3.9.2 Implementation and Maintenance	281
18.10.1	Managing Novell iFolder 3.9.2	281
18.10.2	Configuring Novell iFolder 3.9.2 Servers	281
18.10.3	Creating and Enabling Novell iFolder 3.9.2 Users	281
18.10.4	Novell iFolder 3.9.2 Maintenance	281
18.11	Samba Implementation and Maintenance	282
18.11.1	Implementing Samba File Services	282
18.11.2	Maintaining Samba File Services	282
19	Print Services	283
19.1	Overview of Print Services	283
19.1.1	Using This Overview	283
19.1.2	iPrint Components	283
19.1.3	iPrint Functionality	284
19.2	Planning for Print Services	285
19.3	Coexistence and Migration of Print Services	285
19.4	Print Services Implementation Suggestions	286
19.4.1	Initial Setup	286
19.4.2	Implementation Caveats	287
19.4.3	Other Implementation Tasks	287
19.5	Print Services Maintenance Suggestions	287
20	Search Engine (QuickFinder)	289
21	Web Services	291
22	Security	293
22.1	Overview of OES Security Services	293
22.1.1	Application Security (AppArmor)	293
22.1.2	NSS Auditing Engine	293
22.1.3	Encryption (NICI)	294
22.1.4	General Security Issues	295
22.2	Planning for Security	295
22.2.1	Comparing the Linux and the Novell Trustee File Security Models	295
22.2.2	User Restrictions: Some OES Limitations	297
22.2.3	Ports Used by OES 11 SP2	297

22.3	Configuring and Administering Security	299
22.4	Resolving Nessus Security Scan Issues	299
22.4.1	Port dns (53/tcp): DNS Server Zone Transfer Information Disclosure (AXFR)	300
22.4.2	Port dns (53/udp): DNS Server Recursive Query Cache Poisoning Weakness	300
22.4.3	Port dns (53/udp): DNS Server Cache Snooping Remote Information Disclosure	301
22.4.4	Port dns (53/udp): Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	301
22.4.5	Port ftp (21/tcp): Anonymous FTP Enabled	301
22.4.6	Port ftp (21/tcp): Multiple Vendor Embedded FTP Service Any Username Authentication Bypass	302
22.4.7	Port ldap: LDAP NULL BASE Search Access	302
22.4.8	Port smb (139/tcp) : Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials	302
22.4.9	Port ssh (22/tcp): SSH Protocol Version 1 Session Key Retrieval	303
22.4.10	Port (524/tcp): Novell NetWare ncp Service NDS Object Enumeration	303
22.4.11	Port www (443/tcp): SSL Certificate signed with an unknown Certificate Authority	303
22.4.12	Port www (443/tcp): SSL Version 2 (v2) Protocol Detection	304
22.4.13	Port www (tcp): SSL Weak Cipher Suites Supported	304
22.4.14	Port www (tcp): SSL Medium Strength Cipher Suites Supported	304
22.5	Links to Product Security Considerations	305
22.6	Links to Anti-Virus Partners	306

23 Certificate Management 307

23.1	Overview	307
23.1.1	SLES Default Certificates	307
23.1.2	OES Certificate Management	308
23.1.3	Multiple Trees Sharing a Common Root	309
23.2	Setting Up Certificate Management	309
23.2.1	Setting Up Automatic Certificate Maintenance	310
23.2.2	Eliminating Browser Certificate Errors	310
23.3	If You Don't Want to Use eDirectory Certificates	312

A Adding Services to OES Servers 313

B Changing an OES 11 SP2 Server's IP Address 315

B.1	Caveats and Disclaimers	315
B.2	Prerequisites	315
B.2.1	General	315
B.2.2	iPrint	316
B.2.3	Clustering	316
B.3	Changing the Server's Address Configuration	316
B.4	Reconfiguring the OES Services	316
B.5	Repairing the eDirectory Certificates	317
B.6	Completing the Server Reconfiguration	317
B.6.1	QuickFinder	317
B.6.2	DHCP	318
B.6.3	DSfW	318
B.6.4	iFolder	320
B.6.5	iPrint	321
B.6.6	NetStorage	321
B.7	Modifying a Cluster	321
B.8	Reconfiguring Services on Other Servers That Point to This Server	321

C	Updating/Patching OES 11 SP2 Servers	323
D	Quick Reference to OES User Services	325
E	OES 11 SP2 Browser Support	327
F	Client/Workstation OS Support	329
G	OES 11 SP2 Service Scripts	331
H	System User and Group Management in OES 11 SP2	335
H.1	About System Users and Groups	335
H.1.1	Types of OES System Users and Groups	335
H.1.2	OES System Users and Groups by Name	336
H.2	Understanding Proxy Users	337
H.2.1	What Are Proxy Users?	338
H.2.2	Why Are Proxy Users Needed on OES?	338
H.2.3	Which Services Require Proxy Users and Why?	338
H.2.4	What Rights Do Proxy Users Have?	340
H.3	Common Proxy User	342
H.3.1	Common Proxy User FAQ	342
H.3.2	Managing Common Proxy Users	345
H.4	Planning Your Proxy Users	346
H.4.1	About Proxy User Creation	346
H.4.2	There Are No Proxy User Impacts on User Connection Licenses	351
H.4.3	Limiting the Number of Proxy Users in Your Tree	351
H.4.4	Password Management and Proxy Users	353
H.5	Implementing Your Proxy User Plan	355
H.5.1	Tree-Wide Proxy Users	356
H.5.2	Service-Specific Proxy Users	356
H.5.3	Partition-Wide Proxy Users	356
H.5.4	Server-Wide Proxy User	356
H.5.5	Individual Proxy User Per-Server-Per-Service	357
H.6	Proxy Users and Domain Services for Windows	357
H.7	System Users	357
H.8	System Groups	358
H.9	Auditing System Users	360
I	Administrative Users in OES 11 SP2	361
J	Coordinating Password Policies Among Multiple File Services	363
J.1	Overview	363
J.2	Concepts and Prerequisites	363
J.2.1	Prerequisites for File Service Access	363
J.2.2	eDirectory contexts	364
J.2.3	Password Policies and Assignments	364
J.3	Examples	364
J.3.1	Example 1: Complex Mixed Tree with a Mix of File Access Services and Users from across the Tree	364
J.3.2	Example 2: Mutually Exclusive Users	366
J.4	Deployment Guidelines for Different Servers and Deployment Scenarios	367

J.4.1	Deployment Scenario 1: Complex Mixed Scenario with a Mix of File Access Services	367
J.4.2	Deployment Scenario 2: Mutually /Exclusive Users	369
J.4.3	Deployment Scenario 3: Simple deployments	369
J.4.4	Modifying User Password Policies after Samba/DSfW Is Installed	369
J.4.5	Adding New User eDirectory Contexts to AFP/CIFS after AFP/CIFS/Samba/DSfW Is Installed.	369
J.4.6	Enabling File Access for DSfW Servers Across Domains	370
K	Configuration and Log Files	371
K.1	AFP	371
K.2	Archive and Version Services	372
K.3	CIFS	372
K.4	Common Proxy	373
K.5	DFS	373
K.6	DHCP	373
K.7	DNS	374
K.8	Domain Services for Windows	374
K.9	Install	376
K.10	iFolder Server.	377
K.11	iPrint	378
K.12	Linux User Management	378
K.13	Migration Tool.	379
K.14	NetStorage	380
K.15	Novell Cluster Services	381
K.16	Novell Linux Volume Manager	381
K.17	Novell Storage Services	382
K.18	Novell Samba	382
K.19	NCP	383
K.20	QuickFinder	383
K.21	SMS	384
K.22	Vigil.	384
L	Small Footprint CIM Broker (SFCB)	385
L.1	Overview	385
L.2	OES CIM Providers	386
L.3	SFCB Is Automatically Installed with OES 11 SP2.	386
L.4	Coexistence with NRM and iManager in Earlier Releases.	387
L.5	SFCB and Linux User Management (LUM)	387
L.6	Links to More Information about WBEM and SFCB.	387
M	Documentation Updates	389
M.1	Summary of Changes—OES 11 SP1.	390
M.2	Summary of Changes—OES 11.	390

About This Guide

- ♦ Chapter 1, “What’s New or Changed,” on page 19
- ♦ Chapter 2, “Welcome to Open Enterprise Server 11 SP2,” on page 81
- ♦ Chapter 3, “Planning Your OES 11 SP2 Implementation,” on page 83
- ♦ Chapter 4, “Getting and Preparing OES 11 SP2 Software,” on page 109
- ♦ Chapter 5, “Installing OES 11 SP2,” on page 115
- ♦ Chapter 6, “Caveats for Implementing OES 11 SP2 Services,” on page 117
- ♦ Chapter 7, “Upgrading to OES 11 SP2,” on page 133
- ♦ Chapter 8, “Migrating Existing Servers and Data,” on page 135
- ♦ Chapter 9, “Virtualization in OES 11 SP2,” on page 137
- ♦ Chapter 10, “Clustering and High Availability,” on page 141
- ♦ Chapter 11, “Managing OES 11 SP2,” on page 143
- ♦ Chapter 12, “Network Services,” on page 161
- ♦ Chapter 13, “Storage and File Systems,” on page 189
- ♦ Chapter 14, “eDirectory, LDAP, and Domain Services for Windows,” on page 207
- ♦ Chapter 15, “Users and Groups,” on page 217
- ♦ Chapter 16, “Access Control and Authentication,” on page 231
- ♦ Chapter 17, “Backup Services,” on page 247
- ♦ Chapter 18, “File Services,” on page 249
- ♦ Chapter 19, “Print Services,” on page 283
- ♦ Chapter 20, “Search Engine (QuickFinder),” on page 289
- ♦ Chapter 21, “Web Services,” on page 291
- ♦ Chapter 22, “Security,” on page 293
- ♦ Chapter 23, “Certificate Management,” on page 307
- ♦ Appendix A, “Adding Services to OES Servers,” on page 313
- ♦ Appendix B, “Changing an OES 11 SP2 Server’s IP Address,” on page 315
- ♦ Appendix C, “Updating/Patching OES 11 SP2 Servers,” on page 323
- ♦ Appendix D, “Quick Reference to OES User Services,” on page 325
- ♦ Appendix E, “OES 11 SP2 Browser Support,” on page 327
- ♦ Appendix F, “Client/Workstation OS Support,” on page 329
- ♦ Appendix G, “OES 11 SP2 Service Scripts,” on page 331
- ♦ Appendix H, “System User and Group Management in OES 11 SP2,” on page 335
- ♦ Appendix I, “Administrative Users in OES 11 SP2,” on page 361
- ♦ Appendix J, “Coordinating Password Policies Among Multiple File Services,” on page 363
- ♦ Appendix K, “Configuration and Log Files,” on page 371

- ♦ [Appendix L, “Small Footprint CIM Broker \(SFCB\),” on page 385](#)
- ♦ [Appendix M, “Documentation Updates,” on page 389](#)

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 11 SP2 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 11 SP2. Please use the User Comments feature at the bottom of each page of the online documentation.

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 11 SP2: Getting Started with OES 11 and Virtualized NetWare](#) is the hands-on counterpart to this guide and helps network administrators:

- ♦ Set up a basic lab with an OES 11 SP2 server, a virtualized NetWare server, a test tree, and user objects that represent the different types of users in OES 11 SP2.
- ♦ Use the exercises in the guide to explore how OES 11 SP2 services work.
- ♦ Continue exploring to gain a sound understanding of how OES 11 SP2 can benefit their organization.

Additional documentation is also found on the [OES 11 Documentation Web site \(../../oes11\)](#).

Documentation Conventions

The terms OES 11 and OES 11 SP2 are used in this guide. A support pack is mentioned to differentiate something that is new or changed in that support pack release of OES 11. All statements that refer to OES 11 also apply to the latest OES 11 support pack 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.

1 What's New or Changed

This section summarizes the new features for each release of Novell Open Enterprise Server (OES) 11.

- ♦ [Section 1.1, "What's New or Changed in OES 11 SP1 January 2014 Patches," on page 19](#)
- ♦ [Section 1.2, "What's New or Changed in OES 11 SP2," on page 19](#)
- ♦ [Section 1.3, "What's New or Changed in OES 11 SP1," on page 46](#)
- ♦ [Section 1.4, "What's New or Changed in OES 11," on page 63](#)
- ♦ [Section 1.5, "Where's NetWare?," on page 79](#)

1.1 What's New or Changed in OES 11 SP1 January 2014 Patches

- ♦ [Section 1.1.1, "Novell CIFS," on page 19](#)
- ♦ [Section 1.1.2, "NetWare Core Protocol," on page 19](#)

1.1.1 Novell CIFS

Interoperability with Partnering Vendors

Interoperability with some antivirus and Hierarchical Storage Management (HSM) partner products has been improved in OES 11 SP1.

1.1.2 NetWare Core Protocol

Interoperability with Partnering Vendors

Interoperability with some antivirus and Hierarchical Storage Management (HSM) partner products has been improved in OES 11 SP1.

1.2 What's New or Changed in OES 11 SP2

This section summarizes the new features introduced in the Novell Open Enterprise Server (OES) 11 SP2 release.

- ♦ [Section 1.2.1, "Install and Upgrade," on page 20](#)
- ♦ [Section 1.2.2, "Archive and Version Services," on page 21](#)
- ♦ [Section 1.2.3, "Novell AFP," on page 21](#)
- ♦ [Section 1.2.4, "Novell CIFS," on page 21](#)
- ♦ [Section 1.2.5, "Novell Cluster Services," on page 22](#)

- [Section 1.2.6, “Distributed File Services,” on page 27](#)
- [Section 1.2.7, “Dynamic Storage Technology,” on page 28](#)
- [Section 1.2.8, “Domain Services for Windows,” on page 28](#)
- [Section 1.2.9, “DNS and DHCP,” on page 30](#)
- [Section 1.2.10, “NetIQ eDirectory,” on page 30](#)
- [Section 1.2.11, “Novell iFolder,” on page 30](#)
- [Section 1.2.12, “Novell iPrint,” on page 30](#)
- [Section 1.2.13, “Novell FTP,” on page 31](#)
- [Section 1.2.14, “Novell Linux Volume Manager,” on page 31](#)
- [Section 1.2.15, “Linux User Management,” on page 35](#)
- [Section 1.2.16, “Migration,” on page 35](#)
- [Section 1.2.17, “NetWare Core Protocol \(NCP\),” on page 35](#)
- [Section 1.2.18, “Linux POSIX Volumes,” on page 37](#)
- [Section 1.2.19, “NetStorage,” on page 40](#)
- [Section 1.2.20, “QuickFinder,” on page 40](#)
- [Section 1.2.21, “Novell Remote Manager,” on page 40](#)
- [Section 1.2.22, “Novell Storage Services \(NSS\),” on page 42](#)
- [Section 1.2.23, “Storage Management Services,” on page 43](#)
- [Section 1.2.24, “File Systems Management \(Storage\),” on page 43](#)
- [Section 1.2.25, “NSS Auditing Client Logger \(VLOG\),” on page 44](#)
- [Section 1.2.26, “Web Services,” on page 44](#)

1.2.1 Install and Upgrade

In addition to bug fixes, the following enhancements and behavior changes are provided in OES 11 SP2:

Express Install

Beginning with OES 11 SP2, Express Install has been introduced to help you install OES 11 SP2 with minimal user intervention. For more information, see [“Typical and Custom OES Configuration”](#) in the *OES 11 SP2: Installation Guide*.

Cloning Post Install or Upgrade

Beginning with OES 11 SP2, you can clone an OES server after the installation or upgrade. For more information, see [“Cloning an OES Server Post OES Installation and Configuration”](#) in the *OES 11 SP2: Installation Guide*.

NCPFS Package Dependency Replaced with Novell Client for Linux

Beginning with OES 11 SP2, the OES dependency on the NCPFS open source package has been replaced with the Command Line Utilities for Novell Client, `novell-qtgui-cli`. The NCPFS package is no longer supported or bundled.

Reconfiguring iManager

If iManager is not configured or installed properly, you can use the reconfiguration scripts to reinstall it. For more information, see [“Re-configuring iManager”](#) in the *OES 11 SP2: Installation Guide*.

Interoperability with Partnering Vendors

Interoperability with some antivirus and Hierarchical Storage Management (HSM) partner products has been improved in OES 11 SP2.

1.2.2 Archive and Version Services

The Archive and Version Services in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3.

IMPORTANT: Beginning with OES 11 SP2, no further enhancements are planned for Archive and Version Services. For more information, see the [Notice about certain OES services](#).

1.2.3 Novell AFP

The AFP service in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. In addition to bug fixes, OES 11 SP2 provides the following enhancements and changes for AFP:

Managing AFP Services

`novafp` - A new command line utility to configure, monitor, and manage the AFP service (`afptcpd` daemon). You can also monitor and manage the AFP service using the *Manage AFP Services* menu option provided in NRM. For more information, see [“AFP Monitoring and Management”](#) in the *OES 11 SP2: Novell AFP for Linux Administration Guide*.

1.2.4 Novell CIFS

The CIFS service in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. In addition to bug fixes, OES 11 SP2 provides the following enhancements and changes for CIFS:

Changes to the CIFS Delete Mechanism

The file and folder delete functions for the NSS file system in Novell CIFS were modified to use the POSIX APIs. This change leads to generating three new Vigil NSS auditing events, namely, OPEN, MODIFY, and CLOSE when CIFS protocol is used to delete a file or folder on an NSS file system. These are generated in addition to the DELETE event.

Enhanced Open Connections and Files Monitoring

- ♦ The CIFS service now provides the capability to monitor open files and CIFS connections.

You can monitor the CIFS service using the newly added command line options in the `novcifs` utility or the *Manage CIFS Services* option in NRM. For more information, see “[CIFS Monitoring and Management](#)” in the [OES 11 SP2: Novell CIFS for Linux Administration Guide](#).

- ♦ The `novcifs` long option for active connection count has been changed in OES11 SP2 from `-c | --conn-count` to `-C | --Conn`.

CLI Commands to View the NetBIOS Name of Servers and Change the Behavior of Exporting Volumes by Default

With the new command options introduced in `novcifs`, administrators can choose to export all mounted volumes as shares or export only the required volumes as shares.

```
novcifs --list-servers
```

Displays the NetBIOS name of physical and virtual CIFS servers.

```
novcifs --share-vols-default=SERVER_NAME --value=yes|no
```

Enables or disables all volumes being exported as shares by default.

For more information, see “Viewing the NetBIOS Names of Servers and Changing the Behavior of Exporting Volumes by Default” under `novcifs(8)` in the [OES 11 SP2: Novell CIFS for Linux Administration Guide](#).

Pass-through Information Levels Capability

The Novell CIFS server now implements the pass-through information levels capability. This is a configurable option and is turned off by default. It can be enabled or disabled using the `novcifs --info-level-passthru=yes|no` command.

Pass-through Information Levels are used to set or to query file or folder information on the server. These Information Levels allow SMB clients to directly query Information Levels that are native to the underlying object store or file system.

User-level quota is not supported if this option is disabled.

For more information, see “Enabling or Disabling the Pass-through Information Levels Capability” under `novcifs(8)` in the [OES 11 SP2: Novell CIFS for Linux Administration Guide](#).

Support for DOS Names

The CIFS Service now supports file operations using the short file name format to accommodate applications that require file names to be in the 8.3 name format, for example, `ABPXPS~1.PPT`.

1.2.5 Novell Cluster Services

Novell Cluster Services 2.2 supports OES 11 SP2 services and file systems running on 64-bit SUSE Linux Enterprise Server (SLES) 11 Service Pack (SP) 3. In addition to bug fixes, Novell Cluster Services provides the following enhancements and behavior changes in the OES 11 SP2 release.

Changing the Nodes or Failover Order in the Preferred Nodes List

When you change the nodes or failover order in a resource's *Preferred Nodes* list, the change takes effect immediately when you click *OK* or *Apply* if the resource is running. Otherwise, it takes effect the next time the resource is brought online. Previously, the change did not occur until the cluster resource was taken offline and brought online. See “[Configuring Preferred Nodes and Failover Order for a Resource](http://www.novell.com/documentation/oes11/clus_admin_lx/data/hm13qb8q.html)” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/hm13qb8q.html) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

With this new capability, changes for any resource attributes (such as the resource mode settings, preferred nodes list, and RME groups) other than the scripts take effect immediately.

Availability for prior releases: April 2013 Scheduled Maintenance for OES 11 SP1

Applying Updated Scripts for a Resource

When you modify the load, unload, and monitor scripts for a resource and click *Apply* or *OK*, the updated resource scripts can take effect in any of the following ways:

- When an administrator takes the resource offline and then brings it online.
- When the resource fails over to another node, if both the source and destination nodes have received the updated scripts from eDirectory.
- When an administrator uses the `cluster migrate` command to load the resource on another node, if both the source and destination nodes have received the updated scripts from eDirectory.

Previously, script changes did not take effect until the resource was taken offline and then brought online.

For more information, see “[Applying Updated Resource Scripts by Offline/Online, Failover, or Migration](http://www.novell.com/documentation/oes11/clus_admin_lx/data/apply_updated_scripts.html)” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/apply_updated_scripts.html) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Availability for prior releases: April 2013 Scheduled Maintenance for OES 11 SP1

Modifying Resource Scripts Outside of iManager

You can use the `/opt/novell/ncs/bin/ncs_resource_scripts.pl` script to modify resource scripts without using iManager. You can add, remove, or modify the commands in the script, or retrieve its scripts to search for information from the script. You can issue the command from the command line or in a script. This capability is very useful when you need to make the same script change to multiple resources in a cluster. See “[ncs_resource_scripts.pl \(Modifying Resource Scripts Outside of iManager\)](http://www.novell.com/documentation/oes11/clus_admin_lx/data/ncs_resource_scripts.html)” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/ncs_resource_scripts.html) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Monitoring the Status of the eDirectory Daemon (ndsd)

Some clustered services rely on the eDirectory daemon (`ndsd`) to be running and available in order to function properly. In this release, NCS provides the ability to monitor the status of the eDirectory daemon (`ndsd`) at the NCS level. It is disabled by default. The monitor can be set independently on each node. On a node, if the eDirectory daemon does not respond to a status request within a specified timeout period, NCS can take one of three configurable remedy actions: an `ndsd` restart, a

graceful node restart, or a hard node restart. See “Configuring NCS to Monitor the eDirectory Daemon” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/ncs_monitor_ndsd.html) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Reporting Logged Events for a Specific Time Range

You can get a report of logged events that occurred during a specified time range. The time range filter displays events that occurred during the interval of time before a specified date/time and after a specified date/time. The search includes the specified before and after values. For example, you might want to see events that occurred for a cluster resource before the date/time that a failover event was triggered and after the date/time of its previously known good state. See “Viewing Events in the Cluster Event Log” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/event_log.html) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

DotOutParser Utility

The DotOutParser utility (`/opt/novell/ncs/bin/dotoutparser.pl`) prints summaries of failed or incomplete events that have been recorded in a specified `/var/opt/novell/log/ncs/<resource_name>.<script>.out` log file. It also prints output (if any) from any commands that failed or got stuck. You can include ignored errors if desired. Line numbers allow you to easily refer the summary output to the source lines in the `*.out` file. You can omit the line numbers if desired. See “DotOutParser Utility” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/dotoutparser.html) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Ability to Manage a Cluster in Case of a Faulty Master IP Address

The *Clusters > My Clusters* page in iManager provides the ability to manage the cluster with the IP address of a specified node (preferably the master node) if the master IP address for the Cluster object is experiencing problems. For example, a CIMOM error in iManager can prevent you from connecting to the master IP address, or an IP address conflict can prevent the Master IP Address Resource from coming online. See “Viewing or Modifying the Cluster Master IP Address or Port” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/clus_ip_port.html) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Support for VLAN on NIC Bonding

Novell Cluster Services added support for VLAN on NIC bonding. No modifications to scripts are required. You can use `ethx` or `vlanx` interfaces in any combination for nodes in a cluster.

Availability for prior releases: September 2013 Scheduled Maintenance for OES 11 SP1

Updates for the DHCP_Template

In the DHCP_Template for DHCP cluster resources, the PID file location was changed to `/var/lib/dhcp/var/run/dhcpd.pid`. This is the location used by DHCP since OES 11 SP1. The change applies automatically to any newly created DHCP cluster resources.

The following line in the load script for the DHCP_Template was modified to use the `$MOUNT_POINT` variable that is defined at the beginning of the script:


```
exit_on_error /opt/novell/dhcp/bin/cluster_dhcpd.sh -m $MOUNT_POINT
```

For information about configuring DHCP cluster resources, see “Configuring DHCP with Novell Cluster Services for the Linux File System” in the *OES 11 SP2: Novell DNS/DHCP Services for Linux Administration Guide*.

Availability for prior releases: The PID path change is available in the May 2013 Scheduled Maintenance for OES 11 SP1.

SLP Refresh Interval for Cluster Resource Virtual NCP Servers

NCP Server was modified to refresh its OpenSLP registration of cluster resource virtual NCP servers, based on the setting for the eDirectory advertise-life-time (`n4u.nds.advertise-life-time`) parameter. The `n4u.nds.advertise-life-time` parameter is set by default to 3600 seconds (1 hour) and has a valid range of 1 to 65535 seconds. Previously, NCP Server re-registered the virtual NCP servers with SLP every 30 minutes regardless of the eDirectory advertise-life-time setting. For information about setting the eDirectory advertise-life-time parameter in a cluster, see “SLP” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/ncs_swreqs.html#slp) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Availability for prior releases: May 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

Enforcing Name Restrictions for NCP-Enabled LVM Volumes

For NCP-enabled LVM volumes, the NSSMU utility and `nlvm create linux volume` command have been modified to enforce the NCP length restriction of 14 characters, and to use uppercase letters for the name in the Novell Cluster Services cluster resource scripts for a shared LVM volume. Previously, a new LVM volume cluster resource would go comatose immediately after creation if the name specified with the `NCP_VOLUME` parameter in the script was more than 14 characters or if it included lowercase letters. See “Creating an LVM Volume Group Cluster Resource with NSSMU” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bxv3rde.html#bxv32co) and “Creating an LVM Volume Group Cluster Resource with NLVM Commands” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bxv3rde.html#b11dtkag) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Availability for prior releases: November 2012 Scheduled Maintenance for OES 11 SP1

Unsharing a Device without Stopping NCS

NSS management tools have been modified so that it is not necessary to stop NCS from running in order to disable the *Shareable for Clustering* setting for a device. The device should not contribute space to an SBD partition or to a shared pool or a cluster-enabled pool that is used in any cluster resource. This change is consistent with how unsharing a device works on OES 2 SP3 and earlier. See “Stopping Novell Cluster Services” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bscysdd.html) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Availability for prior releases: September 2013 Scheduled Maintenance for OES 11 SP1

Linux Multipath I/O Changes in SLES 11 SP3

The Linux Device Mapper - Multipath software deprecated some attributes and modified some default settings for attributes in the `/etc/multipath.conf` file in SUSE Linux Enterprise Server 11 SP3. After upgrading to SLES 11 SP3, the `multipathd` daemon might not work with your existing multipath configuration file. Ensure that you verify your `/etc/multipath.conf` file before you start the `multipathd` daemon after an upgrade to OES 11 SP2. For information about the latest attributes and default settings, see the `multipath.conf(5)` man page after you install or upgrade the server.

Key changes to the `/etc/multipath.conf` file:

- ♦ **udev_dir**

The `udev_dir` attribute is deprecated. After you upgrade to SLES 11 SP3, you must remove or comment out the following line from the `defaults` section of your `/etc/multipath.conf` file:

```
udev_dir /dev
```

- ♦ **getuid_callout**

In the `defaults` section of the `/etc/multipath.conf` file, the `getuid_callout` attribute is deprecated and replaced by the `uid_attribute` attribute. This is a `udev` attribute that provides a unique path identifier. The default value is `ID_SERIAL`.

After you upgrade to SLES 11 SP3, modify the attributes in the `defaults` section of your `/etc/multipath.conf` file as follows:

- ♦ Remove or comment out the following line from the `defaults` section:

```
getuid_callout "/lib/udev/scsi_id --whitelisted --device=/dev/%n"
```

- ♦ Add the following line to the `defaults` section:

```
uid_attribute "ID_SERIAL"
```

- ♦ **path_selector**

In the `defaults` section of the `/etc/multipath.conf` file, the default value for the `path_selector` attribute was changed from `"round-robin 0"` to `"service-time 0"`. The `service-time` option chooses the path for the next bunch of I/O based on the amount of outstanding I/O to the path and its relative throughput.

After you upgrade to SLES 11 SP3, you can modify the attribute value in the `defaults` section of your `/etc/multipath.conf` file to use the recommended default:

```
path_selector "service-time 0"
```

- ♦ **user_friendly_names**

The `user_friendly_names` attribute can be configured in the `devices` section and in the `multipaths` section.

- ♦ **max_fds**

The default setting for the `max_fds` attribute was changed to `max`. This allows the multipath daemon to open as many file descriptors as the system allows when it is monitoring paths.

After you upgrade to SLES 11 SP3, you can modify the attribute value in your `/etc/multipath.conf` file:

```
max_fds "max"
```

These key changes are shown in the following `defaults` section for the `/etc/multipath.conf` file. This example comments out the old settings and adds the new or revised settings:

```

defaults {
    verbosity                2
    # udev_dir is deprecated in SLES 11 SP3
    # udev_dir                /dev
    polling_interval         10
    # path_selector default value is service-time in SLES 11 SP3
    # path_selector           "round-robin 0"
    path_selector            "service-time 0"
    path_grouping_policy     "failover"
    # getuid_callout is deprecated in SLES 11 SP3 and replaced with uid_attribute
    # getuid_callout          "/lib/udev/scsi_id --whitelisted --device=/dev/%n"
    # uid_attribute is new in SLES 11 SP3
    uid_attribute            "ID_SERIAL"
    prio                     "const"
    prio_args                ""
    features                 "0"
    path_checker              "directio"
    alias_prefix              "mpath"
    # rr_min_io was deprecated in SLES 11 SP2
    # rr_min_io               100
    # rr_min_io_rq is new in SLES 11 SP2
    rr_min_io_rq             1
    # max_fds default is max in SLES 11 SP3
    # max_fds                 8124
    max_fds                  "max"
    rr_weight                 "uniform"
    queue_without_daemon     "yes"
    flush_on_last_del        "no"
    user_friendly_names      "no"
    fast_io_fail_tmo         5
    bindings_file             "/etc/multipath/bindings"
    wwids_file                "/etc/multipath/wwids"
    log_checker_err           "always"
    retain_attached_hw_handler "no"
    detect_prio               "no"
    failback                  "manual"
    no_path_retry             "fail"
}

```

For information about the requirements, configuration, and management of multipath I/O, see “Managing Multipath I/O for Devices” (http://www.suse.com/documentation/sles11/stor_admin/data/multipathing.html) in the *SUSE Linux Enterprise Server 11 SP3 Storage Administration Guide* (http://www.suse.com/documentation/sles11/stor_admin/data/bookinfo.html).

1.2.6 Distributed File Services

Novell Distributed File Services in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. In addition to bug fixes, OES 11 SP2 provides the following enhancements and changes for DFS:

Setting the [Public] Trustee for a Distributed File Services Junction in iManager

The Distributed File Services plug-in for iManager was modified to allow the [Public] trustee to be selected as a trustee of a junction. For information about setting trustees on DFS junctions, see [Adding or Deleting Trustees for the Junction](#) in the *OES 11 SP2: Novell Distributed File Services Administration Guide for Linux*.

1.2.7 Dynamic Storage Technology

Dynamic Storage Technology supports OES 11 SP2 file systems running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. In addition to bug fixes, the following enhancements are available:

- ♦ **Directory and User Space Quotas Management for DST Volumes:** DST provides a unified quota management system that allows you to manage your disk space usage policy for DST shadow volume pairs. The `ncpcon quotas` command allows you add, modify, or delete directory quotas or user space quotas on the primary volume, and then easily set related quotas on the secondary volume based on those settings. The NSS file system independently enforces the quotas set on each volume.

Previously, a unified quotas management approach across both volumes was not available for DST shadow volume pairs. See “[Managing Directory and User Space Quotas on DST Volumes](http://www.novell.com/documentation/oes11/stor_dst_lx/data/dst_quotas_sync.html)” (http://www.novell.com/documentation/oes11/stor_dst_lx/data/dst_quotas_sync.html) in the *OES 11 SP2: Dynamic Storage Technology Administration Guide* (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bookinfo.html).

- ♦ **ShadowFS:** The *Load ShadowFS (enable only if using Samba)* label has been modified to *Load ShadowFS (Enable only to give LUM-enabled users merged-view access via Samba or Linux file access protocols)*. The change was made for clarity; there is no change in functionality.

Availability for prior releases: May 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

1.2.8 Domain Services for Windows

Domain Services for Windows in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3.

IMPORTANT: To use the DSfW features introduced in the OES 11 SP2 release, you must upgrade all domain controllers in the DSfW domain to OES 11 SP2.

In addition to bug fixes, Domain Services for Windows provides the following enhancements in the OES 11 SP2 release:

Configuring DSfW Server as a WINS Server

Duplicate workstation names in a domain lead to several issues such as slow user logins. Configuring a DSfW server as a WINS server helps to prevent having two workstations with the same name in a domain. For more information, see “[Configuring DSfW Server as a WINS Server](#)” in the *OES 11 SP2: Domain Services for Windows Administration Guide*.

Sites and Subnets

The sites and subnets feature enables you to configure multiple sites and distribute domain controllers over different geographical locations. When a client tries to log in to a domain, the request goes to the nearest available domain controller, thus ensuring faster domain login. For more information, see “[Configuring Sites and Subnets](#)” in the *OES 11 SP2: Domain Services for Windows Administration Guide*.

Mac Client Support

Beginning with OES 11 SP2, DSfW supports the OS X 10.8 and OS X 10.9 clients. This support enables you to join a Mac client to a DSfW domain, log in to the domain using DSfW credentials, and access NSS shares. For more information, see [“Using Mac Client”](#) in the [OES 11 SP2: Domain Services for Windows Administration Guide](#).

SASL NTLMSSP Bind Support

DSfW now includes NTLM support for LDAP authentication. If Kerberos is down or a legacy third-party application is limited only to NTLM authentication, the NTLM support for LDAP authentication goes into effect. This NTLMSSP support is layered over the SASL GSS-SPNEGO mechanism. For more information, see [“Support for SASL NTLMSSP Bind in LDAP”](#) in the [OES 11 SP2: Domain Services for Windows Administration Guide](#).

Novell Client Support

DSfW now enables co-existence of Novell Client with DSfW. Users can now authenticate to a DSfW server using Novell Client. You can now join a workstation pre-installed with Novell Client to a DSfW domain without affecting the DSfW communication.

With Novell Client support, Windows operations such as domain login, password change, GPO policy, content redirection, roaming profile, folder redirection, and advanced login parameters will work.

This feature also enables you to leverage Novell Client features such as login scripts, LDAP contextless login, login with profile, and automated login. For more information about Novell Client features, see the [Novell Client 2 SP3 for Windows Administration Guide](#).

Windows 8 Client Support

Beginning with OES 11 SP2, DSfW supports Windows 8 as a client workstation.

Windows 2012 Support

Beginning with OES 11 SP2, DSfW supports Windows 2012 as a member server.

DSfW Install

DSfW install has been modified to not install NSS by default. This is to ensure that the DSfW server is used only as a domain controller with no other services installed by default. Novell recommends that you not install other services such as file, print, or iManager on the same server as DSfW.

Script to Address NTP-Signed Requests

NTP-signed requests from Windows clients can now be addressed by using the `cross_partition_ntp_setup.pl` script. Execute this script only if `/var/lib/` or `/var/opt/` directory hierarchies are in different partitions. For more information, see [“DSfW Fails to Set Up Signed NTP for Clients to Trust”](#) in the [OES 11 SP2: Domain Services for Windows Administration Guide](#).

1.2.9 DNS and DHCP

The DNS and DHCP services in OES 11 SP2 have been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. In addition to bug fixes, DNS and DHCP services provide the following enhancements and behavior changes in the OES 11 SP2 release:

Updates for the DHCP_Template

In the DHCP_Template for DHCP cluster resources, the PID file location was changed to `/var/lib/dhcp/var/run/dhcpd.pid`. This is the location used by DHCP since OES 11 SP1. The change applies automatically to any newly created DHCP cluster resources.

The following line in the load script for the DHCP_Template was modified to use the `$MOUNT_POINT` variable that is defined at the beginning of the script:

```
exit_on_error /opt/novell/dhcp/bin/cluster_dhcpd.sh -m $MOUNT_POINT
```

For information about configuring DHCP cluster resources, see [“Configuring DHCP with Novell Cluster Services for the Linux File System”](#) in the [OES 11 SP2: Novell DNS/DHCP Services for Linux Administration Guide](#).

Deleting Dynamic Leases

Java Console now enables you to delete dynamic leases. For more information, see ["Deleting Dynamic Leases"](#) in the [OES 11 SP2: Novell DNS/DHCP Services for Linux Administration Guide](#)

The DHCP Server Maintenance Utility Command

The DHCP server maintenance utility command now offers the `-es` option. For more information, see [“DHCP Server Maintenance Utility”](#) in the [OES 11 SP2: Novell DNS/DHCP Services for Linux Administration Guide](#).

1.2.10 NetIQ eDirectory

In OES 11 SP2, eDirectory 8.8.8 is included with IPv4 support only. For more information about eDirectory, see the [eDirectory Documentation web site](#).

Novell eDirectory has been rebranded to NetIQ eDirectory beginning with eDirectory 8.8.8. The eDirectory entitlement to OES customers remains the same as before.

1.2.11 Novell iFolder

Novell iFolder in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. There are no other changes in the OES 11 SP2 release of Novell iFolder.

1.2.12 Novell iPrint

Novell iPrint supports OES 11 SP2 services and file systems running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. iPrint provides the following enhancements and behavior changes in the OES 11 SP2 release:

iPrint Windows Client

The iPrint Client has been upgraded to version 5.94 and is available for Windows XP/Vista/Win 7/Win 8. You can download iPrint Client 5.94 from the OES 11 SP2 welcome page or from the iPrint Printer List web page. You can download the latest version of the iPrint Client from the [iPrint Client for Windows XP/Vista/Win 7/Win 8 download site](#).

iPrint Macintosh Client

A new version of the iPrint Client for Macintosh 5.74 is available for Mac OS X 10.7 and later. The 5.74 client includes support for Mac OS X 10.9 (Mavericks).

Direct Print Accounting for iPrint Macintosh Client

You can now perform accounting operations for iPrint Direct Printers on the iPrint Mac Client 5.74.

1.2.13 Novell FTP

Novell FTP in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. There are no other changes in the OES 11 SP2 release of Novell FTP.

1.2.14 Novell Linux Volume Manager

Novell Linux Volume Manager (NLVM) supports OES 11 SP2 file systems running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. For information about NLVM commands and usage, see the [OES 11 SP2: NLVM Reference \(http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/bookinfo.html\)](http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/bookinfo.html).

In addition to bug fixes, the following changes and enhancements were made to NLVM in the OES 11 SP2 release:

General

- ♦ **Novell Type Partitions:** NetWare type partitions are now referred to as Novell type partitions in guides, help, and error messages.
- ♦ **NLVM options:** The following enhancements were made to [NLVM Options \(http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/nlvmopt.html\)](http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/nlvmopt.html):
 - ♦ NLVM options can appear in any order in the command after `nlvm`. Previously, the NLVM options had to follow immediately after `nlvm`.
 - ♦ The `--terse` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/nlvmopt.html#nlvmopt_terse) option can be used with `nlvm list` commands to display the output in a format for parsing. Values are labeled in the format `ParameterName=value`. Information about a storage object is output in a single line. If the target object contains storage objects (such as partitions on a device or segments in a software RAID), subsequent lines contain information about each of its member objects.
- ♦ **Common options:** The common options `more` and `all` were added for use with the following `nlvm list` commands to provide additional details beyond the standard output. You can use them with or without the `--terse` NLVM option.


```
nlvm [-t] list devices [exclude] [more|all]
nlvm [-t] list linux volumes [more|all]
nlvm [-t] list moves [more|all]
nlvm [-t] list partitions [device] [mask] [more|all]
nlvm [-t] list pools [exclude] [more|all]
nlvm [-t] list snaps [more|all]
nlvm [-t] list volumes [more|all]
```

See “Common Options” (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/nlvm_common_options.html).

- ♦ **Viewing Error Code Messages:** The NSS utility now provides an `/err` switch that can be used from the command prompt. You can use this option to view an error message if a failed NLVM command line operation provides an error code without a corresponding message.

```
nss /err=<error_code_number>
```

For information about error codes, see “NLVM Error Codes” (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/nlvm_ec.html).

Availability for prior releases: November 2012 Scheduled Maintenance for OES 11 SP1

Devices

- ♦ **Unsharing a device:** The `nlvm unshare <device_name>` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/unshare.html) command allows you to disable the Shareable for Clustering state for a device without stopping Novell Cluster Services on the node. The command fails if the device contributes space to an SBD partition, or to a shared pool or a cluster-enabled pool that is used in any cluster resource. Previously, it was necessary to temporarily stop Novell Cluster Services in order to unshare a device after you disabled clustering for a pool.

Partitions

- ♦ **Creating a partition:** The `type=<partition_type>` option in the `nlvm create partition` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/create_part.html) command added support for partition type 1ac for snap partitions.

Linux Volumes

- ♦ **Creating a Linux volume:** The following enhancements and changes were made to the `nlvm create linux volume` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/create_lxvol.html) command:
 - ♦ **Devices option:** The `device=<device_name>` option was modified to allow you to alternatively specify a shared device with no data partitions or an uninitialized device for a clustered LVM volume. Previously, you could specify only an unshared initialized device.
 - ♦ **Partition option:** The `part=<partition_name>` option allows you to specify an existing partition as the location for a non-clustered Linux volume. It can be used instead of the `device` and `size` options.
 - ♦ **Size:** The minimum size for a Linux volume was increased from 1 MB to 8 MB. This change is consistent with the minimum size allowed in NSSMU.
 - ♦ **NCP volume ID for clustered LVM volumes:** The `valid=<ncp_volume_id>` option can be used in combination with the `shared` and `ncp` options to specify an NCP volume ID for an NCP-enabled clustered LVM volume. If the `valid` option is not used, an ID is automatically assigned by Novell Cluster Services when the resource is created. This allows you to assign an NCP volume ID that is unique across all nodes in a cluster, and across all nodes in every peer cluster in a Business Continuity Cluster.

- ♦ **Enforcing name restrictions for NCP-enabled LVM volumes:** For NCP-enabled LVM volumes, the `nlvm create linux volume` command has been modified to enforce the NCP length restriction of 14 characters, and to use uppercase letters for the name in the Novell Cluster Services cluster resource scripts for a cluster-enabled LVM volume. Previously, a new LVM volume cluster resource would go comatose immediately after creation if the name specified with the `NCP_VOLUME` parameter in the script was more than 14 characters, or if it included lowercase letters.

Availability for prior releases: November 2012 Scheduled Maintenance for OES 11 SP1

- ♦ **Linux POSIX Volumes Are Not Supported on NSS Software RAID:** Linux POSIX file systems should not be created on NSS software RAID. NLVM commands have been modified to block NSS software RAID from being used as a device when you create a Linux POSIX volume.

Availability for prior releases: September 2012 Scheduled Maintenance for OES 11 and OES 11 SP1

- ♦ **Listing details for a Linux volume:** The `nlvm list linux volume <lx_volume_name>` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/list_lxvol.html) command displays detailed information for a specified Linux volume.
- ♦ **Mounting a Linux volume:** The `nlvm linux mount <lx_volume_name>` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/linux_mount.html) command allows you to mount non-LVM and LVM volumes in Linux using the mount parameters stored in the `/etc/fstab` file. You can optionally specify the mount options. If the Linux volume is NCP-enabled, it also automatically mounts the volume for NCP, and NCP assigns it a volume ID.
- ♦ **Unmounting a Linux volume:** The `nlvm linux unmount <lx_volume_name>` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/linux_unmount.html) command allows you to unmount non-LVM and LVM volumes in Linux. If the Linux volume is NCP-enabled, it also automatically dismounts the volume for NCP before it dismounts it in Linux.

NSS Pools and Volumes

- ♦ **Creating a volume:** The `valid=<nep_volume_id>` option in the `nlvm create volume` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/create_vol.html) command can be used in combination with a clustered NSS pool to assign an NCP volume ID for a clustered NSS volume. If the `valid` option is not used, an ID is automatically assigned by Novell Cluster Services when the resource is created. This allows you to assign an NCP volume ID that is unique across all nodes in a cluster, and across all nodes in every peer cluster in a Business Continuity Cluster.
- ♦ **Listing attributes for an NSS volume:** The `nlvm list volumes` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/list_vols.html) command displays attribute information for NSS volumes when you use the `more` or `all` option.
- ♦ **Logging NCP and NSS volume dismounts:** NCP Server has been modified to automatically log dismounts of NSS volumes and NCP volumes.

Availability for prior releases: January 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

- ♦ **Pausing a pool move:** The `nlvm move` command uses NSS software RAID mirroring underneath to copy the data to the target location. If server performance is too slow during a move, you can temporarily pause the mirroring with the `nlvm pause move` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/pause_move.html) command. While the move is paused, the pool move status is reported as `Not Enabled`.
- ♦ **Resuming a pool move:** If you have paused a pool move, you can resume the mirroring with the `nlvm resume move` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/resume_move.html) command. The pool move continues from where it was paused.

- ♦ **Unmounting a pool:** The `nlvm unmount <poolname>` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/unmount.html) command has been modified to additionally remove the Device Mapper object for the pool, the link to the Device Mapper object, and the mount point for the pool. This allows you to gracefully log out of the server from an iSCSI device that contains a pool.

See “Logging Out of an iSCSI Device that Contains an NSS Pool” (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/b13pzlj1.html).

Availability for prior releases: January 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

NSS Pool Snapshots

- ♦ **Creating a snapshot:** The following enhancement and change were made for the `nlvm create snap` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/create_snap.html) command:
 - ♦ **Partition option:** The `part=<snap_partition>` option allows you to specify an existing snap partition as the target location for an NSS pool snapshot. It can be used instead of the `device` and `size` options.
 - ♦ **Size:** The minimum snapshot size was increased from 1 MB to 50 MB. This change is consistent with the minimum size allowed in NSSMU.

NSS Software RAIDs

- ♦ **Creating an NSS software RAID:** The following enhancements and changes were made to the `nlvm create raid` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/create RAID.html) command:
 - ♦ **Mirroring an Existing Partition:** The following options have been modified:
 - ♦ **Name option:** The `name` option is mandatory except when you mirror an existing SBD partition. If you specify a name (which should be the cluster name), the RAID1 is given that name. If the name is not specified, the RAID1 name defaults to the SBD partition’s name.
 - ♦ **Type option:** The `type` option is optional when you mirror an existing NSS or SBD partition. It uses the type of the existing partition.

Availability for prior releases: November 2012 Scheduled Maintenance for OES 11 and OES 11 SP1

- ♦ **Mirroring MSDOS Devices:** The command has been modified to transparently accommodate the metadata size differences required by GPT and MSDOS partitioned devices. When mirroring a pool that consumes an entire MSDOS partitioned disk, you can use an MSDOS or GPT partitioned device of the same size. Previously, the GPT device had to be at least 4 MB larger than the MSDOS partitioned device.

Availability for prior releases: November 2012 Scheduled Maintenance for OES 11 and OES 11 SP1

- ♦ **Renaming an NSS software RAID:** The `nlvm rename raid` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/rename RAID.html) command is new. Use this command to rename a specified NSS software RAID device.

Availability for prior releases: September 2012 Scheduled Maintenance for OES 11 and OES 11 SP1

1.2.15 Linux User Management

Linux User Management in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. In addition to bug fixes, Linux User Management provides the following enhancement and behavior change in the OES 11 SP2 release:

Changes to the LUM Configuration

The LUM configuration now includes two new parameters: `dont-deny-pamservice` and `non-posix-members`. For more information, see [“Editing the `nam.conf` File”](#) in the *OES 11 SP2: Novell Linux User Management Administration Guide*.

Adding External LDAP Servers

LUM now enables you to add external LDAP servers during LUM configuration. For more information, see [“Setting Up Linux Computers to Use eDirectory Authentication”](#) in the *OES 11 SP2: Novell Linux User Management Administration Guide*.

1.2.16 Migration

The Migration Tool in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. In addition to bug fixes, the Migration Tool provides the following enhancements and behavior changes in the OES 11 SP2 release.

Enhanced View of Migration Progress

The progress of the file system migration and sync now captures the total number of files and folders, and the size of the data to be migrated, along with migration start and end time. It also displays the total number of errors encountered during migration or sync, along with a link to view the logs.

For more information, see [“Service Information”](#) in the *OES 11 SP2: Migration Tool Administration Guide*.

Enhanced View of Migration Logs

The logs of all services are displayed in a single Migration Log window. You can select a service and use the search functionality to filter logs for specific types of error messages and keywords.

For more information, see [“View Logs”](#) in the *OES 11 SP2: Migration Tool Administration Guide*.

1.2.17 NetWare Core Protocol (NCP)

NCP in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. In addition to bug fixes, OES 11 SP2 provides the following enhancements and changes for NCP:

Changes to the NCP Delete Mechanism

The file and folder delete functions for the NSS file system in NCP were modified to use the POSIX APIs. This change leads to generating three new Vigil NSS auditing events, namely, OPEN, MODIFY, and CLOSE when NCP is used to delete a file or folder on an NSS file system. These are generated in addition to the DELETE event.

Path Visibility is Updated Immediately When a Folder or File is Deleted

NCP Server has been modified to immediately update the path visibility when a folder or file is deleted, if the logged in or mapped user had trustee rights assigned on it. The deleted file or folder and its parent path are no longer displayed unless the user has rights set at a higher level in the directory tree. In previous releases, the parent path remains visible until the NCP Server is restarted.

Command Options to Clear All NCP Server Connections

Two new command options have been added to manage NCP server connections: `connections clearALL` and `connections clearALL except <connection_number>`. These parameters help the NCP server clear all user connections that are open. You can optionally specify connection numbers that you do not want to close in the exception list. NCP server exempts those connections from closing. Specify multiple connection numbers by separating them with commas. For more information, see [“Managing NCP Server Connections”](#) in the [OES 11 SP2: NCP Server for Linux Administration Guide](#).

Command Options to Update UID Number for non-LUM Users

`UID_UPDATE_ENABLED`

Controls the maintenance thread to update UIDs.

`UID_UPDATE_PERIOD`

Sets the frequency in hours. This option is applicable only if `UID_UPDATE_ENABLED` is set to 1.

For more information, see [“Enabling or Disabling UID Updates”](#) in the [OES 11 SP2: NCP Server for Linux Administration Guide](#).

NOTE: These command options are also available in OES 2 SP3 (April 2013 Patches) and OES 11 SP1 (April 2013 Patches).

NCPCON's Whitespace Support in File Path and Trustee Names

The `ncpcon` utility allows spaces in file path or trustee names. If the file path or trustee names contain spaces, enclose them within double or single quotes. This change affects the following commands:

`rights, irm, files, create shadow_volume, remove shadow_volume, and shift.`

For more information, see [“Commands and Utilities for NCP Server and NCP Volumes”](#) in the [OES 11 SP2: NCP Server for Linux Administration Guide](#).

Auditing Closed User Connections and Deleted eDirectory User Entries

NCP audits the graceful and forced termination of user connections, and deleted eDirectory user entries for connections. For more information, see [“Auditing Closed User Connections and Deleted eDirectory User Entries”](#) in the [OES 11 SP2: NCP Server for Linux Administration Guide](#).

1.2.18 Linux POSIX Volumes

The NLVM and NSSMU management tools support Linux POSIX volumes on OES 11 SP2 running on 64-bit SUSE Linux Enterprise Server (SLES) 11 Service Pack (SP) 3.

NSSMU

In addition to bug fixes, the following changes and enhancements were made in NSSMU for Linux POSIX volume management in the OES 11 SP2 release.

General

- ♦ **Novell Type Partitions:** NetWare type partitions are now referred to as Novell type partitions in guides, help, and error messages.

Devices

- ♦ **Unsharing a device:** The NSSMU Devices page allows you to disable the *Shareable for Clustering* state for a device without stopping Novell Cluster Services on the node. The command fails if the device contributes space to an SBD partition, or to a shared pool or a cluster-enabled pool that is used in any cluster resource. Previously, it was necessary to temporarily stop Novell Cluster Services in order to unshare a device after you disabled clustering for a pool.

Linux Volumes

- ♦ **Creating Linux Volumes:**
 - ♦ **Devices:** The device selection was modified to allow you to alternatively select a shared device with no data partitions or an uninitialized device for a clustered LVM volume. Previously, only unshared initialized devices were available for selection.
 - ♦ **Enforcing Name Restrictions for NCP Enabled LVM Volumes:** For NCP-enabled LVM volumes, the NSSMU utility has been modified to enforce the NCP length restriction of 14 characters and to use uppercase letters for the name in the Novell Cluster Services cluster resource scripts for a cluster-enabled LVM volume. Previously, a new LVM volume cluster resource would go comatose immediately after creation if the name specified with the NCP_VOLUME parameter in the script was more than 14 characters, or if it included lowercase letters.
Availability for prior releases: November 2012 Scheduled Maintenance for OES 11 SP1
- ♦ **Linux POSIX Volumes Are Not Supported on NSS Software RAIDs:** Linux POSIX file systems should not be created on NSS software RAIDs. NSSMU has been modified to block NSS software RAIDs from being presented as device options when you create a Linux POSIX volume.
Availability for prior releases: September 2012 Scheduled Maintenance for OES 11 and OES 11 SP1
- ♦ **Mounting a Linux volume:** The NSSMU *Linux Volumes* menu option F7 allows you to mount non-LVM and LVM volumes in Linux using the mount parameters stored in the `/etc/fstab` file. You can optionally specify the mount options. If the Linux volume is NCP-enabled, it also automatically mounts the volume for NCP, and NCP assigns it a volume ID.
- ♦ **Unmounting a Linux volume:** The NSSMU *Linux Volumes* menu option F7 allows you to unmount non-LVM and LVM volumes in Linux. If the Linux volume is NCP-enabled, it also automatically dismounts the volume for NCP before it dismounts it in Linux.
- ♦ **Logging NCP volume dismounts:** NCP Server has been modified to automatically log dismounts of NCP-enabled volumes, including NSS volumes and NCP-enabled Linux volumes.

Availability for prior releases: January 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

NLVM Commands

In addition to bug fixes, the following changes and enhancements were made in NLVM commands for Linux POSIX volume management in the OES 11 SP2 release. For information about NLVM commands and usage, see the *OES 11 SP2: NLVM Reference* (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/bookinfo.html).

General

- ♦ **Novell Type Partitions:** NetWare type partitions are now referred to as Novell type partitions in guides, help, and error messages.
- ♦ **NLVM options:** The following enhancements were made to [NLVM Options](http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/nlvmopt.html) (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/nlvmopt.html):
 - ♦ NLVM options can appear in any order in the command after `nlvm`. Previously, the NLVM options had to follow immediately after `nlvm`.
 - ♦ The `--terse` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/nlvmopt.html#nlvmopt_terse) option can be used with `nlvm list` commands to display the output in a format for parsing. Values are labeled in the format `ParameterName=value`. Information about a storage object is output in a single line. If the target object contains storage objects (such as partitions on a device or segments in a software RAID), subsequent lines contain information about each of its member objects.
- ♦ **Common options:** The common options `more` and `all` were added for use with the following `nlvm list` commands to provide additional details beyond the standard output. You can use them with or without the `--terse` NLVM option.

```
nlvm [-t] list devices [exclude] [more|all]
nlvm [-t] list linux volumes [more|all]
nlvm [-t] list moves [more|all]
nlvm [-t] list partitions [device] [mask] [more|all]
nlvm [-t] list pools [exclude] [more|all]
nlvm [-t] list snaps [more|all]
nlvm [-t] list volumes [more|all]
```

See “Common Options” (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/nlvm_common_options.html).

- ♦ **Viewing Error Code Messages:** The NSS utility now provides an `/err` switch that can be used from the command prompt. You can use this option to view an error message if a failed NLVM command line operation provides an error code without a corresponding message.

```
nss /err=<error_code_number>
```

For information about error codes, see “NLVM Error Codes” (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/nlvm_ec.html).

Availability for prior releases: November 2012 Scheduled Maintenance for OES 11 SP1

Devices

- ♦ **Unsharing a device:** The `nlvm unshare <device_name>` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/unshare.html) command allows you to disable the Shareable for Clustering state for a device without stopping Novell Cluster Services on the node. The command fails if the device contributes space to an SBD partition, or to a shared pool or a

cluster-enabled pool that is used in any cluster resource. Previously, it was necessary to temporarily stop Novell Cluster Services in order to unshare a device after you disabled clustering for a pool.

Partitions

- ♦ **Creating a partition:** The `type=<partition_type>` option in the `nlvm create partition` (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/create_part.html) command added support for partition type 1ac for snap partitions.

Linux Volumes

- ♦ **Creating a Linux volume:** The following enhancements and changes were made to the `nlvm create linux volume` (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/create_lxvol.html) command:
 - ♦ **Devices option:** The `device=<device_name>` option was modified to allow you to alternatively specify a shared device with no data partitions or an uninitialized device for a clustered LVM volume. Previously, you could specify only an unshared initialized device.
 - ♦ **Partition option:** The `part=<partition_name>` option allows you to specify an existing partition as the location for a non-clustered Linux volume. It can be used instead of the `device` and `size` options.
 - ♦ **Size:** The minimum size for a Linux volume was increased from 1 MB to 8 MB. This change is consistent with the minimum size allowed in NSSMU.
 - ♦ **NCP volume ID for clustered LVM volumes:** The `valid=<ncp_volume_id>` option can be used in combination with the `shared` and `ncp` options to specify an NCP volume ID for an NCP-enabled clustered LVM volume. If the `valid` option is not used, an ID is automatically assigned by Novell Cluster Services when the resource is created. This allows you to assign an NCP volume ID that is unique across all nodes in a cluster, and across all nodes in every peer cluster in a Business Continuity Cluster.
 - ♦ **Enforcing name restrictions for NCP-enabled LVM volumes:** For NCP-enabled LVM volumes, the `nlvm create linux volume` command has been modified to enforce the NCP length restriction of 14 characters, and to use uppercase letters for the name in the Novell Cluster Services cluster resource scripts for a cluster-enabled LVM volume. Previously, a new LVM volume cluster resource would go comatose immediately after creation if the name specified with the `NCP_VOLUME` parameter in the script was more than 14 characters, or if it included lowercase letters.

Availability for prior releases: November 2012 Scheduled Maintenance for OES 11 SP1
- ♦ **Linux POSIX Volumes Are Not Supported on NSS Software RAID:** Linux POSIX file systems should not be created on NSS software RAID. NLVM commands have been modified to block NSS software RAID from being used as a device when you create a Linux POSIX volume.
- ♦ **Availability for prior releases:** September 2012 Scheduled Maintenance for OES 11 and OES 11 SP1
- ♦ **Listing details for a Linux volume:** The `nlvm list linux volume <lx_volume_name>` (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/list_lxvol.html) command displays detailed information for a specified Linux volume.
- ♦ **Mounting a Linux volume:** The `nlvm linux mount <lx_volume_name>` (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/linux_mount.html) command allows you to mount non-LVM and LVM volumes in Linux using the mount parameters stored in the `/etc/fstab` file. You can optionally specify the mount options. If the Linux volume is NCP-enabled, it also automatically mounts the volume for NCP, and NCP assigns it a volume ID.

- ♦ **Unmounting a Linux volume:** The `nlvm linux unmount <lx_volume_name>` (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/linux_unmount.html) command allows you to unmount non-LVM and LVM volumes in Linux. If the Linux volume is NCP-enabled, it also automatically dismounts the volume for NCP before it dismounts it in Linux.

Linux Volume Support in SLES 11 SP3

For information about Linux volume support changes in SUSE Linux Enterprise Server 11 SP3, see “What’s New in SLES 11 SP3” (http://www.suse.com/documentation/sles11/stor_admin/data/new_sles11sp3.html) in the *SUSE Linux Enterprise Server 11 Storage Administration Guide* (http://www.suse.com/documentation/sles11/stor_admin/data/bookinfo.html).

1.2.19 NetStorage

NetStorage in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. There are no other changes in the OES 11 SP2 release of NetStorage.

IMPORTANT: Beginning with OES 11 SP2, no further enhancements are planned for NetStorage. For more information, see the [Notice about certain OES services](#).

1.2.20 QuickFinder

QuickFinder in OES 11 SP2 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. There are no other changes in the OES 11 SP2 release of QuickFinder.

IMPORTANT: Beginning with OES 11 SP2, no further enhancements are planned for QuickFinder. For more information, see the [Notice about certain OES services](#).

1.2.21 Novell Remote Manager

Novell Remote Manager provides the following enhancements and changes in OES 11 SP2:

Managing AFP Services

The AFP plug-in for Novell Remote Manager allows you to manage AFP connections and open files for Novell AFP users. For an overview of the AFP plug-in, see “Managing AFP Services” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nrm_afp.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Managing CIFS Services

The CIFS plug-in for Novell Remote Manager allows you to manage CIFS connections and open files for Novell CIFS users. For an overview of the CIFS plug-in, see “Managing CIFS Services” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nrm_cifs.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Ganglia and Nagios Health Monitoring Tools

Ganglia and Nagios open source health monitoring tools replace the Health Monitor function in Novell Remote Manager in OES 11 SP2. Unlike the Health Monitor, Ganglia and Nagios tools do not use SFCB for management communications. See “[Diagnosing Problems Using Ganglia and Nagios \(OES 11 SP2\)](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_ganglia_nagios.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_ganglia_nagios.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Ganglia and Nagios Monitoring Tools Obsolete the NRM Health Monitor

The Health Monitor function in Novell Remote Manager is obsoleted in OES 11 SP2. It is replaced by the Ganglia and Nagios open source monitoring tools, which do not use the Small Footprint CIM Broker (SFCB) for communications. For information about configuring and using Ganglia and Nagios to monitor the health of the server and services, see “[Diagnosing Problems Using Ganglia and Nagios](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_ganglia_nagios.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_ganglia_nagios.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

For information about using the Health Monitor in OES 11 SP1 and earlier releases, see “[Diagnosing Problems Using Health Monitor \(OES 11 SP1\)](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_monitor_oes11sp1.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_monitor_oes11sp1.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Nagios Alert Notification Obsoletes HTTPSTKD Email Notification

The Novell Remote Manager email notification system is obsoleted in OES 11 SP2. For health monitoring, it is replaced by the Nagios alert notification system, which is used to send alerts from the Ganglia and Nagios health monitoring tools.

After you install or upgrade to OES 11 SP2, the Novell Remote Manager email notification system is not available. The commands `mailserver` and `mailto` are not found in the HTTPSTKD configuration file (`/etc/opt/novell/httpstkd.conf`) for a new install, and they are no longer supported after an upgrade.

Other functions or plug-ins that leveraged the HTTPSTKD email notification commands do not work with the Nagios alert notification system. Thus, they do not work in OES 11 SP2. For example, the NCP Server plug-in *Manage NCP Services*, the *Send* option in the *Email Report* column no longer works on the NCP Inventory Reports page and the NCP Trustee Reports page. This issue will be addressed in a future release.

In order to receive health monitoring alerts from Ganglia and Nagios, you must configure Nagios and its alert notification system. You must set up an email address for the `nagiosadmin` user. You can define other Nagios contacts. You can set up various notification methods for each Nagios contact, and assign the contacts to receive notifications for designated monitored services. For more information, see “[Configuring Nagios](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nagios-config.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nagios-config.html) and “[Configuring Nagios Notification System for Contacts](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nagios_notifications.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nagios_notifications.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Support for Internet Explorer 10

Web-based access to Novell Remote Manager is supported for the Internet Explorer 10 web browser in the desktop user interface view for Windows 7 clients and Windows 8 clients.

Availability for prior releases: January 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

Support for Safari 6.0 on Mac OS X 10.8

Web-based access to Novell Remote Manager is supported for the Apple Safari 6.0 web browser on Mac OS X 10.8 clients.

Availability for prior releases: January 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

1.2.22 Novell Storage Services (NSS)

In addition to bug fixes, NSS provides the following enhancements and changes in OES 11 SP2:

- ♦ **_admin supports up to 64 concurrent requests:** The re-entrance issue in the `_admin` for user space calls has been resolved, and it can handle up to 64 concurrent requests.
- ♦ **file.cmd Supports All NSS Namespaces and Nametypes:** The `file.cmd` interface now works with all the NSS supported nametypes (regular, deleted file) and namespaces (DOS, UNIX, LONG, Macintosh).
- ♦ **NSS Change Owner Utility (nsschown):** The `nsschown` utility has been introduced in OES 11 SP2 to identify the files and directories that have obsolete owners, and to list or change the files owned by existing or obsolete owners for directories or files in an NSS volume. For more information, see “[nsschown](#)” in the *OES 11 SP2: NSS File System Administration Guide for Linux*.
- ♦ **Rights to Files and Folders:** Using the Users or Groups plug-in, you can add or modify rights to files and folders for a user or group on a specified volume from a *Rights to Files and Folders* tab. You can do this even while creating users or groups. You can also verify the explicit rights of a user or group on a given volume. For more information, see “[Managing Rights](#)” in the *OES 11 SP2: NSS File System Administration Guide for Linux*.
- ♦ **View Effective Rights:** In iManager, using the Files and Folders plug-in, you can view the effective rights that a trustee has on a folder or file. For more information, see “[Managing Rights](#)” in the *OES 11 SP2: NSS File System Administration Guide for Linux*.
- ♦ **Linux Multipath I/O Changes in SLES 11 SP3:** The Linux Device Mapper - Multipath software deprecated some attributes and modified some default settings for attributes in the `/etc/multipath.conf` file in SUSE Linux Enterprise Server 11 SP3. After upgrading to SLES 11 SP3, the `multipathd` daemon might not work with your existing multipath configuration file. Ensure that you verify your `/etc/multipath.conf` file before you start the `multipathd` daemon after an upgrade to OES 11 SP2. For information about the latest attributes and default settings, see the `multipath.conf(5)` man page after you install or upgrade the server. For more information, see “[Linux Multipath I/O Changes in SLES 11 SP3](#)” in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide*.
- ♦ **New metamig Export Option:** A new export option (`-p`) has been added to `metamig`. This option exports the metadata of all the files under a given path. For more information, see the `metamig` man page. For more information, see “[metamig](#)” in the *OES 11 SP2: NSS File System Administration Guide for Linux*.

1.2.23 Storage Management Services

Novell SMS supports OES 11 SP2 services and file systems running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. There are no other changes in the OES 11 SP2 release of SMS.

1.2.24 File Systems Management (Storage)

In addition to bug fixes, OES 11 SP2 provides the following enhancements and changes for file systems management:

Path Visibility Is Updated Immediately When a Folder or File Is Deleted

NCP Server has been modified to immediately update the path visibility when a folder or file is deleted, if the logged in/mapped user had trustee rights assigned on it. The deleted file or folder and its parent path are no longer displayed unless the user has rights set at a higher level in the directory tree. In previous releases, the parent path remains visible until NCP Server gets restarted.

Setting the [Public] Trustee for a Distributed File Services Junction in iManager

The Distributed File Services plug-in for iManager was modified to allow the [Public] trustee to be selected as a trustee of a junction. For information about setting trustees on DFS junctions, see “[Adding or Deleting Trustees for the Junction](#)” in the *OES 11 SP2: Novell Distributed File Services Administration Guide for Linux*.

Availability for prior releases: May 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

Rights to Files and Folders

The Files and Folders plug-in to iManager provides a Rights to Files and Folders view that lists the directories and files where a specified user or group has been assigned explicit rights as a trustee. This reverse look-up shows the locations where rights are set; it does not list all locations where the user has access through rights granted by inheritance or [Public]. See “[Managing Effective Rights](#)” (http://www.novell.com/documentation/oes11/stor_filesys_lx/data/effective_rights.html) in the *OES 11 SP2: File Systems Management Guide* (http://www.novell.com/documentation/oes11/stor_filesys_lx/data/bookinfo.html).

Novell Client Support for Windows 8 and Server 2012

The Novell Client 2 SP3 for Windows added support for the following:

- ♦ Windows 8 (32-bit and 64-bit), excluding Windows 8 RT
- ♦ Windows Server 2012 (64-bit)

Novell Client 2 SP3 for Windows documentation is available [online \(http://www.novell.com/documentation/windows_client/\)](http://www.novell.com/documentation/windows_client/). Documentation for earlier versions is available under [Previous Releases \(http://www.novell.com/documentation/windows_client/#previous\)](http://www.novell.com/documentation/windows_client/#previous).

Availability for prior releases: January 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

OES Client Services Support for Windows 8 and IE 10

OES client services (that is, OES-related products that support access to files stored on OES servers) added support for user access from Windows 8 clients (excluding Windows 8 RT) effective in January 2013 Scheduled Maintenance.

Domain Services for Windows (DSfW) supports Windows 8 beginning with OES 11 SP2.

Client applications are supported to run on Windows 8 clients in the desktop user interface view.

Web-based client access is supported for the Internet Explorer 10 web browser in the desktop user interface view for Windows 7 clients and Windows 8 clients.

Availability for prior releases: January 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

OES Client Services Support for Windows Server 2012

OES client services added support for user access from Windows Server 2012 servers.

OES Client Services Support for Mac OS X 10.8 and Safari 6.0

OES client services added support for user access from Mac OS X Mountain Lion (version 10.8) clients with the exception of Novell iFolder.

Web-based client access is supported for the Apple Safari 6.0 web browser on Mac OS X 10.8 clients with the exception of Novell iFolder:

The Novell iFolder client does not run on Mac OS X 10.8 clients and does not support them. Novell iFolder does not support the Safari 6.0 browser.

Availability for prior releases: January 2013 Scheduled Maintenance for OES 11 and OES 11 SP1. DSfW support begins in OES 11 SP2.

1.2.25 NSS Auditing Client Logger (VLOG)

The NSS Auditing Client Logger (VLOG) Utility supports OES 11 SP2 running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP3. In addition to bug fixes, VLOG provides the following enhancements:

- ♦ **MaxFileCount:** The default value for maxStreamFileCount has changed from 50 files to 4096 files.

Availability for prior releases: July 2013 Scheduled Maintenance for OES11 and OES 11 SP1

- ♦ **Four Events Are Logged for a File or Folder Delete from an NCP or CIFS Client:** The file and folder delete functions for the NSS file system in NCP Server and Novell CIFS were modified to use the POSIX APIs. When you use an NCP client or a CIFS client to delete a file or folder on an NSS file system, three new auditing events are logged in addition to the DELETE event: OPEN, MODIFY, and CLOSE.

For OES 11 SP1 and earlier, the delete action triggers only a DELETE event.

1.2.26 Web Services

The web services and applications in Novell Open Enterprise Server (OES) 11 Support Pack 2 (SP2) are Novell software and open source software that support SUSE Linux Enterprise Server (SLES) 11 Service Pack 3 (SP3).

Upgrading from MySQL 5.0 to MySQL 5.5 Introduces a New Database Format

SUSE Linux Enterprise Server 11 SP3 introduces an upgrade of MySQL from version 5.0 to version 5.5. This upgrade involves a change of the database format. You must manually migrate your existing MySQL database to the new format before MySQL can run again. After you upgrade to MySQL 5.5, its daemon is not automatically started. We recommend that you back up the database before you migrate it to the new format.

To migrate an existing MySQL database to the version 5.5 database format:

- 1 Log in to the server as the *root* user, then open a terminal console.
- 2 At the command prompt, enter

```
touch /var/lib/mysql/.force_upgrade
```

This assumes a local database setup path.

If the database is clustered with Novell Cluster Services, take the MySQL cluster resource offline on a node, manually mount the volume locally, then issue the command using the path to the location on the mounted volume. For example:

```
touch /mnt/mysql/var/lib/mysql/.force_upgrade
```

After the database is reformatted, dismount the volume locally.

- 3 After the migration to the new database format is complete, start MySQL. At the command prompt, enter

```
rcmysql restart
```

- 4 If the database is clustered with Novell Cluster Services, bring the MySQL cluster resource online.

Upgrading from PostgreSQL 8.3 to PostgreSQL 9.1 Introduces a New Database Format

SLES 11 SP3 introduces an upgrade of PostgreSQL from version 8.3 to version 9.1. This upgrade involves a change of the database format. You must manually migrate your existing PostgreSQL database to the new format before PostgreSQL can run again. After you upgrade to PostgreSQL 9.1, its daemon is not automatically started. We recommend that you back up the database before you migrate it to the new format.

A new `pg_upgrade` tool is provided to migrate the PostgreSQL database to the new format. Both the 8.3 version and 9.1 version of the software are included in SLES 11 SP3 to accommodate the use of this tool. For information about how to perform a database migration using the `pg_upgrade` tool, see the `pg_upgrade` tool documentation (`/usr/share/doc/packages/postgresql91/html/pgupgrade.html`) on the server (requires the `postgresql91-docs` package).

- 1 Ensure that you apply the latest patches for PostgreSQL 8.3.

The latest patch relocates the software from its standard location to a versioned location such as `/usr/lib/postgresql83/bin`. Symbolic links are used to make the software available in the standard location.

- 2 Install PostgreSQL 9.1 and its dependent packages. The `pg_upgrade` tool is found in the `postgresql91-contrib` package.

The packages are installed to a versioned location such as `/usr/lib/postgresql91/bin`. Symbolic links are used to make the software available in the standard location instead of version 8.3.

- 3 Use the `pg_upgrade` tool to migrate the PostgreSQL database format from version 8.3 to version 9.1.

Unless the tool is used in link mode, the server must have enough free disk space to temporarily hold a copy of the database files. You can run the `du -hs` command to determine if enough space is available:

```
du -hs /var/lib/pgsql/data
```

This directory is the default PostgreSQL location for databases. Use the actual database path for your system.

PHP 5.3 Replaces PHP 5.2

PHP 5.3 is supported in SLES 11 SP3. The PHP 5.2 package has been removed. Both PHP 5.2 (deprecated) and PHP 5.3 were available in SLES 11 SP2.

WebSphere Application Server CE Is Removed in SLES 11 SP3

The WebSphere Application Server CE package has been removed from SLES 11 SP3. It is no longer supported.

1.3 What's New or Changed in OES 11 SP1

OES 11 SP1 includes new or changed features in the following components:

- [Section 1.3.1, "AFP," on page 47](#)
- [Section 1.3.2, "Archive and Version Services," on page 47](#)
- [Section 1.3.3, "CIFS," on page 47](#)
- [Section 1.3.4, "Distributed File Services," on page 47](#)
- [Section 1.3.5, "DNS and DHCP," on page 48](#)
- [Section 1.3.6, "Domain Services for Windows," on page 48](#)
- [Section 1.3.7, "Dynamic Storage Technology," on page 49](#)
- [Section 1.3.8, "eDirectory," on page 50](#)
- [Section 1.3.9, "File Systems Management \(Storage\)," on page 50](#)
- [Section 1.3.10, "Install," on page 50](#)
- [Section 1.3.11, "iPrint," on page 51](#)
- [Section 1.3.12, "Linux POSIX Volume Support," on page 51](#)
- [Section 1.3.13, "Linux User Management," on page 54](#)
- [Section 1.3.14, "Migration Tool," on page 54](#)
- [Section 1.3.15, "NCP Server," on page 55](#)
- [Section 1.3.16, "NetStorage," on page 55](#)
- [Section 1.3.17, "Novell Cluster Services 2.1," on page 55](#)
- [Section 1.3.18, "Novell Linux Volume Manager," on page 59](#)

- ♦ [Section 1.3.19, “Novell Remote Manager,” on page 61](#)
- ♦ [Section 1.3.20, “Novell Samba,” on page 61](#)
- ♦ [Section 1.3.21, “Novell Storage Services,” on page 61](#)
- ♦ [Section 1.3.22, “NSS Auditing Client Logger \(VLOG\),” on page 62](#)
- ♦ [Section 1.3.23, “QuickFinder,” on page 62](#)
- ♦ [Section 1.3.24, “Storage Management Services,” on page 62](#)
- ♦ [Section 1.3.25, “Web Services,” on page 63](#)

1.3.1 AFP

Novell AFP in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, Novell AFP provides the following enhancements and behavior changes in the OES 11 SP1 release:

Subtree Search

Subtree search feature is introduced for searching AFP users in subtrees in eDirectory. For more information, see [Subtree Search](#) in the [OES11 SP1: Novell AFP Administration Guide](#).

1.3.2 Archive and Version Services

The Archive and Version Services in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. There are no other changes in the OES 11 SP1 release of Archive and Version Services.

1.3.3 CIFS

Novell CIFS in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, OES 11 SP1 provides the following enhancements and changes for CIFS:

Ability to View Trustees/IRM Assigned to Files and Folders

Novell CIFS will now be able to display the list of trustees associated with the specified file or folder as per the CIFS cache record, import the trustee information from the `trustee_database.xml` file associated with the specified volume into the CIFS cache, and display the count of new, modified, and removed trustees for the specified volume. For more information, see [“Viewing the Trustees Associated with a File or Folder,”](#) [“Synchronizing the Trustee List for a Volume,”](#) and [“Viewing Statistics of Trustees for a Volume”](#) in the [OES 11 SP1: Novell CIFS for Linux Administration Guide](#).

1.3.4 Distributed File Services

Novell Distributed File Services in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, OES 11 SP1 provides the following enhancements and changes for DFS:

Setting the [Public] Trustee for a Distributed File Services Junction in iManager

The Distributed File Services plug-in for iManager was modified to allow the [Public] trustee to be selected as a trustee of a junction. For information about setting trustees on DFS junctions, see [Adding or Deleting Trustees for the Junction](#) in the [OES 11 SP1: Novell Distributed File Services Administration Guide for Linux](#).

1.3.5 DNS and DHCP

The DNS and DHCP Services in OES 11 SP1 have been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, the following enhancements are available:

Path Change for dhcpd.pid

In OES 11, the DHCP process ID is located in `/var/run/dhcpd.pid`.

In OES 11 SP1, the DHCP process ID is located in `/var/lib/dhcp/var/run/dhcpd.pid`. The path for `dhcpd.pid` was changed because the `/opt/novell/dhcp/bin/cluster_dhcpd.sh` script was modified to support DHCP-4.2.3-P2 in SLES 11 SP2. To improve security, SLES 11 SP2 included a security update that enables `dhcpd` to run in a chroot environment. For information about this security update, see “[The SUSE Linux Enterprise Server Version](#)” in the [SLES 11 Administration Guide](#).

The `cluster_dhcpd.sh` script was modified to alter the location of the `dhcpd.pid` file to `/var/lib/dhcp/var/run/`, and set the ownership of the path to the `dhcp` user instead of the root user.

If you use DHCP in a cluster with Novell Cluster Services, you must manually modify the path for the `dhcpd.pid` file in the unload script for the DHCP resource. This allows the process to be gracefully unloaded from a node when the DHCP cluster resource fails over to a different node. For information on how to modify the path, see “[Changing the Path for dhcpd.pid](#)”.

Support for Chinese Characters in Resource Record Names

Beginning in OES 11 SP1, the Java Console supports resource record names specified in the Chinese language. You can now specify resource record names with a combination of English, Chinese, and numeric characters. You can specify a maximum of three Chinese characters during resource record creation.

1.3.6 Domain Services for Windows

Domain Services for Windows in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, Domain Services for Windows provides the following enhancement in the OES 11 SP1 release:

Simplified Install

DSfW installation and configuration using the YaST administrative tool has been modified. The configuration screens have been reorganized to enable you to deploy a Domain Controller in a fast and easy manner. DSfW now enables you to deploy a domain controller using the *Express Install* option. Express Install minimizes the number of configuration screens and assigns default values for certain configuration parameters. For more information, see [Installing Domain Services for Windows](http://www.novell.com/documentation/oes11/acc_dsfw_lx/?page=/documentation/oes11/) (http://www.novell.com/documentation/oes11/acc_dsfw_lx/?page=/documentation/oes11/)

[acc_dsfw_lx/data/bjcs5rp.html](http://www.novell.com/documentation/oes11/acc_dsfw_lx/data/bjcs5rp.html)) in the *OES 11 SP1: Domain Services for Windows Administration Guide* (http://www.novell.com/documentation/oes11/acc_dsfw_lx/?page=/documentation/oes11/acc_dsfw_lx/data/bookinfo.html).

DSfW AutoYaST Install

DSfW AutoYaST enables you to install DSfW for a new forest domain, new domain in an existing forest, and new domain controller in an existing domain without any manual intervention. For information, see *Installing DSfW Using AutoYast* (https://www.novell.com/documentation/oes11/acc_dsfw_lx/?page=/documentation/oes11/acc_dsfw_lx/data/b11i6bnj.html) in the *OES 11 SP1: Domain Services for Windows Administration Guide* (http://www.novell.com/documentation/oes11/acc_dsfw_lx/?page=/documentation/oes11/acc_dsfw_lx/data/bookinfo.html).

1.3.7 Dynamic Storage Technology

Dynamic Storage Technology supports OES 11 SP1 file systems running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, the following enhancements are available:

- ♦ **Search Pattern:** You can specify file names with spaces in them.
- ♦ **ShadowFS:** The *Load ShadowFS now and at boot time* option has been renamed as *Load ShadowFS*. When you select the *Load ShadowFS* check box and click *Submit*, Dynamic Storage Technology starts an instance of ShadowFS by issuing the `/etc/init.d/novell-shadowfs start` command when you click the button, and configures the server to load ShadowFS at system restart. Only one instance of ShadowFS should be running at a time. ShadowFS should be enabled only if you are using Novell Samba or supported Linux file access protocols to access the DST volume.
- ♦ **Subdirectory Restrictions:** The Subdirectory Restrictions filter has been modified as follows:
 - ♦ Precede subdirectory paths with a forward slash (/), such as
`/subdir1/subdir2`
 - ♦ In addition to subdirectory paths, the Exclude Subdirectory option allows you to specify a directory name that might exist in multiple places on a volume. You indicate this intended action by specifying only a directory name with no forward slashes, and the directory name must contain at least one wildcard (such as ? or *). All instances of directories that match the specified directory name are excluded from the policy run.

For example, to exclude all GroupWise archive subdirectories, specify the following directory name with wildcards:

`of???arc`

For information, see “Subdirectory Restrictions” (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bb8ubn2.html#bb8udwu) in the *OES 11 SP1: Dynamic Storage Technology Administration Guide* (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bookinfo.html).

1.3.8 eDirectory

The Graphical DS Repair Utility has been added to OES 11 SP1. This tool is automatically installed during a new OES 11 SP1 installation. If you are upgrading to OES 11 SP1, you must manually select *novell-ndsgrepair* under the eDirectory pattern.

The eDirectory team is updating the documentation for the Graphical DS Repair. When the documentation is completed, a link will be posted here and in the OES 11 SP1 online documentation pages on the Web.

1.3.9 File Systems Management (Storage)

The storage file systems, management tools, and file access protocols support OES 11 SP1 running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. The following changes and enhancements are available for file system management in Novell Open Enterprise Server 11 SP1:

- ♦ **Btrfs:** Support was added for the Btrfs file system. The Novell Storage Services (NSS) Management Utility (NSSMU), Novell Linux Volume Manager (NLVM) Linux commands, NCP Server, and Novell Cluster Services were modified to support the Btrfs file system for Linux volumes. The Btrfs file system is now available as an alternative to other supported file systems (Ext2, Ext3, Reiserfs, and XFS) when you create a Linux volume. The *btrfsprogs* package is required. You can use NSSMU or NLVM to manage the Btrfs volumes as you would manage other Linux data volumes. Btrfs volumes can also be configured for NCP file access and for clustering with Novell Cluster Services.

SUSE Linux Enterprise Server (SLES) 11 Service Pack 2 (SP2) also supports the Btrfs file system in the YaST2 Partitioner. You can use the Partitioner during the system installation to configure a Btrfs solution for the system device. YaST2 automatically installs the *btrfsprogs* package if you use Btrfs for the root (/) file system. Bootloader support for /boot on Btrfs is not available in SLES 11 SP2; it is planned to be available beginning in SUSE Linux Enterprise 12.

For information about the features of Btrfs, see “Btrfs” (http://www.novell.com/documentation/oes11/stor_posixvol_lx/data/bwk8gda.html) in the *OES 11 SP1: Linux POSIX Volume Administration Guide* (http://www.novell.com/documentation/oes11/stor_posixvol_lx/data/bookinfo.html).

- ♦ **NCP Volumes:** You can NCP enable Linux volumes as you create them by using NSSMU or the `nlvm create linux volume` command. For information, see the following:
 - ♦ “Managing Linux Volumes with NSSMU” and “Clustering LVM Volume Groups with Novell Cluster Services” in the *OES 11 SP2: Linux POSIX Volume Administration Guide*
 - ♦ “Create Linux Volume” in the *OES 11 SP2: NLVM Reference*
- ♦ **NCP Trustee Report:** The NCP Trustee Report in Novell Remote Manager can be used to generate reports for an NSS volume, including a Dynamic Storage Technology shadow volume comprised of two NSS volumes. For information, see “Generating and Viewing NCP Trustee Reports for NSS Volumes” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/trustee_reports.html) in the *OES 11 SP1: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

1.3.10 Install

- ♦ Unattended upgrade from OES 2 or OES 11 to OES 11 SP1 has been enhanced and has undergone some changes. For more information, see “Using AutoYaST for an OES 11 SP2 Upgrade” in the *OES 11 SP2: Installation Guide*.

- ♦ A single integrated ISO to install or upgrade OES 11 SP1 is now available. This ISO contains both SLES 11 SP2 and OES 11 SP1.
- ♦ Channel upgrade support is added in OES 11 SP1. It supports upgrade from OES 11 to OES 11 SP1.

1.3.11 iPrint

This section describes enhancements and changes to Novell iPrint for Novell Open Enterprise Server (OES) 11 SP1.

- ♦ Novell iPrint now runs on the OES 11 SP1 platform. Novell iPrint supports the SLES 11 base completely, along with its enhancements and hardware for its lifecycle.
- ♦ Novell secure printing and iPrint Client Management features can now function without the Novell Client component. Users working on Windows / Active Directory environments now can have ICM and shared login abilities with or without the Novell Client.
- ♦ Print driver transfer methods in iPrint Migration have been improved, and dependencies on other stacks have been reduced to increase reliability and robustness. iPrint Migration has also been enhanced in areas such as Print Driver transfer and Driver Platform selection.
- ♦ The `iprintman` utility now runs on Windows, Mac, and Linux clients, and has been rewritten to use the Java IPP libraries for performing various operations.

NOTE: This feature is under development and might not function as expected in all cases. Novell plans to complete development in a future OES release.

Novell iPrint in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, iPrint provides the following enhancements and behavior changes in the OES 11 SP1 release:

You can download iPrint Clients from the OES 11 SP1 welcome page or from the iPrint Printer List web page. You can download the latest version of the iPrint Client from the [iPrint Client download site](#).

iPrint Windows Client

A new version of the iPrint Client 5.94 is available for Windows XP/Vista/Win 7/Win 8/Win 8.1.

iPrint Macintosh Client

A new version of the iPrint Client for Macintosh 5.74 is available for Mac OS X 10.7 and later. The 5.74 client includes support for Mac OS X 10.9 (Mavericks).

Direct Print Accounting for iPrint Macintosh Client

You can now perform accounting operations for iPrint Direct Printers on the iPrint Mac Client 5.74.

1.3.12 Linux POSIX Volume Support

The NLVM and NSSMU management tools support Linux POSIX volumes on OES 11 SP1 running on 64-bit SUSE Linux Enterprise Server (SLES) 11 Service Pack (SP) 2.

NSSMU

In addition to bug fixes, NSSMU provides the following changes and enhancements for Linux POSIX volume management in the OES 11 SP1 release:

- ♦ **Create Linux Volume:**
 - ♦ The *NCP Enable* option can be used to enable the Linux POSIX file system on the volume to be accessed with the NetWare Core Protocol (NCP).
 - ♦ Support was added for the Btrfs file system. The Btrfs file system is now available as an alternative to other supported file systems (Ext2, Ext3, Reiserfs, and XFS) when you create a Linux volume. The `btrfsprogs` package is required. You can use NSSMU or NLVM to manage the Btrfs volumes as you would manage other Linux data volumes. Btrfs volumes can also be configured for NCP file access and for clustering with Novell Cluster Services.
- ♦ **Confirmation Prompt:** You are automatically prompted to confirm actions for certain commands that destroy data, such as when you initialize a device or delete Linux POSIX volumes.
- ♦ **File System Types:** When you create a Linux POSIX volumes, the supported file system types are now listed in alphabetical order: btrfs, ext2, ext3, reiserfs, and xfs.
- ♦ **Linux Volume Details:** On the Linux Volumes page, a volume's information includes the *NCP Enabled* parameter and status (Yes or No).
- ♦ **Mount Point Path:** The default mount point path for Linux volumes is `/usr/novell/<volume_name>`.
- ♦ **Partitions:** On the NSSMU Partitions page, the Partitions list panel has been widened to accommodate long partition names. If you widen the NSSMU display screen, it widens the Partitions list panel and allows you to see the partitions' full names.

NLVM Commands

In addition to bug fixes, NLVM commands provide the following changes and enhancements for Linux POSIX volume management in the OES 11 SP1 release:

- ♦ **Sizes:** The following enhancements are available for the `size` option:
 - ♦ The default multiplier for sizes was changed from M (megabytes) to G (gigabytes). If no multiplier is provided, the value is assumed to be in gigabytes. For example:

```
size=20 (20 gigabytes is used)
```
 - ♦ Use the T multiplier to specify sizes in terabytes (TB).
 - ♦ All sizes can be entered as whole numbers or with fractional parts such as 200.45G and 3.98T.
- ♦ **Multiple Devices:** You can specify multiple devices for the following commands:
 - ♦ **Init:** You can specify multiple devices to be initialized at the same time. Each device is formatted with the same specified partitioning scheme and share state.
 - ♦ **Share:** You can specify multiple devices to be shared at the same time.
 - ♦ **Unshare:** You can specify multiple devices to be unshared at the same time.
- ♦ **No Prompt:** The `--no-prompt` NLVM option can be used with the `nlvm delete linux volume` command and the `nlvm init` command to prevent a confirmation message from being displayed.
- ♦ **Confirmation Prompt:** You are automatically prompted to confirm actions to initialize a device or to delete a Linux POSIX volume.

- ♦ **Create Linux Volume:**

- ♦ Support was added for the Btrfs file system. The Btrfs file system is now available as an alternative to other supported file systems (Ext2, Ext3, ReiserFs, and XFS) when you create a Linux volume. The `btrfsprogs` package is required. You can use NSSMU or NLVM to manage the Btrfs volumes as you would manage other Linux data volumes. Btrfs volumes can also be configured for NCP file access and for clustering with Novell Cluster Services
- ♦ The `ncp` option for the `nlvm create linux volume` command can be used to enable the Linux POSIX file system on the volume to be accessed with the NetWare Core Protocol (NCP).

- ♦ **List Linux Volumes:** The volume information displays `NCP` if the Linux volume is enabled for NCP.

Btrfs File System

NSSMU, NLVM Linux commands, NCP Server, and Novell Cluster Services were modified to support the Btrfs file system for Linux volumes. The Btrfs file system is now available as an alternative to other supported file systems (Ext2, Ext3, Reiserfs, and XFS) when you create a Linux volume. The `btrfsprogs` package is required. You can use NSSMU or NLVM to manage the Btrfs volumes as you would manage other Linux data volumes. Btrfs volumes can also be configured for NCP file access and for clustering with Novell Cluster Services.

SUSE Linux Enterprise Server (SLES) 11 Service Pack 2 (SP2) also supports the Btrfs file system in the YaST2 Partitioner. You can use the Partitioner during the system installation to configure a Btrfs solution for the system device. YaST2 automatically installs the `btrfsprogs` package if you use Btrfs for the root (/) file system. Bootloader support for `/boot` on Btrfs is not available in SLES 11 SP2; it is planned to be available beginning in SUSE Linux Enterprise 12.

For information about the features of Btrfs, see “Btrfs” (http://www.novell.com/documentation/oes11/stor_posixvol_ix/data/bwk8gda.html) in the *OES 11 SP1: Linux POSIX Volume Administration Guide* (http://www.novell.com/documentation/oes11/stor_posixvol_ix/data/bookinfo.html).

NCP Volumes and Cluster Resources

NSSMU and NLVM were modified to support the creation of NCP volumes on Linux POSIX file systems. You can NCP enable Linux POSIX volumes, an LVM volumes, and clustered LVM volumes as you create them. When you enable NCP for a Linux volume, an NCP volume of the same name (using all capital letters) is automatically created. An NCP share is created at the root of the Linux volume.

For clustered LVM volumes, the NCP Virtual Server object is automatically created and the NCP mount, dismount, and status commands are added to the scripts for the LVM volume group cluster resource. The Novell Cluster Services Generic File System template is used to specify the default cluster policies and scripts for the cluster resource. After you create the resource, you can use the Clusters plug-in for iManager to set up preferred nodes for the resource and to manage the resource.

Linux Volume Support in SLES 11 SP2

For information about Linux volume support changes in SUSE Linux Enterprise Server 11 SP2, see “What’s New in SLES 11 SP2” (http://www.suse.com/documentation/sles11/stor_admin/data/bwkb7my.html) in the *SUSE Linux Enterprise Server 11 Storage Administration Guide* (http://www.suse.com/documentation/sles11/stor_admin/data/bookinfo.html).

1.3.13 Linux User Management

Linux User Management in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, Linux User Management provides the following enhancements and behavior changes in the OES 11 SP1 release:

- ♦ **Enabling Multiple Users for Linux in a LUM Group:** The LUM iManager plug-in provides a new tab that allows you to linux-enable multiple users in a group in a simplified manner. For more information, see “Enabling Multiple Users for Linux in a LUM Group” (http://www.novell.com/documentation/oes11/acc_linux_svcs_lx/index.html?page=/documentation/oes11/acc_linux_svcs_lx/data/bv1u9ka.html#bzv3vj6.) in the *OES 11 SP1: Novell Linux User Management Administration Guide* (http://www.novell.com/documentation/oes11/acc_linux_svcs_lx/?page=/documentation/oes11/acc_linux_svcs_lx/data/bookinfo.html).
- ♦ **Enabling Multiple Users for Linux in a Container:** You can now Linux-enable multiple users in a container. The LUM iManager plug-in provides a new tab that allows you to linux-enable multiple users in a container. For more information, see “Enabling Multiple Users for Linux in a Container” (http://www.novell.com/documentation/oes11/acc_linux_svcs_lx/?page=/documentation/oes11/acc_linux_svcs_lx/data/bv1u9ka.html) in the *OES 11 SP1: Novell Linux User Management Administration Guide* (http://www.novell.com/documentation/oes11/acc_linux_svcs_lx/?page=/documentation/oes11/acc_linux_svcs_lx/data/bookinfo.html).

You can linux-enable multiple users using the command line as well. The `namuseradd` command provides the `-A` option that allows you to enable all non-LUM users in the specified context. For more information, see the `namuseradd` utility (http://www.novell.com/documentation/oes11/acc_linux_svcs_lx/?page=/documentation/oes11/acc_linux_svcs_lx/data/bv1u77n.html) in the *OES 11 SP1: Novell Linux User Management Administration Guide* (http://www.novell.com/documentation/oes11/acc_linux_svcs_lx/?page=/documentation/oes11/acc_linux_svcs_lx/data/bookinfo.html).

- ♦ **Option to Select administrator group in YaST:** The LUM configuration in YaST always adds the administrator to a group called the `admingroup`. LUM configuration in YaST now provides an option to browse and specify an already existing group instead of creating a new `admingroup`.

1.3.14 Migration Tool

The Migration Tool in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, the Migration Tool provides the following enhancements and behavior changes.

Linux to Linux Service Migration

You can now migrate services from OES 2 SP2, OES 2 SP3, OES 11, and OES 11 SP1 source servers to an OES 11 SP1 target server using service-specific migration scripts. For information, see “Service Migration” in the *OES 11 SP2: Migration Tool Administration Guide*.

Enhanced Sync Performance

The Migration Tool data synchronization feature has been enhanced. You must upgrade the source server with the latest patches before performing migration.

- ♦ If the source server is NetWare, contact Novell Technical Support (NTS) for information on patching the server.

Copy Trustees Only At the Directory Level

Synchronizes trustees only at the directory level. Trustees at the file level are not synchronized.

Do Not Copy Trustees

Trustees on the source server are not synchronized to the target server; only data is synchronized.

1.3.15 NCP Server

NCP in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, NCP provides the following enhancements and behavior changes in the OES 11 SP1 release:

- ♦ NCP Server was modified to refresh its OpenSLP registration of cluster resource virtual NCP servers based on the setting for the eDirectory advertise-life-time (`n4u.nds.advertise-life-time`) parameter. The `n4u.nds.advertise-life-time` parameter is set by default to 3600 seconds (1 hour) and has a valid range of 1 to 65535 seconds. Previously, NCP Server re-registered the virtual NCP servers with SLP every 30 minutes regardless of the eDirectory advertise-life-time setting. For information about setting the eDirectory advertise-life-time parameter in a cluster, see [SLP](#) in the [OES 11 SP1: Novell Cluster Services 2.1 for Linux Administration Guide](#).
- ♦ Introduced `NCP_TCP_KEEPALIVE_INTERVAL` parameter to configure keep alive timeout for all the TCP client connections accepted by the NCP server.
- ♦ The maximum value of `CONCURRENT_ASYNC_REQUESTS` parameter has been increased to 256 from the earlier value of 128.
- ♦ The default value of `CONCURRENT_ASYNC_REQUESTS` and `ADDITIONAL_SSG_THREADS` has been increased to 25.
- ♦ Added a new switch `/v` to `ncpcon volumes` command to list the volume IDs.
- ♦ NCP server does not support NFS and AFP namespaces and hence it will not return these namespaces in response to NCP requests regardless of what namespaces are supported on that volume by NSS.
- ♦ Configuration options are provided to update UID number for non-LUM users.

1.3.16 NetStorage

NetStorage has been modified to run on OES 11 SP1. There are no other changes in the OES 11 SP1 release of NetStorage.

1.3.17 Novell Cluster Services 2.1

Novell Cluster Services 2.1 supports OES 11 SP1 services and file systems running on 64-bit SUSE Linux Enterprise Server 11 SP2. In addition to bug fixes, Novell Cluster Services provides the following enhancements and behavior changes in the OES 11 SP1 release:

Cluster-Enabling an Existing Pool

In the Clusters plug-in to iManager, when you cluster-enable an existing Novell Storage Services (NSS) pool, the *Online Resource after Creation* option on the Cluster Pool Information page is available and deselected by default. If the pool is deactive when you cluster-enable it, you can select this option to automatically bring the resource online, which activates the pool on a preferred node and mounts the pool's volumes.

Previously, the option was deselected and dimmed, the resource was automatically placed in an offline state, and no action was taken for the state of the pool and its volumes.

For information, see “Cluster-Enabling an Existing NSS Pool and Its Volumes” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/hrt0ekvg.html) in the *OES 11 SP1: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Default CIFS Virtual Server Name

When you enable Novell CIFS as an advertising protocol for a cluster-enabled pool, the default name is based on the NCP virtual server object name. If you change the NCP virtual server name in NSSMU or in the Storage plug-in for iManager, the CIFS virtual server name is updated accordingly. For information, see “Novell CIFS for Linux” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bff13ks.html#bgh0tjp) in the *OES 11 SP1: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Enabling NCP for a Clustered Linux POSIX Volume Group

When you create a cluster-enabled Linux POSIX volume group with NSSMU or with the `nlvm create linux volume` command, you can use the `ncp` option to enable users to access the Linux POSIX file system on the volume with the NetWare Core Protocol (NCP). Previously, the NCP volume (share) was created manually after the resource was created and brought online.

For information, see “Configuring an LVM Volume Group Cluster Resource with NSS Management Tools” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bxv3rde.html) in the *OES 11 SP1: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Btrfs File System

The SUSE Linux Enterprise Server 11 SP2 operating system supports the Btrfs file system. The `btrfsprogs` package must be installed.

Novell Cluster Services supports using the Btrfs file system when you create a clustered Linux LVM volume group by using the NSS Management Utility (NSSMU) or Novell Linux Volume Manager (NLVM) commands. If you use Linux commands to create the LVM volume group, you can use the `mkfs.btrfs(8)` command to add the Btrfs file system to the volume. You specify `btrfs` as the file system type for the LVM volume group cluster resource. You can enable NCP file access for the Btrfs volume.

For information, see “Configuring an LVM Volume Group Cluster Resource with NSS Management Tools” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bxv3rde.html) in the *OES 11 SP1: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Cluster Migrate Command

The `cluster migrate` command now offers the `-list`, `-most`, and `-next` options. For information, see “MIGRATE” in the Cluster Management Commands table (https://www.novell.com/documentation/oes11/clus_admin_lx/data/cluster_commands.html#b2klg4d) of the *OES 11 SP1: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Clusters Plug-In for iManager

The Clusters plug-in for iManager 2.7.5 has been reorganized. In *Roles and Tasks* under *Clusters*, the *Cluster Manager*, *BCC Manager*, *Cluster Event Log*, and *Cluster Options* menu items have been replaced with two options: *My Clusters* and *My Resources*. Links on these pages take you to the familiar cluster options presented as tabs: *Cluster Manager*, *BCC Manager*, *Cluster Event Log*, and *Cluster Options*.

- ♦ **My Clusters:** The logged-in cluster administrator can set up a personalized list of clusters to manage. This allows an administrator to view at a glance the status of multiple clusters. An administrator can also customize the display to sort the entries, modify the columns, or filter the entries. The list of clusters and display preferences persist between the administrator's logins to iManager on the same server. For information, see “Setting Up a Personalized List of Clusters to Manage” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/myclusters.html) in the *OES 11 SP1: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).
- ♦ **My Resources:** The logged-in cluster administrator can set up a personalized list of cluster resources to manage. This allows an administrator to view at a glance the status of multiple cluster resources for multiple clusters. An administrator can also customize the display to sort the entries, modify the columns, or filter the entries. The list of cluster resources and display preferences persist between the administrator's logins to iManager on the same server. For information, see “Setting Up a Personalized List of Resources to Manage” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/myresources.html) in the *OES 11 SP1: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

The Clusters plug-in supports the management of OES and NetWare clusters and resources. It cannot be installed on a NetWare server.

If you use Role-Based Services (RBS), upgrading the Clusters plug-in does not automatically update the RBS settings. The RBS Configuration page reports that the Clusters plug-in is out-of-date. The plug-in must be reinstalled on the RBS Configuration page in order to pick up the *My Clusters* and *My Resources* menu options. For information, see “Updating Role-Based Services for the Clusters Plug-in for OES 11 SP1” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/inst_clusters.html#inst_clusters_rb) in the *OES 11 SP1: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

A comparison of the old and new interface is available in “Clusters Plug-In Changes for Novell iManager 2.7.5” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/apdx_clusters_plugin_changes.html) in the *OES 11 SP1: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Availability for prior releases: January 2013 Scheduled Maintenance for OES 11

STONITH

The STONITH (shoot-the-other-node-in-the-head) capability allows Novell Cluster Services to kill a suspect node by using remote power control. Unlike a poison pill, it does not require a response from the suspect node. STONITH is used after a poison pill is issued; it does not replace the poison pill. For information, see “Configuring STONITH” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/stonith.html) in the *OES 11 SP1: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Master Election Process

Novell Cluster Services for OES 11 SP1 introduces some intelligence in the master election process when the master leaves a cluster (voluntarily or involuntarily). The same master is elected under both the old and new algorithms, but the conclusion is reached sooner, especially for larger clusters. The new algorithm substantially reduces the time needed for master election in some cases.

For information about the old and new algorithms, see “Electing a Master Node” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/ncs_master_election.html) in the *OES 11 SP1: Novell Cluster Services NetWare to Linux Conversion Guide* (http://www.novell.com/documentation/oes11/clus_conversion_lx/data/bookinfo.html).

Availability for prior releases: September 2012 Scheduled Maintenance for OES 11

NetWare to Linux Cluster Conversion: File Access Protocol Commands for Monitor Scripts

When you convert NetWare 6.5 SP8 clusters to OES 11 SP1, if the AFP or CIFS protocols are configured as advertising protocols for an NSS pool cluster resource on the NetWare cluster, the corresponding monitoring commands are automatically added to the monitor script for the resource on OES 11 SP1. Monitoring is not available for NetWare clusters and is disabled while the cluster is in mixed mode. Monitoring can be enabled for the resource after the final cluster conversion is complete. For information, see “File Access Protocols for Monitor Scripts” (http://www.novell.com/documentation/oes11/clus_conversion_lx/data/bh9em7s.html#b115ip7x) in the *OES 11 SP1: Novell Cluster Services NetWare to Linux Conversion Guide* (http://www.novell.com/documentation/oes11/clus_conversion_lx/data/bookinfo.html).

DHCP Cluster Resource: Path Change for dhcpd.pid

The DHCP process ID file location was changed from `/var/run/dhcpd.pid` to `/var/lib/dhcp/var/run/dhcpd.pid`. During a cluster upgrade from OES 11 to OES 11 SP1, you must modify the location of the `dhcpd.pid` file in the DHCP cluster resource's unload script. After you modify the script, you should bring the resource online only on OES 11 SP1 nodes. This is necessary to ensure a graceful shutdown of the `dhcpd.pid` process when the DHCP resource fails over to a different node. For information, see “Path Change for dhcpd.pid” and “Changing the Path for dhcpd.pid” in the *OES 11 SP2: Novell DNS/DHCP Services for Linux Administration Guide*.

Change in the Command Sequence for Pool Cluster Resource Scripts

The default sequence of commands has changed for the load script and unload script of newly created NSS pool cluster resources. In the load script, the secondary IP address is added after the volumes are mounted. In the unload script, the secondary IP address is removed before the pool is deactivated.

The new sequence improves the handling of client reconnects because it leverages the clients' auto-reconnect mechanisms. With the previous order, clients might attempt to connect to the IP address before the data is ready or after the data is unavailable, which results in an `Object Not Found` error. Some clients might automatically try again to connect, but some do not. Thus, it is more efficient to add the IP address after data is available and remove it before the data is not available.

Newly created pool cluster resources use the following sequence for commands in a load script. The order is reversed in an unload script.

NSS

[NFS] (If NFS is used, you manually add the command here.)

Secondary IP address

NCP

[AFP]

[CIFS]

Existing scripts are not modified during a cluster upgrade. We recommend that you modify the command sequence accordingly in your existing load scripts and unload scripts for pool cluster resources.

1.3.18 Novell Linux Volume Manager

Novell Linux Volume Manager (NLVM) supports OES 11 SP1 file systems running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. For information about NLVM commands and usage, see the *OES 11 SP1: NLVM Reference* (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/bookinfo.html).

In addition to bug fixes, the following changes and enhancements were made in the OES 11 SP1 release:

General

- ♦ **Sizes:** The following enhancements are available for the `size` option:
 - ♦ The default multiplier for sizes was changed from M (megabytes) to G (gigabytes). If no multiplier is provided, the value is assumed to be in gigabytes. For example:

```
size=20 (20 gigabytes is used)
```
 - ♦ Use the `T` multiplier to specify sizes in terabytes (TB).
 - ♦ All sizes can be entered as whole numbers or with fractional parts such as 200.45G and 3.98T.
- ♦ **Multiple Devices:** You can specify multiple devices for the following commands:
 - ♦ **Init:** You can specify multiple devices to be initialized at the same time. Each device is formatted with the same specified partitioning scheme and share state.
 - ♦ **Share:** You can specify multiple devices to be shared at the same time.
 - ♦ **Unshare:** You can specify multiple devices to be unshared at the same time.
- ♦ **Multiple Device and Size Instances:** You can specify multiple device and size instances for the following commands. Each device entry must have a corresponding size entry.
 - ♦ **Create Pool:** You can specify multiple device and size instances to be used for a new pool.
 - ♦ **Expand Pool:** You can specify multiple device and size instances to be added to an existing pool.

- ♦ **Confirmation Prompt:** You are automatically prompted to confirm actions for certain commands that destroy data, such as when you initialize a device or delete Linux POSIX volumes, pool moves, partitions, pools, RAID, RAID segments, snapshots, and NSS volumes.
- ♦ **No Prompt:** The `--no-prompt` (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/nlvmlmopt.html#nlvmopt_noprompt) NLVM option can be used with certain commands to prevent a confirmation message from being displayed, such as when you initialize a device or delete Linux POSIX volumes, pool moves, partitions, pools, RAID, RAID segments, snapshots, and NSS volumes.

Linux Volumes

- ♦ **Create Linux Volume:** The following enhancements were made for the `nlvm create linux volume` (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/create_lxvol.html) command:
 - ♦ **Btrfs:** Support was added for the Btrfs file system. The Btrfs file system is now available as an alternative to other supported file systems (Ext2, Ext3, Reiserfs, and XFS) when you create a Linux volume. The `btrfsprogs` package is required. You can use NSSMU or NLVM to manage the Btrfs volumes as you would manage other Linux data volumes. Btrfs volumes can also be configured for NCP file access and for clustering with Novell Cluster Services.
 - ♦ **NCP option:** The `ncp` option for the `nlvm create linux volume` command can be used to enable the Linux POSIX file system on the volume to be accessed with the NetWare Core Protocol (NCP).

When you enable NCP for a Linux volume, an NCP volume of the same name (using all capital letters) is created. An NCP share is created at the root of the Linux volume. For clustered LVM volumes, the NCP Virtual Server object is automatically created and the NCP mount, dismount, and status commands are added to scripts for the LVM volume group cluster resource.
- ♦ **List Linux Volumes:** The `nlvm list linux volumes` (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/list_lxvol.html) command displays NCP if the Linux volume is enabled for NCP.

NSS Pools and Volumes

- ♦ **Create Pool:** The following enhancements were made for the `nlvm create pool` (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/create_pool.html) command:
 - ♦ **Device and Size:** You can specify multiple device and size instances to be used for a new pool. Each device entry must have a corresponding size entry.
 - ♦ **CIFS Virtual Server Name:** When creating a cluster enabled NSS pool, the default CIFS virtual server name is based on the NCP virtual server name.
- ♦ **Expand Pool:** The `nlvm expand pool` (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/expand_pool.html) command allows you to specify multiple device and size instances to be added to an existing pool. Each device entry must have a corresponding size entry.
- ♦ **List Move:** The following enhancements have been made to the `nlvm list move` (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/list_move.html) command:
 - ♦ You can alternatively specify the pool name instead of the pool move name.
 - ♦ The display includes the names of the devices that are being used in the move with the `from` parameter and `to` parameter.

- ♦ The concept of *move blocks* has been renamed as *regions*.
- ♦ The `complete` parameter (formerly the `percentage` parameter) displays the number of regions moved so far and the percentage of regions moved so far.
- ♦ **Delete Move:** The following enhancements were made for the `nlvm delete move` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/delete_move.html) command:
 - ♦ You can alternatively specify the pool name instead of the pool move name.
 - ♦ The `abort` option has been deprecated.

The `nlvm delete move` command deletes the move request, returns the pool to its original location, and removes the new location. You can delete the move at any time while the move is in progress, even if it is pending only the `nlvm complete move` command to be finalized.
- ♦ **Rename Volume:** You can use the `nlvm rename volume` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/rename_volume.html) command to rename a specified NSS volume. This option is new.

1.3.19 Novell Remote Manager

Novell Remote Manager supports OES 11 SP1 running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, the following enhancement is available:

NCP Server Plug-In: NCP Trustee Report

Under *Manage NCP Services*, the new *View Trustee Reports* option opens the NCP Trustee Reports page where you can generate a trustee report for a specified NSS volume. You can display the last trustee report in the web browser, or send the report to the email addresses that you have preconfigured for Novell Remote Manager. The trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume. For information, see “[Generating and Viewing NCP Trustee Reports for NSS Volumes](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/trustee_reports.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/trustee_reports.html) in the *OES 11 SP1: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

1.3.20 Novell Samba

Novell Samba file services now run on the SLES 11 SP3 platform as part of OES 11 SP1.

1.3.21 Novell Storage Services

Novell Storage Services in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, NSS provides the following enhancements and behavior changes in the OES 11 SP1 release:

Support for Managing Btrfs Volumes Using NSSMU and NLVM

- ♦ Support was added for the Btrfs file system. The Btrfs file system is now available as an alternative to other supported file systems (Ext2, Ext3, ReiserFs, and XFS) when you create a Linux volume. The `btrfsprogs` package is required. You can use NSSMU or NLVM to manage the Btrfs volumes as you would manage other Linux data volumes. Btrfs volumes can also be

configured for NCP file access and for clustering with Novell Cluster Services. For more information, see “[Overview of Linux POSIX File Systems](#)” in the [OES 11 SP2: Linux POSIX Volume Administration Guide](#).

- ♦ The NCP option for the NSSMU or `nlvm create linux volume` command can be used to enable the Linux POSIX file system on the volume to be accessed with the NetWare Core Protocol (NCP).

nssquota

- ♦ The `clear` option is introduced to remove the user quota, directory quota, and volume quota restriction.
- ♦ The `nssquota` utility now supports Volume quota. You can use this utility to set, get, or clear the volume quota on NSS volumes.

For more information, see [nssquota utility](#) in the [OES 11 SP1: NSS File System Administration Guide for Linux](#).

metamig

`metamig` can restore trustee information gathered by `TRUSTEE.NLM`. For more information, see [metamig](#) in the [OES 11 SP1: NSS File System Administration Guide for Linux](#).

nssAdminInstall

`--delete` command is introduced to delete the existing NSS Admin User from eDirectory.

Widened Partition List Panel

On the NSSMU Partitions page, the Partitions list panel has been widened to accommodate long partition names. If you widen the NSSMU display screen, it widens the Partitions list panel and allows you to see the partitions' full names.

1.3.22 NSS Auditing Client Logger (VLOG)

The NSS Auditing Client Logger (VLOG) Utility supports OES 11 SP1 running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2.

1.3.23 QuickFinder

Novell QuickFinder has been modified to run on OES 11 SP1. There are no other changes in the OES 11 SP1 release of Novell QuickFinder.

1.3.24 Storage Management Services

Novell SMS supports OES 11 SP1 services and file systems running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. There are no other changes in the OES 11 SP1 release of SMS.

1.3.25 Web Services

The web services and applications in Novell Open Enterprise Server (OES) 11 SP1 are Novell software and open source software that support SUSE Linux Enterprise Server (SLES) 11 Service Pack 2 (SP2).

PHP 5.3

The PHP 5.3 package is available in SLES 11 SP2.

PHP 5.2 Is Deprecated

The PHP 5.2 is still available, but is deprecated in SLES 11 SP2.

1.4 What's New or Changed in OES 11

Novell Open Enterprise Server 11 addresses the number one customer request: support for Open Enterprise Server with SUSE Linux Enterprise Server 11.

Product-level changes include the following:

- ♦ **Novell Linux Volume Manager:** NLVM allows for 8TB partitions, pool moves, and NSS partitions on the same disk as system partitions.
- ♦ **Seamless upgrades and migrations:** Upgrade to OES 11 from OES 2.
- ♦ **SLES 11:** OES 11 services run on a SLES 11 SP1 64-bit base. Most of them also run as 64-bit applications. The exceptions are iManager, Storage Management Services (SMS), and Novell Remote Manager (NRM).
- ♦ **Updated third-party support:** Latest hardware and third-party vendor support on the Linux Platform
- ♦ **Agile feature-delivery support:** The new foundation supports agile delivery of new features.

Service-specific changes are summarized in the following sections.

- ♦ [Section 1.4.1, "AFP," on page 64](#)
- ♦ [Section 1.4.2, "Archive and Version Services," on page 64](#)
- ♦ [Section 1.4.3, "CIFS," on page 64](#)
- ♦ [Section 1.4.4, "Distributed File Services \(DFS\)," on page 65](#)
- ♦ [Section 1.4.5, "DNS and DHCP," on page 65](#)
- ♦ [Section 1.4.6, "Domain Services for Windows," on page 66](#)
- ♦ [Section 1.4.7, "Dynamic Storage Technology," on page 66](#)
- ♦ [Section 1.4.8, "File Systems and Storage," on page 66](#)
- ♦ [Section 1.4.9, "Install," on page 68](#)
- ♦ [Section 1.4.10, "iPrint," on page 68](#)
- ♦ [Section 1.4.11, "Linux POSIX Volumes," on page 69](#)
- ♦ [Section 1.4.12, "Linux User Management," on page 69](#)
- ♦ [Section 1.4.13, "Migration Tool," on page 69](#)
- ♦ [Section 1.4.14, "NCP Server," on page 70](#)

- [Section 1.4.15, “NetStorage,” on page 70](#)
- [Section 1.4.16, “Novell Cluster Services 2.0,” on page 70](#)
- [Section 1.4.17, “Novell Linux Volume Manager,” on page 73](#)
- [Section 1.4.18, “Novell Remote Manager,” on page 74](#)
- [Section 1.4.19, “Novell Samba,” on page 77](#)
- [Section 1.4.20, “Novell Storage Services,” on page 77](#)
- [Section 1.4.21, “NSS Auditing Client Logger \(VLOG\) Utility,” on page 78](#)
- [Section 1.4.22, “QuickFinder,” on page 79](#)
- [Section 1.4.23, “Storage Management Services \(SMS\),” on page 79](#)
- [Section 1.4.24, “Web Services,” on page 79](#)

Service-specific changes are summarized in the following sections.

1.4.1 AFP

Mac clients(10.5.x or later versions) can authenticate to AFP server using DHX2 authentication mechanism.

1.4.2 Archive and Version Services

The Archive and Version Services service has been modified to run on OES 11. There are no other changes in the OES 11 release of Archive and Version Services.

1.4.3 CIFS

This section describes enhancements and changes to Novell CIFS for Novell Open Enterprise Server (OES) 11.

Detection of Cluster Resources/Volumes/Shares upon CIFS Restart

It is now possible to restart CIFS service in a cluster setup when cluster resources are active.

Monitoring Running Status of CIFS Server

You can now use the monitor command with the `rcnovell-cifs` script to check the CIFS server status. When `rcnovell-cifs monitor` is invoked, it returns the status of CIFS if it is already running otherwise (dead/not running) it starts a new instance and returns the status. For more information, see [Configuring CIFS with Novell Cluster Services for an NSS File System](#) in the [OES 11: Novell CIFS for Linux Administration Guide](#).

Large Number of Open Files Support

Novell CIFS will now be able to increase the file id pool size from 65k to 600k. In addition, you can also dump file handle statistics and directory cache statistics. For more information, see [“Enabling CIFS File Id Pool”](#) and [“Dumping File Handle Statistics”](#) in the [OES 11 SP1: Novell CIFS for Linux Administration Guide](#).

Blocking Invalid User Authentication Requests

Novell CIFS will now be able to cache the invalid user logins for a specific timeout period. Further authentication requests from the same user name will be ignored based on the configured timeout period. For more information, see “[Enabling Invalid User Caching](#)” in the [OES 11 SP1: Novell CIFS for Linux Administration Guide](#).

1.4.4 Distributed File Services (DFS)

The Novell Distributed File Services in OES 11 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP1. In addition to bug fixes, OES 11 provides the following enhancements and changes for file systems management:

Setting the [Public] Trustee for a Distributed File Services Junction in iManager

The Distributed File Services plug-in for iManager was modified to allow the [Public] trustee to be selected as a trustee of a junction.

1.4.5 DNS and DHCP

Novell Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services have been modified to support Novell Open Enterprise Server 11. In addition, the following enhancements have been added:

What’s New in DHCP

- ♦ **Starting or Stopping a DHCP Server:** A DHCP server can be remotely started or stopped by using the Java Console. For more information, refer to “[Starting or Stopping a DHCP Server](#)” (http://www.novell.com/documentation/oes11/ntwk_dnshcp_lx/?page=/documentation/oes11/ntwk_dnshcp_lx/data/bclypg6.html) in the *OES 11: Novell DNS/DHCP Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/ntwk_dnshcp_lx/index.html?page=/documentation/oes11/ntwk_dnshcp_lx/data/bookinfo.html#bookinfo).
- ♦ **IP Address Utilization:** IP address utilization of a pool can now be determined. For more information, refer to “[To determine the utilization of the IP addresses of a pool](#)” (http://www.novell.com/documentation/oes11/ntwk_dnshcp_lx/index.html?page=/documentation/oes11/ntwk_dnshcp_lx/data/bclypg6.html#bun23lh) in the *OES 11: Novell DNS/DHCP Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/ntwk_dnshcp_lx/index.html?page=/documentation/oes11/ntwk_dnshcp_lx/data/bookinfo.html#bookinfo).
- ♦ **iManager Plug-in Support:** iManager plug-in support for DHCP is no longer available. DHCP services can be managed only by using the Java Console.

What’s New in DNS

- ♦ **iManager Plug-in Support:** iManager plug-in support for DNS is no longer available. DNS services can be managed only by using the Java Console.

1.4.6 Domain Services for Windows

Novell Domain Services for Windows (DSfW) service was modified to support Novell Open Enterprise Server 11. In addition, the following enhancements are added:

- ♦ **Samba Package:** The base Samba package and its related rpm's are replaced by novell-oes-samba.

1.4.7 Dynamic Storage Technology

Novell Dynamic Storage Technology was modified to support Novell Open Enterprise Server 11. In addition to bug fixes, the following enhancements were added since the OES 2 release:

- ♦ **Include/Exclude Folders:** The Subdirectory Restrictions filter allows you to specify multiple paths to include or exclude in a policy when it runs. You can specify either included paths or excluded paths in a given policy, but not both. For information, see “[Subdirectory Restrictions](http://www.novell.com/documentation/oes11/stor_dst_lx/data/bb8ubn2.html#bb8udwu)” (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bb8ubn2.html#bb8udwu) in the *OES 11: Dynamic Storage Technology Administration Guide* (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bookinfo.html).
- ♦ **Search Pattern:** The Search Pattern filter allows you to specify multiple file extensions for a given policy. For information, see “[Search Pattern](http://www.novell.com/documentation/oes11/stor_dst_lx/data/bb8ubn2.html#bb8udkh)” (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bb8ubn2.html#bb8udkh) in the *OES 11: Dynamic Storage Technology Administration Guide* (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bookinfo.html).
- ♦ **Novell CIFS:** Novell CIFS supports the merged view of Dynamic Storage Technology volumes that are configured with NSS volumes. See “[Novell CIFS](http://www.novell.com/documentation/oes11/stor_dst_lx/data/bsrzg7.html#bss0cs9)” (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bsrzg7.html#bss0cs9) in the *OES 11: Dynamic Storage Technology Administration Guide* (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bookinfo.html).
- ♦ **Encrypted NSS Volumes:** You can use encrypted NSS volumes in a DST shadow volume. See “[Using NSS Encrypted Volumes in a DST Shadow Volume](http://www.novell.com/documentation/oes11/stor_dst_lx/data/bsrky2b.html)” (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bsrky2b.html) in the *OES 11: Dynamic Storage Technology Administration Guide* (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bookinfo.html).
- ♦ **Stop a Running Policy:** The Stop a Running Policy option allows you to stop all currently running policies, or to stop an individual running policy. See “[Stopping a Running Policy](http://www.novell.com/documentation/oes11/stor_dst_lx/data/bovhz4x.html)” (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bovhz4x.html) in the *OES 11: Dynamic Storage Technology Administration Guide* (http://www.novell.com/documentation/oes11/stor_dst_lx/data/bookinfo.html).

1.4.8 File Systems and Storage

- ♦ **EVMS:** The Enterprise Volume Management System (EVMS) is deprecated in SUSE Linux Enterprise Server 11.
- ♦ **Novell Linux Volume Manager:** The Novell Linux Volume Manager (NLVM) replaces EVMS for Novell Open Enterprise Server (OES) 11. It provides the interface for working with Novell Storage Services (NSS) in OES 11. The NLVM libraries are used by the NSSMU and storage-related iManager tools. The NLVM CLI interface also provides command line instructions for creating Linux POSIX file systems, Linux Logical Volume Manager (LVM) volume groups and logical volumes, and clustered LVM volume groups. For information about NLVM commands, see the *OES 11: NLVM Reference* (http://www.novell.com/documentation/oes11/stor_nlvmlx/data/bookinfo.html).

- ♦ **Shared Linux POSIX File Systems:** Novell Cluster Services uses the clustered Linux Volume Manager (LVM) volume groups and logical volumes for clustering Linux POSIX file systems. This replaces the EVMS Cluster Segment Manager (CSM). The cluster resource templates that use shared Linux POSIX file systems have been modified to use LVM volume groups. For information, see “[Upgrading and Managing Cluster Resources for Linux POSIX Volumes with CSM Containers](http://www.novell.com/documentation/oes11/clus_admin_lx/data/ncsshvollxlv.html)” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/ncsshvollxlv.html) in the *OES 11: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).
- ♦ **CSMPort Utility:** The Novell Cluster Services CSM Import/Export (CSMPort) utility provides support in OES 11 clusters for importing and managing Linux POSIX volume cluster resources that were created with Cluster Segment Manager containers on OES 2 SP3 and earlier servers. For information, see “[Configuring and Managing Cluster Resources for LVM Volume Groups](http://www.novell.com/documentation/oes11/clus_admin_lx/data/ncsshvollx.html)” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/ncsshvollx.html) in the *OES 11: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).
- ♦ **Files and Folders Plug-In to iManager:** The Files and Folders plug-in to iManager has been modified to support OES 11. The following enhancements are available:
 - ♦ Move a file or folder
 - ♦ Rename a file or folder
 - ♦ Delete a non-empty folder
 - ♦ Specify quotas in kilobytes, megabytes, or gigabytes

For information, see “[Managing Files and Folders](http://www.novell.com/documentation/oes11/stor_filesys_lx/data/bs3fn88.html)” (http://www.novell.com/documentation/oes11/stor_filesys_lx/data/bs3fn88.html) in the *OES 11: File Systems Management Guide*. (http://www.novell.com/documentation/oes11/stor_filesys_lx/data/bookinfo.html).
- ♦ **Novell Client 2 SP1 for Windows:** The Novell Client 2 SP1 for Windows added support for Windows 7. See the *Novell Client 2 SP1 for Windows* (http://www.novell.com/documentation/vista_client/).
- ♦ **Novell Client for SUSE Linux Enterprise 11 SP1:** The Novell Client for Linux was modified to support OES 11 and SUSE Linux Enterprise 11 SP1 desktops and servers. See the *Novell Client for SUSE Linux Enterprise 11 SP1* (http://www.novell.com/documentation/linux_client/linuxclient_sle11sp1_admin/data/index.html).
- ♦ **Novell AFP:** Novell AFP has been modified to support NSS volumes on OES 11. See the *OES 11: Novell AFP for Linux Administration Guide* (http://www.novell.com/documentation/oes11/file_afp_lx/data/h9izvdy.html).
- ♦ **Novell CIFS:** Novell CIFS has been modified to support NSS volumes on OES 11 servers. It also supports the merged view of Dynamic Storage Technology volumes that are configured with NSS volumes. See the *OES 11: Novell CIFS for Linux Administration Guide* (http://www.novell.com/documentation/oes11/file_cifs_lx/data/front.html).
- ♦ **Novell Samba:** Novell Samba has been modified to support NSS volumes and Linux POSIX volumes on OES 11. See the *Samba Administration Guide* (http://www.novell.com/documentation/oes11/file_samba_cifs_lx/data/bookinfo.html).
- ♦ **Novell FTP:** Novell provides integration of the native Linux Pure-FTPd with eDirectory to provide authenticated and anonymous access to FTP sites on OES 11 servers. See “[Novell FTP \(Pure-FTPd\) and OES 11](http://www.novell.com/documentation/oes11/oes_implement_lx/data/bn0rvzm.html)” (http://www.novell.com/documentation/oes11/oes_implement_lx/data/bn0rvzm.html) in the *OES 11: Planning and Implementation Guide* (http://www.novell.com/documentation/oes11/oes_implement_lx/data/bookinfo.html).
- ♦ **Domain Services for Windows:** Domain Services for Windows (DSfW) has been modified to support NSS volumes on OES 11. See the *OES 11: Domain Services for Windows Administration Guide* (http://www.novell.com/documentation/oes11/acc_dsfw_lx/data/bookinfo.html).

1.4.9 Install

- ♦ Novell Linux Volume Manager (NLVM) replaces the Enterprise Volume Management System (EVMS).
- ♦ Rug and Zen-updater are now replaced with zypper and PackageKit.
- ♦ OpenWBEM has now been replaced with Small Footprint CIM Broker (SFCB) as the Web-Based Enterprise Management system.

1.4.10 iPrint

This section describes enhancements and changes to Novell iPrint for Novell Open Enterprise Server (OES) 11 SP1.

- ♦ Novell iPrint now runs on the OES 11 SP1 platform. Novell iPrint supports the SLES 11 base completely, along with its enhancements and hardware for its lifecycle.
- ♦ Novell secure printing and iPrint Client Management features can now function without the Novell Client component. Users working on Windows / Active Directory environments now can have ICM and shared login abilities with or without the Novell Client.
- ♦ Print driver transfer methods in iPrint Migration have been improved, and dependencies on other stacks have been reduced to increase reliability and robustness. iPrint Migration has also been enhanced in areas such as Print Driver transfer and Driver Platform selection.
- ♦ The iprintman utility now runs on Windows, Mac, and Linux clients, and has been rewritten to use the Java IPP libraries for performing various operations.

NOTE: This feature is under development and might not function as expected in all cases. Novell plans to complete development in a future OES release.

Novell iPrint in OES 11 SP1 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, iPrint provides the following enhancements and behavior changes in the OES 11 SP1 release:

You can download iPrint Clients from the OES 11 SP1 welcome page or from the iPrint Printer List web page. You can download the latest version of the iPrint Client from the [iPrint Client download site](#).

iPrint Windows Client

A new version of the iPrint Client 5.94 is available for Windows XP/Vista/Win 7/Win 8/Win 8.1.

iPrint Macintosh Client

A new version of the iPrint Client for Macintosh 5.74 is available for Mac OS X 10.7 and later. The 5.74 client includes support for Mac OS X 10.9 (Mavericks).

Direct Print Accounting for iPrint Macintosh Client

You can now perform accounting operations for iPrint Direct Printers on the iPrint Mac Client 5.74.

1.4.11 Linux POSIX Volumes

The NLVM and NSSMU management tools support Linux POSIX volumes on OES 11 running on 64-bit SUSE Linux Enterprise Server (SLES) 11 Service Pack (SP) 1.

Creating Linux Volumes with NSSMU and NLVM Commands

For Novell Open Enterprise Server (OES) 11 servers, the Novell Storage Services Management Utility (NSSMU) and the Novell Linux Volume Manager (NLVM) commands allow you to create, mount, and delete the following Linux POSIX storage objects:

- ♦ Linux POSIX volumes (non-LVM volumes)
- ♦ Linux Logical Volume Manager 2 (LVM2) volume groups and LVM logical volumes
- ♦ Shared Linux Clustered LVM (cLVM) volume groups and logical volumes that are cluster-enabled with Novell Cluster Services

Linux Volume Support in SLES 11 SP1

For information about Linux volume support changes in SUSE Linux Enterprise Server 11 SP1, see “What’s New in SLES 11 SP1” (http://www.suse.com/documentation/sles11/stor_admin/data/bndgyod.html) in the *SUSE Linux Enterprise Server 11 Storage Administration Guide* (http://www.suse.com/documentation/sles11/stor_admin/data/bookinfo.html).

Linux Volume Support in SLES 11

For information about Linux volume support changes in SUSE Linux Enterprise Server 11, see “What’s New in SLES 11” (http://www.suse.com/documentation/sles11/stor_admin/data/bndgyoe.html) in the *SUSE Linux Enterprise Server 11 Storage Administration Guide* (http://www.suse.com/documentation/sles11/stor_admin/data/bookinfo.html).

1.4.12 Linux User Management

The LUM service has been modified to run on OES 11. There are no feature changes in the OES 11 release of LUM.

1.4.13 Migration Tool

NOTE: Starting with OES 11, migration of data from Windows to OES is no longer supported by the Migration Tool.

The Migration Tool in OES 11 has been modified to run on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP1. In addition to bug fixes, the Migration Tool provides the following enhancements and behavior changes:

Supervisory Rights for Container Admin

To perform transfer id using container admin, the container admin must have supervisory rights on the container the admin exists.

Common Proxy Repair Script

A new proxy script `mignwproxy.sh` has been added to repair common proxy on an OES 11 server.

1.4.14 NCP Server

This section describes enhancements to the Novell NCP Server for Novell Open Enterprise Server (OES) 11.

- `LOCK_RANGE_MASK` parameter introduced to acquire a lock above the `0x7fffffffffff` region limitation set by Linux files system. For more information about `LOCK_RANGE_MASK`, see [Locks Management for File Access on NCP Server](#) in the [OES 11: NCP Server for Linux Administration Guide](#).
- Included `AUDITING_SUPPORT` parameter to indicate whether auditing support is enabled for NCP.
- Included `LOG_LOCK_STATISTIC` parameter that will display a message in the `ncpserv.log` file if the NCP volume lock is held for more than the configured time.
- An upgrade to NetIQ eDirectory 8.8 SP7 is available in the April 2013 Scheduled Maintenance for OES 11. For information about the eDirectory upgrade, see [TID 7011599](#) (<http://www.novell.com/support/kb/doc.php?id=7011599>) in the Novell Knowledgebase.

There will be no further eDirectory 8.8 SP6 patches for the OES platform. Previous patches for NetIQ eDirectory 8.8 SP6 are available on [Novell Patch Finder](#) (<http://download.novell.com/patch/finder/#familyId=112&productId=29503>).

1.4.15 NetStorage

NetStorage has been modified to run on OES 11. There are no other changes in the OES 11 release of NetStorage.

1.4.16 Novell Cluster Services 2.0

Novell Cluster Services 2.0 supports OES 11 services and file systems running on 64-bit SUSE Linux Enterprise Server 11 SP1. In addition to bug fixes and performance improvements, it includes the following changes and enhancements:

EVMS Is Deprecated

The Enterprise Volume Management System (EVMS) has been deprecated in SLES 11, and is also deprecated in OES 11. Novell Linux Volume Manager (NLVM) replaces EVMS for managing NetWare partitions under Novell Storage Services (NSS) pools.

NSS Pool Cluster Resources

Novell Cluster Services for OES 11 supports NSS pools that are created on OES 11, OES 2 SP3 and earlier, and NetWare 6.5 SP8.

A new NSS capability supports the GPT partitioning scheme. This allows you to create NSS pools up to 8 TB (terabytes) in size on a single device. Pools created with GPT-partitioned devices are not backward compatible with prior releases of OES and NetWare. The DOS partitioning scheme is also available and supports devices up to 2 TB in size.

The NSS management tools use the Novell Linux Volume Manager instead of the Enterprise Volume Management System that is used in previous OES releases. The Storage plug-in to iManager and NSSMU can be used to create pool cluster resources. You can also use NLVM commands to create shared pools and volumes at a command prompt or in scripts.

During a rolling cluster upgrade, the existing NSS pool cluster resources can be cluster migrated to any node in the mixed-node cluster. However, you must not create new NSS pools on OES 11 nodes while you are upgrading the cluster from OES 2 to OES 11. For information, see “NSS Pools” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/btvuil3.html#btvv2vn) in the *OES 11: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

LVM Volume Group Cluster Resources

Novell Cluster Services uses a Linux Logical Volume Manager (LVM) volume group and logical volume to create the cluster resource for shared Linux POSIX file systems (such as Ext2, Ext3, ReiserFS, and XFS) on OES 11.

The NSS Management Utility (NSSMU) and Novell Linux Volume Manager (NLVM) commands support creating Linux POSIX file systems and Linux Logical Volume Manager (LVM) volume groups and logical volumes. The tools support both the DOS and the GPT partitioning schemes. The DOS partitioning scheme supports devices up to 2 TB in size. The GPT partitioning scheme supports devices up to 8 zettabytes (ZB, or one billion terabytes). Your actual device size is limited by your storage hardware and the size recognized by your target file system. For information about maximum file system sizes on Linux, see the *SUSE Linux Enterprise Server Technical Information: File System Support* (<http://www.suse.com/products/server/technical-information/#FileSystem>).

You can create a Linux volume group cluster resource by using NSSMU and Novell Linux Volume Manager commands. You can also use native Linux LVM2 commands to create a shared LVM volume group, and then create a resource by using the generic file system (Generic_FS) resource template in iManager, or by using other application resource templates that need shared Linux POSIX file systems. For information, see “Configuring and Managing Cluster Resources for an LVM volume groups” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/ncsshvollxlv.html) in the *OES 11: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Linux POSIX Cluster Resources with CSM Containers

On OES 2, Linux POSIX volume cluster resources use a Cluster Segment Manager (CSM) container on devices that are managed by EVMS. Because EVMS has been deprecated in OES 11, you must modify the scripts and cluster settings so that the CSM containers can run on OES 11 clusters. You cannot create new cluster resources with CSM containers on OES 11 clusters. For information, see “Upgrading and Managing Cluster Resources for Linux POSIX Volumes with CSM Containers” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/ncsshvollx.html) in the *OES 11: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

CSMPORT Utility

The Cluster Segment Manager Import/Export (CSMPORT, `/opt/novell/ncs/bin/csmport`) utility allows you to import and use Linux POSIX volume cluster resources that use CSM containers in OES 11 clusters. After the resource is configured to run on OES 11, you must configure its Preferred Nodes list to ensure that it can fail over only to OES 11 nodes in the mixed-node cluster. For information about CSMPORT, see “Cluster Segment Manager Import/Export (csmport) Utility” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

www.novell.com/documentation/oes11/clus_admin_lx/data/csmport.html) in the *OES 11: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Cluster Resource Templates Use LVM Volume Groups for Shared Data Locations

The following cluster resource templates have been modified to use LVM volume groups and logical volumes for cluster resources that share data on Linux POSIX file systems. Previously, the templates used the EVMS Cluster Segment Manager container and Linux POSIX volumes.

OES 11 Application	Cluster Resource Template
Archive and Version Services	AV_Template
DHCP	DHCP_Template (for an NSS pool or for an LVM volume group)
Linux POSIX file system	Generic_FS_Template
iFolder	iFolder_Template (for an NSS pool or for an LVM volume group)
iPrint	IPrint_Template (for an NSS pool or for an LVM volume group)
MySQL 5.x	MySQL_Template
Samba	Samba_Template
Xen virtual machine	Xen_Template

The `DNS_Template` uses an NSS file system. The `Generic_IP_Service` and `XenLive_Template` templates do not use a shared data location.

The monitor scripts for resources that use a Linux volume group were modified to check the status of the LVM logical volume in addition to the file system and the IP address.

Ext3 is the default file system type used in the scripts. The Ext2, Ext3, ReiserFS, and XFS file systems have been tested and are fully supported.

Virtual Server Name for Cluster Resources

The default virtual server name for cluster resources now uses hyphens instead of underscores, such as `MYCLUS-MYPOOL-SERVER`. The suggested name is compliant with the Internet Engineering Task Force (IETF) RFC 1123 standard that allows host names to contain only letters, digits, and hyphens. Underscores can still be used in the virtual server name if your network environment supports them.

CIFS Monitor Command in the NSS Monitor Script

Novell CIFS provides a `monitor` command option in OES 11 that provides a restart capability if the `cifs` daemon goes down. If you create a new pool cluster resource with CIFS enabled as an advertising protocol, the following line is added to the resource's monitor script:

```
exit_on_error rcnovell-cifs monitor
```


Previously, the `CIFS status` command was used. You can replace it with the `monitor` command for existing pool cluster resources to take advantage of the CIFS restart capability. For information, see “Configuring a Monitor Script for the Shared NSS Pool” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bffzpj5.html) in the *OES 11: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Assigned Nodes List

If you attempt to online or migrate a cluster resource to a node that is not in the resource's Assigned Nodes list, the resource stays offline or is not migrated. This change makes the command behavior consistent with the online and migrate options in the Cluster plug-in in iManager. The node that you specify must be running in the cluster and must also be in the resource's Assigned Nodes list.

Previously, if the specified node was not a preferred node, the `cluster online` and `cluster migrate` commands brought the resource online on a node in its Assigned Nodes list.

Order of Servers in the LDAP Server List

When you configure the cluster node in YaST, the LDAP server list is created. The default order is to list the local LDAP server first and others second. In previous OES releases, the default order was based on the IP address.

You cannot change the order of LDAP servers in the list during the cluster node configuration in YaST, but you can modify it later by running the `/opt/novell/ncs/install/ncs_install.py` script. For information, see “Changing the Administrator Credentials or LDAP Server IP Address for a Cluster” (http://www.novell.com/documentation/oes11/clus_admin_lx/data/clus_moving.html#bgjnbnv) in the *OES 11: Novell Cluster Services for Linux Administration Guide* (http://www.novell.com/documentation/oes11/clus_admin_lx/data/bookinfo.html).

Cascade Failover Prevention

Novell Cluster Services added the Cascade Failover Prevention function that detects if a node has failed because of a bad cluster resource and prevents that bad resource from failing over to other servers in the cluster. This function was previously available on NetWare, but not on Linux.

1.4.17 Novell Linux Volume Manager

The Novell Linux Volume Manager (NLVM) replaces the Enterprise Volume Management System (EVMS) for the management of Novell Storage Services (NSS) storage objects in Novell Open Enterprise Server (OES) 11. For information about NLVM commands and usage, see the *OES 11: NLVM Reference* (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/bookinfo.html).

NLVM provides the same media management functionality that was used by NSS in EVMS, and makes the following enhancements for OES 11:

- ♦ **Initialize a Device with a DOS or GPT Partitioning Scheme:** The `nlvm init` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/init_device.html) command allows you to specify partitioning scheme format of MS-DOS (the default) or GPT. MS-DOS has a 2 TB size limit. Devices of any size can be configured with GPT.
- ♦ **8 TB Device Size for Pools:** The `nlvm create pool` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/create_pool.html) command allows you to use devices up to 8 TB in size. The maximum pool size is 8 TB. Previously, pools could use devices of up to 2 TB in size.

- ♦ **Move Pool:** The `nlvm move` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/move_pool.html) command allows you to move an NSS pool from one location to a new location on the same system.

See also the related commands:

- ♦ `nlvm complete move` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/complete_move.html)
- ♦ `nlvm delete move` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/delete_move.html)
- ♦ `nlvm list move` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/list_move.html)
- ♦ `nlvm list moves` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/list_moves.html)
- ♦ **Rescan:** The `nlvm rescan` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/rescan.html) command performs a rescan of the storage objects (such as partitions, NSS pools, and NSS software RAID) on known devices, and creates or updates any Device Mapper device or partition objects as needed.
- ♦ **Expand Partition:** The `nlvm expand partition` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/expand_part.html) command allows you to expand a partition by using free contiguous space that follows the partition.
- ♦ **Create Linux Volume:** The `nlvm create linux volume` (http://www.novell.com/documentation/oes11/stor_nlvm_lx/data/create_lxvol.html) command allows you to create a volume with a Linux POSIX file system. The volume can be created as a traditional Linux volume or as a Linux Logical Volume Manager 2 (LVM2) volume on an LVM2 volume group. If the device is shared with nodes in a Novell Cluster Services cluster, you can cluster-enable the LVM2 volume group.

1.4.18 Novell Remote Manager

Novell Remote Manager has been modified to run on Novell Open Enterprise Server 11. In addition to bug fixes, the following changes and enhancements are available:

HttpOnly Command

The `HttpOnly` configuration option is available in the Novell Remote Manager `/etc/opt/novell/httpstkd.conf` file. By default, Novell Remote Manager sets an `HttpOnly` cookie attribute that specifies that the cookie is not accessible through a script. This helps mitigate the risk of cross-site scripting. For information, see “[HttpOnly Command](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/httponly.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/httponly.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

InventoryResolveNonLumOwnerName Command

The `InventoryResolveNonLumOwnerName` configuration option is available in the Novell Remote Manager `/etc/opt/novell/httpstkd.conf` file. This allows you to choose whether the inventory of a Novell Storage Services (NSS) volume reports the names of owners as the Nobody user if their eDirectory usernames are not enabled with Linux User Management. By default, this option is set to false (not resolved) in order to give you faster performance for an inventory of files on an NSS volume. For information, see “[InventoryResolveNonLumOwnerName Command](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/inventoryresolve.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/inventoryresolve.html).

www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/bwv2pua.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

SSL Key Cipher Strength Command

You can set the cipher strength for the SSL key in the `/etc/opt/novell/httpstk.conf` file. The default allows any encryption level. A setting of High is recommended. For information, see “SSL Key Cipher Strength Command” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/budlpt0.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

VNC Consoles

The `root` user can view VNC consoles from within Novell Remote Manager. This capability requires that the `HttpOnly` security feature be disabled in the `/etc/opt/novell/httpstk.conf` file. For information, see “HttpOnly Command” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/httponly.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

General File Inventory

On the File System Listing page (*View File System > View File System Listing*), the *Inventory* link generates a *General File Inventory* report with statistics about the files stored on a selected file system path or sub-folder path. For information, see “Inventorying Directories or NCP Volumes” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/b2kl4kn.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

NCP Volume Inventory

- The *View File Systems > NCP Volume Inventory* option allows you to view a list of NCP volumes and generate inventories for them.
- The Volume Information page (*Manage NCP Services > Manage Shares*, then click the NSS volume name link), for a volume provides an *Inventory* option to generate an inventory. This provides the same output as running *View File System > General File Inventory* for Linux paths and for *View File Systems > NCP Volume Inventory* for NCP volumes.
- An inventory report is saved when you run an inventory on an NCP volume. You can view the last saved report by going to the *Manage NCP Services > Volume Inventory Reports* page and clicking the *View Last Report > Display* option for the volume. The saved report provides the same statistics as running *View File Systems > NCP Volume Inventory*. Graphics are not available in a saved report.
- You can email a saved NCP volume inventory report to addresses that are configured in the `/etc/opt/novell/httpstk.conf` file. To send the report, go to the *Manage NCP Services > Volume Inventory Reports* page and click the *Email Report > Send* option for the volume.
- In a file inventory for NSS volumes, the *File Owner Profile* reports the eDirectory identity of the file owner without requiring the users to be enabled with Linux User Management (LUM).

For information, see “Inventorying Directories or NCP Volumes” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/b2kl4kn.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Open Connections for NCP Volumes and NSS Volumes

On the *Connection Information* page (*Manage NCP Services > Manage Connections*), then select a connection link under *Connections*) for a selected connection, the *Open Files* list now links to the file and lock details for each file that is held open by a connection. For information, see “[Viewing Connections for NCP Server](http://www.novell.com/documentation/oes11/file_ncp_lx/data/ba47cgt.html)” (http://www.novell.com/documentation/oes11/file_ncp_lx/data/ba47cgt.html) in the *OES 11: NCP Server for Linux Administration Guide* (http://www.novell.com/documentation/oes11/file_ncp_lx/data/h9izvdy.html).

Salvage and Purge Deleted Files for NSS Volumes

On the *Share Information* page (*Manage NCP Services > Manage Shares*, then click the *Information* (i) icon to the left of the NSS volume name) and on the *Directory Information* page (*Manage NCP Services > Manage Shares*), then navigate to a directory of interest and click the *Directory Information* icon to the left of the directory name), the following capabilities were added for salvaging and purging deleted files for NSS volumes where the Salvage attribute is enabled:

- ♦ The *Salvageable Files* list option allows you to view a list of deleted files that are available for salvage or purge in the selected directory on an NSS volume.
- ♦ The *Purge* option allows you to permanently remove a deleted file from the file system.
- ♦ The *Salvage* option allows you to recover a deleted file.
- ♦ The *Purge all files* option allows you to permanently remove all deleted files on a selected volume.

For information, see “[Salvaging and Purging Deleted Files on an NSS Volume](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nssactions.html#nsssalvage)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nssactions.html#nsssalvage) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Create, Rename, and Delete Directories

On the *Directory Information* page (*View File System > View File System Listing*, navigate to the directory of interest, then click the *Directory Information* icon to the left of the directory name), the following capabilities were added:

- ♦ The *Delete Directory and Contents* option allows you to recursively delete a selected folder and its contents.
- ♦ The *Rename Directory* option allows you modify the name of a selected directory.
- ♦ The *Create Subdirectory* option allows you to create subdirectories in the selected directory.
- ♦ The *Create Symbolic Link* option allows you to create a symbolic link in the selected directory.

For information, see “[Viewing Details about Directories and Performing Actions on Them](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/butlqph.html#butltrr)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/butlqph.html#butltrr) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

NSS Volume Share Information

On the Share Information page (*Manage NCP Services > Manage Shares*, then click the *Information* (i) icon to the left of the NSS volume name), the following capabilities were added:

- ♦ Additional details about the volume are displayed, such as the sector size and loaded name spaces.
- ♦ For NSS volumes, the *Compression* option shows whether the Compression attribute is enabled for the volume.

NSS Volume Directory and File Listing

On an NSS volume's Directory and File Listing page (*Manage NCP Services > Manage Shares*, then click the NSS volume name link), the following capabilities were added:

- ♦ The *Text Search* option allows you to search the content of files for a specified text string.
- ♦ The *File Search* option allows you to search for a file on the selected volume.
- ♦ The *Inventory* option generates an *NCP Volume Inventory* report with statistics about the files stored on a selected volume.
- ♦ The *Upload* option allows you to upload a file to the selected volume.

For information, see “Browsing Files and Performing Actions on NSS Volumes” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nssactions.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

1.4.19 Novell Samba

- ♦ Novell Samba file services now run on the SLES 11 SP1 platform as part of OES 11.
- ♦ The Samba resource template has been updated to work with Linux Logical Volume Manager (LVM) volume groups. For information, see “Section 5.2 What's New for the Samba Template in OES 11” in the *OES 11 SP1: Novell Samba Administration Guide*.
- ♦ If Samba is running in a cluster, upgrading from OES 2 or OES 1 requires that you make special changes to the existing load, unload, and monitor scripts for Samba resources before you add OES 11 nodes to the cluster. For information, see the following sections of the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide*:
 - ♦ “Upgrading Clusters from OES 2 SP3 to OES 11 SPx”
 - ♦ “Upgrading and Managing Cluster Resources for Linux POSIX Volumes with CSM Containers”

1.4.20 Novell Storage Services

This section describes enhancements and changes to the Novell Storage Services for Novell Open Enterprise Server 11. The following features are added:

Change in the Volume Manager

Novell Linux Volume Manager (NLVM) replaces the Enterprise Volume Management System (EVMS) volume manager, which is now deprecated. For more information, see the [OES 11 NLVM Reference Guide](#) or see the `nlvm` (8) man page.

Support for Creating >2TB Partition

When you initialize a device, you can choose to use the DOS partition table scheme or the GUID Partition Table (GPT) scheme for a given device.

The DOS partition table scheme supports devices up to 2TB in size. It allows up to four partitions on a device.

The GPT partition table scheme supports device sizes up to 2⁶⁴ sectors (that is, up to 8388608 petabytes (PB) based on the 512-byte sector size). It allows up to 128 partitions per disk. Each of its disks partitions is a logical device that is identified by a unique 128-bit (16-byte) GUID.

Support for Creating Linux Volumes

Using the NSSMU and NLVM command line option, you can create Linux volumes. For more information, see [Table 9-11, Create Linux Volume](#) in the [OES 11 NLVM Reference Guide](#), the `nssmu(8)` or the `nlvm(8)` manpage.

Single Disk System Support

You can now use the system device containing the root partition also to create/manage NSS pools and volumes.

quota Utility is Renamed to nssquota

For more information, see [nssquota](#).

Moving a Pool

Using the NSSMU and NLVM command line option, you can move a pool from one location to another on the same system. For more information, see [Table 9-11, Moving a Pool](#), and the [Move](#) in the [OES 11 NLVM Reference Guide](#).

nssraid Utility

The `nssraid` utility options are soft linked to the Novell Linux Volume Manager `nlvm raid` options. You can alternatively use `nlvm raid` commands to manage NSS software RAIDS at the command line and in scripts in OES 11. `nlvm raid` commands have more options than the `nssraid` utility.

For information, see [RAID](#) in the [OES 11 NLVM Reference Guide](#) or see the `nlvm` man page.

1.4.21 NSS Auditing Client Logger (VLOG) Utility

The NSS Auditing Client Logger (VLOG) utility has been modified to run on OES 11. In addition to bug fixes, the following options were added:

- ♦ **LogFilePath:** Use this option to specify a path for the `vlog` log file. The default log file directory is `/var/log/audit`. The `vlog` file is created in the specified location.

```
[--logFilePath] FILE_PATH
```


- ♦ **MaxFileCount:** Use this option to limit the vigil auditing client's log files count. The default count is 50 files.

```
[-m, --maxFileCount] maxStreamFileCount
```

1.4.22 QuickFinder

Novell QuickFinder has been modified to run on OES 11. There are no other changes in the OES 11 release of Novell QuickFinder.

1.4.23 Storage Management Services (SMS)

Novell SMS supports OES 11 services and file systems running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP1. There are no other changes in the OES 11 release of SMS.

1.4.24 Web Services

The Web services and applications in Novell Open Enterprise Server (OES) 11 are Novell software and open source software that support SUSE Linux Enterprise Server (SLES) 11 Service Pack 1 (SP1).

1.5 Where's NetWare?

Novell Open Enterprise Server does not include NetWare. Anyone who wants to deploy NetWare in an OES 11 environment should download NetWare 6.5 SP8 from the [Novell download site \(http://download.novell.com/Download?buildid=dp1R3H1ymhk~\)](http://download.novell.com/Download?buildid=dp1R3H1ymhk~).

1.5.1 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 11 is included in this guide and in the OES 11 documentation set—especially in the *OES 11 SP2: Upgrading to OES—Best Practices Guide*.

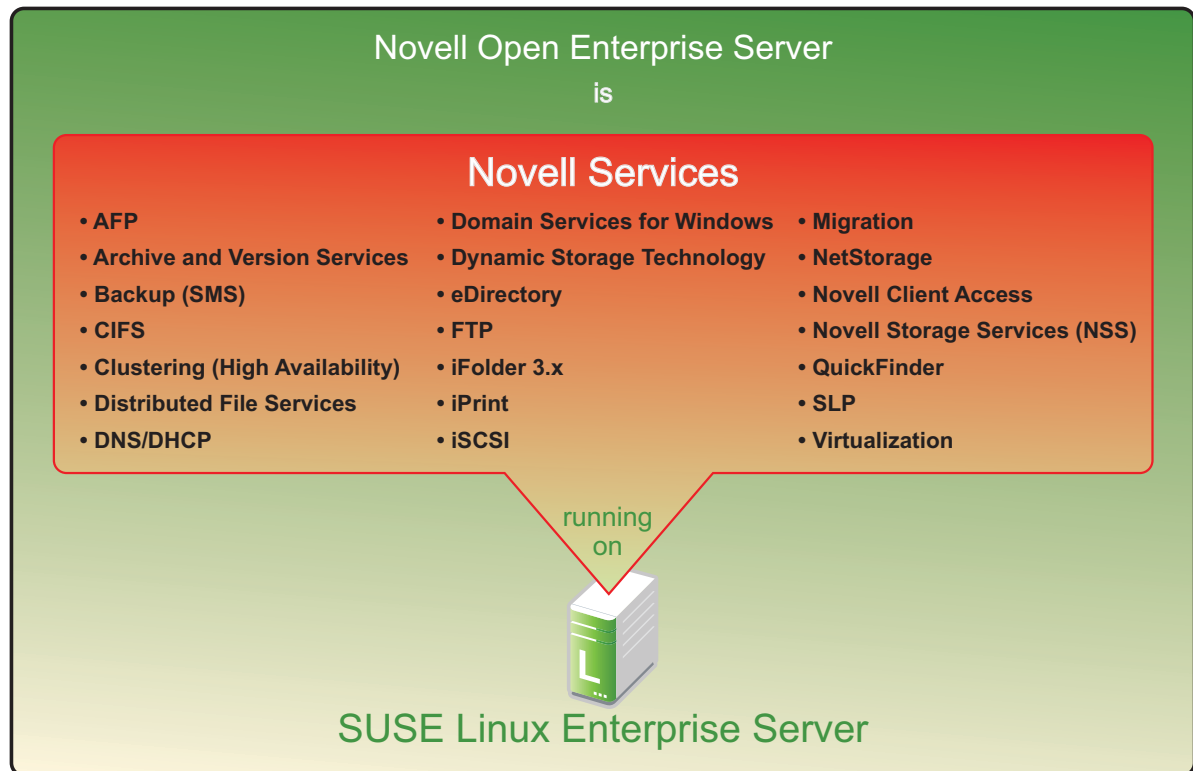
1.5.2 NetWare Documentation

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).

2 Welcome to Open Enterprise Server 11 SP2

Novell Open Enterprise Server 11 SP2 (OES 11 SP2) includes all the network services that organizations traditionally expect from Novell.

Figure 2-1 OES 11 SP2 Overview



NOTE: For a list of OES 11 SP2 services, see [Table 3-1, “Service Comparison Between NetWare 6.5 SP8 and OES 11 SP2,”](#) on page 83.

3 Planning Your OES 11 SP2 Implementation

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 11 SP2?,” on page 83](#)
- [Section 3.2, “Which Services Do I Need?,” on page 90](#)
- [Section 3.3, “Exploring OES 11 SP2 services,” on page 90](#)
- [Section 3.4, “Plan for eDirectory,” on page 90](#)
- [Section 3.5, “Prepare Your Existing eDirectory Tree for OES,” on page 91](#)
- [Section 3.6, “Identify a Purpose for Each Server,” on page 92](#)
- [Section 3.7, “Understand Server Requirements,” on page 92](#)
- [Section 3.8, “Understand User Restrictions and Linux User Management,” on page 92](#)
- [Section 3.9, “Caveats to Consider Before You Install,” on page 92](#)
- [Section 3.10, “Consider Coexistence and Migration Issues,” on page 105](#)
- [Section 3.11, “Understand Your Installation Options,” on page 106](#)

3.1 What Services Are Included in OES 11 SP2?

[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 \(http://www.novell.com/documentation/oes11\)](http://www.novell.com/documentation/oes11).

Table 3-1 Service Comparison Between NetWare 6.5 SP8 and OES 11 SP2

Service	NetWare 6.5 SP8	OES 11 SP2	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 (POSIX) 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 11 SP2	Platform Differences / Migration Issues
Apache Web Server	Yes - NetWare port of open source product	Yes - Standard Linux	<p>“Using Apache HTTP Server on OES Servers (Single Server or Cluster Nodes)” in the <i>OES 11 SP2: Web Services and Applications Guide</i>.</p> <p>Administration Instance vs. Public Instance on NetWare.</p> <p>What's Different about Apache on NetWare.</p>
Archive and Version Services (Novell)	Yes	Yes	Setup varies slightly, but there are no functional differences.
Backup (SMS) <ul style="list-style-type: none"> ♦ SMS ♦ NSS-Xattr 	Yes	Yes	<p>SMS provides backup applications with a framework to develop complete backup and restore solutions. For information, see the <i>OES 11 SP2: Storage Management Services Administration Guide for Linux</i>.</p> <p>NSS provides extended attribute handling options for NSS on Linux. For information, see “Using Extended Attributes (xAttr) Commands” in the <i>OES 11 SP2: NSS File System Administration Guide for Linux</i>.</p>
CIFS (Windows File Services)	Yes - NFAP	Yes - Novell CIFS and Novell Samba	<p>Both NFAP and Novell CIFS are Novell proprietary and tightly integrated with eDirectory and Novell Storage Services (NSS).</p> <p>Samba is an open source product distributed with SUSE Linux Enterprise Server (SLES).</p> <p>Novell Samba is enhanced by Novell with configuration settings for eDirectory LDAP authentication via Linux User Management (LUM). Novell Samba is not tightly integrated with NSS on Linux and works with any of the supported file systems.</p>
Clustering	Yes	Yes	“Comparing Novell Cluster Services for Linux and NetWare” in the <i>OES 11 SP2: Novell Cluster Services NetWare to Linux Conversion Guide</i> .
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 Btrfs, Ext3, and XFS. The VLDB command offers additional options to manage entries in the VLDB for NCP volumes.

Service	NetWare 6.5 SP8	OES 11 SP2	Platform Differences / Migration Issues
DHCP	Yes	Yes	<p>For a comparison between what is available on OES 11 SP2 and NetWare, see “DHCP Differences Between NetWare and OES 11” in the <i>OES 11 SP2: Planning and Implementation Guide</i>.</p> <p>To plan your DHCP implementations, see “Planning a DHCP Strategy” in the <i>OES 11 SP2: Novell DNS/DHCP Services for Linux Administration Guide</i> and “Planning a DHCP Strategy” in the <i>NW 6.5 SP8: Novell DNS/DHCP Services Administration Guide</i>.</p>
DNS	Yes	Yes	<p>For a comparison between what is available on OES 11 SP2 and NetWare, see “DNS Differences Between NetWare and OES 11” in the <i>OES 11 SP2: Planning and Implementation Guide</i>.</p> <p>See “Planning a DNS Strategy” in the <i>OES 11 SP2: Novell DNS/DHCP Services for Linux Administration Guide</i> and “Planning a DNS Strategy” in the <i>NW 6.5 SP8: Novell DNS/DHCP Services Administration Guide</i>.</p>
Dynamic Storage Technology	No	Yes	
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 User Application. For more information, see the User Application: Administration Guide .
FTP Server	Yes	Yes	<p>FTP file services on OES 11 SP2 servers are provided by Pure-FTPd, a free (BSD), secure, production-quality and standard-conformant FTP server. The OES implementation includes support for FTP gateway functionality as on NetWare and offers a level of integration between eDirectory and Pure-FTP that allows users to authenticate to eDirectory for FTP access to the server.</p> <p>See “Novell FTP” in the <i>OES 11 SP2: Planning and Implementation Guide</i>.</p>

Service	NetWare 6.5 SP8	OES 11 SP2	Platform Differences / Migration Issues
Health Monitoring Services	Yes	Yes	<p>In OES 11 SP2, NRM provides health monitoring via the open source monitoring tools Ganglia and Nagios. These tools do not use SFCB.</p> <p>For help with diagnosing problems using Ganglia and Nagios in OES 11 SP2, see “Diagnosing Problems Using Ganglia and Nagios (OES 11 SP2)” in the <i>OES 11 SP2: Novell Remote Manager Administration Guide</i>.</p> <p>The NRM Health Monitor tool is no longer available in OES 11 SP2 and later.</p> <p>For information about using Health Monitor in OES 11 SP1 and earlier, see “Diagnosing Problems Using Health Monitor (OES 11 SP1)” in the <i>OES 11 SP2: Novell Remote Manager Administration Guide</i>.</p>
Identity Manager 4.0.2 Bundled Edition	No	Yes	See “ Using the Identity Manager 4.0.2 Bundle Edition .” (http://wwwtest.provo.novell.com/documentation/oes11/oes_implement_lx/data/b143d3j6.html).
iPrint	Yes	Yes	See “ Overview ” in the <i>OES 11 SP2: iPrint 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	<p>The iSCSI target for Linux does not support eDirectory access controls like the NetWare target does. Nor is the iSCSI initiator or target in OES 11 SP2 integrated with NetWare Remote Manager management. You use YaST management tools instead.</p> <p>On the other hand, the iSCSI implementation for Linux is newer and performs better.</p> <p>See Linux-iSCSI Project on the Web (http://linux-iscsi.sourceforge.net).</p> <p>See “Overview” in the <i>NW 6.5 SP8: iSCSI 1.1.3 Administration Guide</i>.</p>
KVM Virtualization Guest	No	Yes	Of the two OES virtualization solutions (KVM and Xen), only Xen is supported for running Netware.
KVM Virtualization Host Server	Yes	N/A	
LDAP Server for eDirectory	Yes	Yes	No functional differences.
Multipath Device Management	Yes	Yes	NetWare uses NSS multipath I/O. Linux uses Device Mapper - Multipath that runs underneath other device management services.

Service	NetWare 6.5 SP8	OES 11 SP2	Platform Differences / Migration Issues
MySQL	Yes - NetWare port of open source product	Yes - Standard Linux	<p>See MySQL.com on the Web (http://www.mysql.com).</p> <p>See “Overview: MySQL” in the <i>NW 6.5 SP8: Novell MySQL Administration Guide</i>.</p> <p>See also “Configuring MySQL with Novell Cluster Services” in the <i>OES 11 SP2: Web Services and Applications Guide</i>.</p>
NCP Volumes	No	Yes	<p>NCP Server on Linux supports creating NCP volumes on Linux POSIX file systems such as btrfs, Reiser, Ext2, Ext3, and XFS.</p> <p>For information, see “Managing NCP Volumes” in the <i>OES 11 SP2: NCP Server for Linux Administration Guide</i>.</p>
NCP Server	Yes	Yes	<p>NCP services are native to NetWare 6.5 and NSS volumes; to have NCP services on OES, the NCP Server must be installed.</p> <p>See “Benefits of NCP Server” in the <i>OES 11 SP2: NCP Server for Linux Administration Guide</i>.</p>
NetStorage	Yes	Yes	NetStorage on Linux offers connectivity to storage locations through the CIFS, NCP, and SSH protocols. NetWare uses only NCP.
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 requires that the NCP Server be installed.

Service	NetWare 6.5 SP8	OES 11 SP2	Platform Differences / Migration Issues
Novell Cluster Services	Yes	Yes	See “ Product Features ” in the <i>OES 11 SP2: Novell Cluster Services for Linux Administration Guide</i> . See “ Product Features ” in the <i>NW6.5 SP8: Novell Cluster Services 1.8.5 Administration Guide</i> .
Novell iFolder 2.x	Yes	No	For migration information, see “ Migrating iFolder 2.x ” in the <i>OES 11 SP2: Migration Tool Administration Guide</i> .
Novell iFolder 3.9	No	Yes	OES 11 SP2 includes Linux, Macintosh, and Windows clients.
Novell Licensing Services	Yes	No	See OES Doesn't Support NLS in the <i>OES 11 SP2: Planning and Implementation Guide</i> .
Novell Linux Volume Manager	No	Yes	The Novell Linux Volume Manager (NLVM) command line interface can be used to create and manage Linux POSIX file systems. For information about the syntax and options for the NLVM commands used in this section, see the <i>OES 11 SP2: NLVM Reference</i> .
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 11 SP2: NSS File System Administration Guide for Linux</i> . In OES 11 and later, NSS supports both the DOS and GPT partitioning scheme. It also supports partitions up to 8 TB in size. (NetWare supports only DOS and partitions up to 2 TB in size.) In OES 11 SP1 and later, NSSMU supports Linux volumes in addition to NSS pools and volumes.
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) .
PKI (Public Key Infrastructure)	Yes	Yes	No functional differences.
Printing	Yes	Yes	See iPrint .

Service	NetWare 6.5 SP8	OES 11 SP2	Platform Differences / Migration Issues
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>OES 11 SP2: Novell Samba Administration Guide</i> .
Search (QuickFinder)	Yes	Yes	<p>When indexing a file system, the QuickFinder engine indexes only what it has rights to see.</p> <p>On NetWare, it has full access to all mounted volumes. On Linux, it has rights to only the files that the novlwww user in the www group has rights to see.</p> <p>For more information, see “Security Characteristics” and “Generating an Index For a Linux-Mounted NSS Volume” in the <i>OES 11 SP2: Novell QuickFinder Server 5.0 Administration Guide</i>.</p>
SLP	Yes - Novell SLP	Yes - OpenSLP	<p>For OES 11, see SLP in the <i>OES 11 SP2: Planning and Implementation Guide</i>.</p> <p>NetWare uses Novell SLP, which provides caching of Directory Agent scope information in eDirectory. This provides for sharing of scope information among DAs.</p> <p>OpenSLP on Linux is now customized to provide DA information retention and sharing as well.</p>
Software RAIDS (NSS volumes)	Yes (0, 1, 5, 10, 15)	Yes (0, 1, 5, 10, 15)	See “ Understanding Software RAID Devices ” in the <i>OES 11 SP2: NSS File System Administration Guide for Linux</i> .
Storage Management Services (SMS)	Yes	Yes	<p>No functional differences, except that the SBCON backup engine is not supported on Linux.</p> <p>The nbackup engine is available for exploring SMS capabilities, but in a production environment, you should use a third-party, full-featured backup engine.</p>
TCP/IP	Yes	Yes	No functional differences.
Timesync NLM	Yes	No	<p>Timesync will not be ported to Linux. However, NTPv3 is available on both Linux and NetWare.</p> <p>See Time Services in the <i>OES 11 SP2: Planning and Implementation Guide</i>.</p>

Service	NetWare 6.5 SP8	OES 11 SP2	Platform Differences / Migration Issues
Tomcat	Yes	Yes	NetWare includes Tomcat 4 and a Tomcat 5 servlet container for iManager 2.7. OES 11 SP2 includes Tomcat 6. There is no impact to any of the OES 11 SP2 administration tools, which are tested and supported on both platforms. See “Administration Instance vs. Public Instance on NetWare”
Virtual Office (Collaboration)	Yes	No	Virtual Office has been replaced by Novell Vibe OnPrem. A separate purchase is required. For more information, see the Novell Vibe OnPrem Web Site (http://www.novell.com/products/vibe-onprem/) .
WAN Traffic Manager	Yes	No	
Xen Virtualization Guest	Yes	Yes	NetWare 6.5 SP8 (and NetWare 6.5 SP 7) can run as a paravirtualized machine. OES 11 SP2 can run as 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 11 SP2 offers. It is not uncommon that administrators discover capabilities in OES that they didn't know existed.

3.3 Exploring OES 11 SP2 services

We also recommend that you explore commonly used OES services by following the step-by-step instructions provided in the [OES 11 SP2: Getting Started with OES 11 and Virtualized NetWare](#).

3.4 Plan for eDirectory

eDirectory is the heart of OES network services and security.

- ♦ [Section 3.4.1, “Installing Into a New Tree,” on page 90](#)
- ♦ [Section 3.4.2, “Installing Into an Existing Tree,” on page 91](#)

3.4.1 Installing Into a New Tree

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 NetIQ eDirectory Network](#)” in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.
- ♦ **Time synchronization:** eDirectory requires that all servers, both NetWare and OES, be time synchronized. For more information, see [Chapter 12.3, “Time Services,”](#) on page 164.
- ♦ **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 *NetIQ eDirectory 8.8 SP8 Administration Guide*.

For information on these and other eDirectory planning tasks, see the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

The *OES 11 SP2: Getting Started with OES 11 and Virtualized NetWare* guide provides a basic introduction to creating container objects as well as Group and User objects in eDirectory.

3.4.2 Installing Into an Existing Tree

When installing into an existing tree, make sure you observe the following best practices whenever possible:

- ♦ **Use Existing eDirectory Objects:** Whenever possible, existing eDirectory objects, organizational units, users, groups, password policies, etc. should be used during the installation.

If new contexts or users are needed, it is best to create these prior to the installation.
- ♦ **Synchronize Replicas Before and After:** Ensure that all eDirectory partitions affected by the installation are synchronized before you begin and after you finish the installation.

Also, before installing into an existing tree, be sure you understand the information in [Section 14.2.3, “eDirectory Coexistence and Migration,”](#) on page 209.

3.5 Prepare Your Existing eDirectory Tree for OES

Complete all of the instructions in “[Preparing eDirectory for OES 11 SP2](#)” in the *OES 11 SP2: Installation Guide*.

NOTE: If you are installing the first OES server into an existing tree on a NetWare server, 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 11 SP2 has 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 11 SP2 Server (Physical):** “Preparing to Install OES 11 SP2” in the [OES 11 SP2: Installation Guide](#).
- ♦ **OES 11 SP2 Server (Virtual):** “System Requirements” in the [OES 11 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 22.2.2, “User Restrictions: Some OES Limitations,” on page 297](#).

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 \(http://www.novell.com/documentation/oes11/oes_readme/data/readme.html\)](http://www.novell.com/documentation/oes11/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 93](#)
- ♦ [Section 3.9.2, “Always Double-Check Service Configurations Before Installing,” on page 93](#)
- ♦ [Section 3.9.3, “Back Button Doesn’t Reset Configuration Settings,” on page 93](#)
- ♦ [Section 3.9.4, “Cluster Upgrades Must Be Planned Before Installing OES,” on page 94](#)
- ♦ [Section 3.9.5, “Common Proxy Password Policy Should Be Assigned,” on page 94](#)
- ♦ [Section 3.9.6, “Cross-Protocol File Locking Might Need To Be Reconfigured if AFP or CIFS Is Functioning on an NCP Server,” on page 94](#)
- ♦ [Section 3.9.7, “Do Not Create Local \(POSIX\) Users,” on page 95](#)

- [Section 3.9.8, “Do Not Upgrade to eDirectory 8.8 Separately,” on page 95](#)
- [Section 3.9.9, “Follow the Instructions for Your Chosen Platforms,” on page 95](#)
- [Section 3.9.10, “If You’ve Ever Had OES 1 Servers with LUM and NSS Installed,” on page 95](#)
- [Section 3.9.11, “iFolder 3.9.2 Considerations,” on page 98](#)
- [Section 3.9.12, “Incompatible TLS Configurations Give No Warning,” on page 99](#)
- [Section 3.9.13, “Installing into an Existing eDirectory Tree,” on page 99](#)
- [Section 3.9.14, “NetStorage Caveats,” on page 100](#)
- [Section 3.9.15, “NetWare Caveats,” on page 101](#)
- [Section 3.9.16, “Novell Distributed Print Services Cannot Migrate to Linux,” on page 101](#)
- [Section 3.9.17, “NSS Caveats,” on page 101](#)
- [Section 3.9.18, “Plan eDirectory Before You Install,” on page 102](#)
- [Section 3.9.19, “Samba Enabling Disables SSH Access,” on page 102](#)
- [Section 3.9.20, “Unsupported Service Combinations,” on page 102](#)
- [Section 3.9.21, “VNC Install Fails to Set the IP Address in /etc/hosts,” on page 105](#)

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 the [OES 11 SP2: Novell Cluster Services NetWare to Linux Conversion 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. One reason for this is explained in [Section 3.9.3, “Back Button Doesn’t Reset Configuration Settings,” on page 93](#).

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

Because of differences between Novell Cluster Services on NetWare 6.5 SP8 and OES, 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 94](#)
- ♦ [“Working with Mixed Node Clusters” on page 94](#)

Service Failover in a Mixed Cluster

The only cluster-enabled service that can fail over cross-platform (run on either OES 11 SP2 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 11 SP2 server can fail over to another OES 11 SP2 server in the cluster, but the service cannot fail over to a NetWare 6.5 SP8 server.

Working with Mixed Node Clusters

See the following sections before working with mixed NetWare and OES clusters:

- ♦ [“Planning the Cluster Conversion”](#) and [“Planning the Conversion of Load and Unload Scripts”](#) in the *OES 11 SP2: Novell Cluster Services NetWare to Linux Conversion Guide*.
- ♦ [“What’s New or Changed for Novell Cluster Services”](#) and [“Requirements and Guidelines for Upgrading Clusters from OES 2 SP3”](#) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide*.

3.9.5 Common Proxy Password Policy Should Be Assigned

When you install a Common Proxy user, it is possible to deselect the *Assign Common Proxy Password Policy to Proxy User* checkbox. This is not recommended because then the user inherits the password policies of the container where it is installed, and that can lead to service failures.

3.9.6 Cross-Protocol File Locking Might Need To Be Reconfigured if AFP or CIFS Is Functioning on an NCP Server

Cross-protocol file locking (CPL) default behavior works 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% by disabling CPL. 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. The CPL settings for clustered nodes must match.

For more information about cross-protocol locking, see [“Configuring Cross-Protocol File Locks for NCP Server”](#) in the *OES 11 SP2: NCP Server for Linux Administration Guide*.

3.9.7 Do Not Create Local (POSIX) Users

During the OES 11 SP2 install you are prompted by the SLES portion of the install to create at least one local user besides `root`, and you are warned if you bypass the prompt.

Creating local users is not recommended on OES servers because user management in OES 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 to servers through the Linux User Management (LUM) technology installed by default on every OES 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 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 217](#).

3.9.8 Do Not Upgrade to eDirectory 8.8 Separately

If you are running OES 11 SP2, do not upgrade to eDirectory 8.8 independently of upgrading to OES 11 SP2.

For example, do not upgrade from eDirectory 8.7.3 to eDirectory 8.8.6 through the `oes-edir88` patch channel prior to upgrading to OES 11 SP2. Doing so causes configuration problems that the OES 11 SP2 install is not designed to handle.

3.9.9 Follow the Instructions for Your Chosen Platforms

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

3.9.10 If You’ve Ever Had OES 1 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 H, “System User and Group Management in OES 11 SP2,” on page 335](#).

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 server with both LUM and NSS installed.

- ♦ [“NetStorage, XTier, and Their System Users” on page 96](#)
- ♦ [“An NSS Complication” on page 96](#)
- ♦ [“eDirectory Solves the Basic Problem” on page 96](#)
- ♦ [“ID Mismatches on OES 1” on page 96](#)
- ♦ [“The OES 1 Solution: The `nssid.sh` Script” on page 96](#)
- ♦ [“OES 2 SP1 or Later Requires a New Approach” on page 97](#)
- ♦ [“The Solution: Standardizing the UIDs on all OES servers” on page 97](#)

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, Reiser, or XFS, 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 217](#).

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 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

IMPORTANT: The following processes described in the next section (“[The Solution: Standardizing the UIDs on all OES servers](#)”) only need to be done once per eDirectory tree.

Unfortunately, system-level changes in SUSE Linux Enterprise Server 10 SP2 invalidated the `nssid.sh` script solution for OES 2 SP1 and later. Synchronizing the XTier IDs with an OES 1 installation can cause instability in other non-OES components. Therefore, if you have not already done so, you should standardize all XTier IDs on existing servers before installing a new OES 11 SP2 server with XTier-dependent services.

The Solution: Standardizing the UIDs on all OES servers

If your eDirectory tree has ever contained an OES 1 server with NSS and LUM installed, and if you have not already standardized the UIDs for a prior OES 2 SP1 or later release, do the following on each server that has NSS and LUM installed:

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

```
id novlxtierd
```

```
id novlxtierd
```

The standardized XTier IDs are UID 81 for `novlxtierd`, UID 82 for `novlxtierd`, and GID 81 for `novlxtierd`.

- 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(novlxtierd) gid=81(novlxtierd) groups=81(novlxtierd)
uid=82(novlxtierd) gid=81(novlxtierd) groups=81(novlxtierd),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 `novlxtierd` 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/oes11/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 97](#).

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 97](#).

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 97](#).

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 affects 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.

3.9.11 iFolder 3.9.2 Considerations

For best results, be sure you read and carefully follow the instructions in the [.Novell iFolder 3.9.2 Administration Guide](#) and the [Novell iFolder 3.9.2 Deployment Guide](#). This is especially critical if you plan to use NSS for your iFolder 3.9.2 data volume.

3.9.12 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.

3.9.13 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 99](#)
- ♦ [“Do Not Add OES to a Server That Is Already Running eDirectory” on page 99](#)
- ♦ [“Be Sure That eDirectory Is Healthy” on page 99](#)
- ♦ [“Be Sure That Network Time Is Synchronized” on page 100](#)
- ♦ [“Be Sure that OpenSLP on OES Is Configured Properly” on page 100](#)

Consider Coexistence and Migration Issues

If you are installing a new OES 11 SP2 server into an existing eDirectory tree, be sure to read and follow the instructions in “[Preparing eDirectory for OES 11 SP2](#)” in the [OES 11 SP2: Installation Guide](#).

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

Although you can add OES to an existing SLES 11 server if needed, you cannot install OES on a SLES 11 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 [NetIQ eDirectory 8.8 SP8 Administration Guide](#).

Be Sure That Network Time Is Synchronized

OES 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 11 SP2 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 164](#).

Be Sure that OpenSLP on OES 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 176](#).

3.9.14 NetStorage Caveats

- ♦ [“NetStorage Access to a Cluster Resource Fails When the Resource Comes Online from a Comatose State” on page 100](#)
- ♦ [“Unable to Use a Common Proxy if ZENworks and NetStorage Are Installed on the Same System” on page 100](#)
- ♦ [“Common Proxy Password Cannot Exceed 20 Characters” on page 100](#)
- ♦ [“NetStorage Purge and Salvage Options Do Not Work on Macintosh with Safari 4.0.x” on page 100](#)

NetStorage Access to a Cluster Resource Fails When the Resource Comes Online from a Comatose State

To restore access to the storage object, restart the `novell-xsrvc` process by running the following command:

```
/etc/init.d/novell-xsrvc restart
```

Unable to Use a Common Proxy if ZENworks and NetStorage Are Installed on the Same System

If you are using ZENworks along with NetStorage on the same OES server, you must not use a common proxy user.

Common Proxy Password Cannot Exceed 20 Characters

If a common proxy user used by NetStorage is assigned a password policy, you must ensure that the password size specified in the policy does not exceed 20 characters.

NetStorage Purge and Salvage Options Do Not Work on Macintosh with Safari 4.0.x

If you are using Safari 4.0.x with Macintosh, the Salvage and Purge options do not work.

3.9.15 NetWare Caveats

- ♦ [“NetWare Licenses and OES Trees” on page 101](#)
- ♦ [“NetWare 6.5 Servers Must Be Running SP3 or Later” on page 101](#)

NetWare Licenses and OES Trees

OES doesn't use Novell Licensing Services ([Section 4.6, “Licensing,” on page 113](#)). As a result, OES servers don't need a license container in eDirectory as part of the server installation.

In a mixed OES 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 *NetIQ iManager Installation Guide*](#).
- 2 Add a Read/Write replica to the server as described in [“Adding a Replica” in the *NetIQ eDirectory 8.8 SP8 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 *NetIQ iManager Installation Guide*](#).

NetWare 6.5 Servers Must Be Running SP3 or Later

If you are installing OES 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:

- ♦ **SLP Directory Agents:** If the SLP Directory Agents on your network are not running NetWare 6.5 SP3 or later, installing an OES 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.

3.9.16 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*](#).

3.9.17 NSS Caveats

- ♦ [“About New Media Support and Clusters” on page 102](#)
- ♦ [“Removable Media Cannot Be Mounted on OES” on page 102](#)

About New Media Support and Clusters

The new media support for hard links on OES 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 a later version of OES.

Removable Media Cannot Be Mounted on OES

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 11 SP2: NSS File System Administration Guide for Linux*.

3.9.18 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 11 Services](#)” in the *OES 11 SP2: Installation Guide*.

3.9.19 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 11.5, “SSH Services on OES 11 SP2,”](#) on page 155.

3.9.20 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	<ul style="list-style-type: none">♦ 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	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows (DSfW) ♦ Xen Virtual Machine Host Server
Novell Backup / Storage Management Services	No restrictions
Novell CIFS	<ul style="list-style-type: none"> ♦ File Server (Samba) ♦ Novell Domain Services for Windows ♦ Novell Samba ♦ Xen Virtual Machine Host Server
Novell Cluster Services (NCS)	<ul style="list-style-type: none"> ♦ High Availability ♦ Novell Domain Services for Windows <p>DSfW can actually be installed and run on the same server as NCS, but DSfW cannot run as a clustered service.</p>
Novell DHCP	<ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server
Novell DNS	<ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server
Novell Domain Services for Windows	<ul style="list-style-type: none"> ♦ File Server (Samba) ♦ Novell AFP ♦ Novell Archive and Version Services ♦ Novell CIFS ♦ Novell Cluster Services (NCS) <p>NCS can actually be installed and run on the server, but DSfW cannot run as a clustered service.</p> <ul style="list-style-type: none"> ♦ Novell FTP ♦ Novell iFolder ♦ Novell NetStorage ♦ Novell Pre-Migration Server ♦ Novell QuickFinder ♦ Novell Samba ♦ Xen Virtual Machine Host Server
NetIQ eDirectory	<ul style="list-style-type: none"> ♦ Directory Server (LDAP) ♦ Xen Virtual Machine Host Server
Novell FTP	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell iFolder	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell iManager	<ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server

Service	Unsupported on the Same Server
Novell iPrint	<ul style="list-style-type: none"> ♦ 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 Server," on page 124. ♦ Xen Virtual Machine Host Server
Novell Linux User Management (LUM)	No restrictions
Novell NCP Server / Dynamic Storage Technology	<ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server
Novell NetStorage	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell Pre-Migration Server	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell QuickFinder	<ul style="list-style-type: none"> ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell Remote Manager (NRM)	<ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server
Novell Samba	<ul style="list-style-type: none"> ♦ File Server (Samba) ♦ Novell CIFS ♦ Novell Domain Services for Windows ♦ Xen Virtual Machine Host Server
Novell Storage Services (NSS)	<ul style="list-style-type: none"> ♦ Xen Virtual Machine Host Server

Service	Unsupported on the Same Server
Xen Virtual Machine Host Server	<ul style="list-style-type: none"> ♦ File Server (Samba) ♦ Novell AFP ♦ Novell Archive and Version Services ♦ Novell CIFS ♦ Novell DHCP ♦ Novell DNS ♦ Novell Domain Services for Windows ♦ NetIQ 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)

3.9.21 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. In some cases, there are specific paths to follow so that the OES 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 11 SP2 servers with existing NetWare and Linux networks, see [Chapter 8, "Migrating Existing Servers and Data," on page 135](#).

3.11 Understand Your Installation Options

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

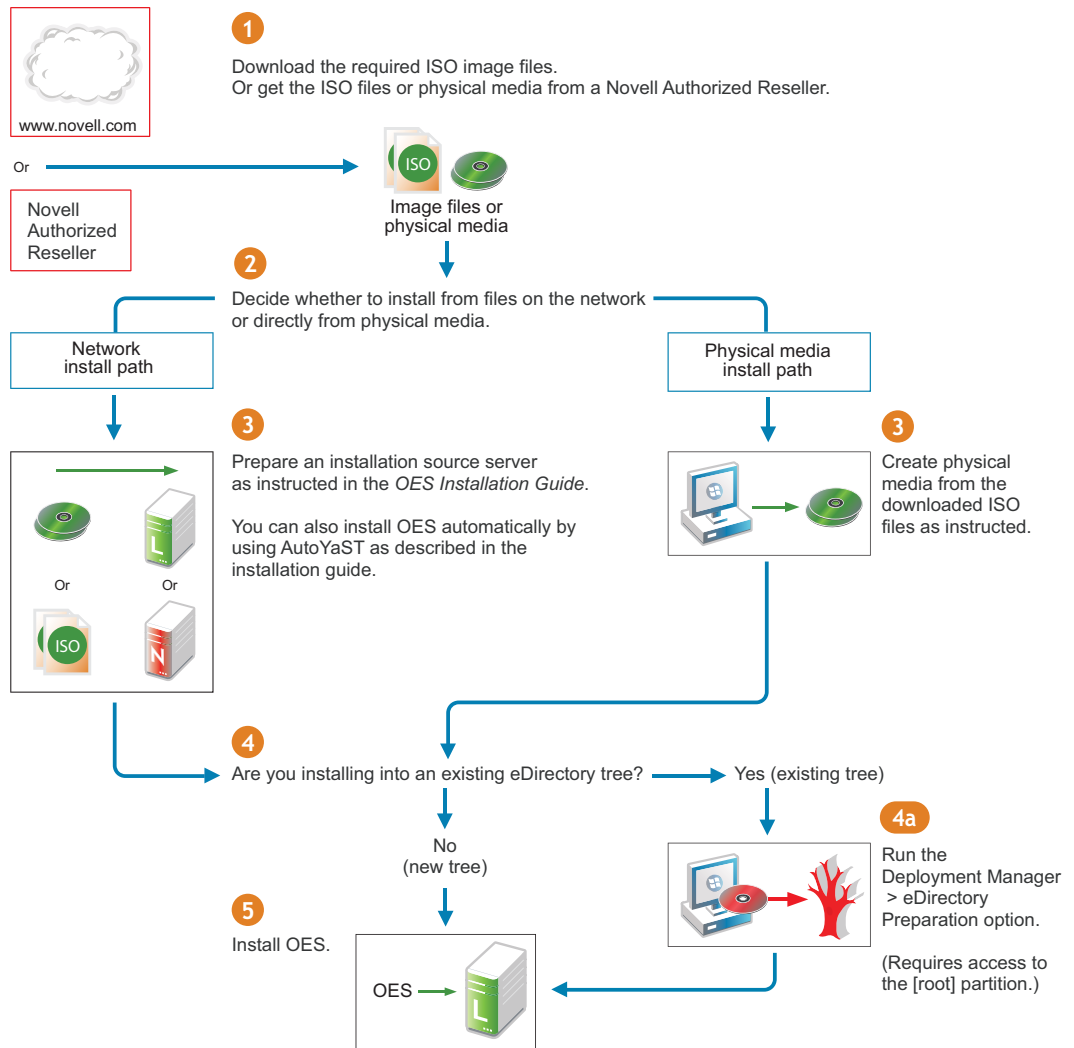
- [Section 3.11.1, “OES 11 SP2 Installation Overview,” on page 106](#)
- [Section 3.11.2, “About Your Installation Options,” on page 107](#)
- [Section 3.11.3, “Use Predefined Server Types \(Patterns\) When Possible,” on page 107](#)
- [Section 3.11.4, “If You Want to Get Acquainted with SP2 First,” on page 108](#)

3.11.1 OES 11 SP2 Installation Overview

The software and network preparation processes required to install OES 11 SP2 are outlined in [Figure 3-1](#).

NOTE: [Chapter 4, “Getting and Preparing OES 11 SP2 Software,” on page 109](#) contains instructions for obtaining the ISO image files referred to in the following illustration.

Figure 3-1 OES 11 SP2 Install Preparation



For detailed instructions, see “[Setting Up a Network Installation Source](#)” in the *OES 11 SP2: Installation Guide*.

3.11.2 About Your Installation Options

As illustrated in the previous section, OES 11 SP2 lets you install from either physical media or from files on the network.

- ♦ “[OES 11 SP2 Options](#)” on page 107
- ♦ “[Virtual Machine Installation Options](#)” on page 107

OES 11 SP2 Options

OES 11 SP2 includes numerous installation options as documented in the *OES 11 SP2: Installation Guide*.

- ♦ **Integrated Media Install:** You can install SLES 11 SP3 and OES 11 SP2 from a single ISO or DVD obtained from a Novell Authorized Reseller or created from a downloaded ISO image file.

See “[Preparing Physical Media for a New Server Installation or an Upgrade](#)” in the *OES 11 SP2: Installation Guide*.
- ♦ **CD/DVD Install:** You can install SLES 11 SP3 by using a DVD and then install OES 11 SP2 from a CD, both 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 11 SP2: Installation Guide*.
- ♦ **Network Install:** You can install from the network by using the NFS, FTP, or HTTP protocol.

If you are installing from both SLES and OES media, using the network saves you from swapping media on the server during the installation.

See “[Setting Up a Network Installation Source](#)” in the *OES 11 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 11 SP2: Installation Guide*.

Virtual Machine Installation Options

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

- ♦ “[Installing, Upgrading, or Updating OES on a VM](#)” in the *OES 11 SP2: Installation Guide*
- ♦ “[Installing and Managing NetWare on a Xen-based VM](#)” in the *OES 11 SP2: Installation Guide*

3.11.3 Use Predefined Server Types (Patterns) When Possible

OES 11 SP2 includes predefined server installation options that install only the components required to provide a specific set of network services. These server types are called *patterns*.

For example, if you want to install an OES 11 SP2 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 11 SP2 server with only the service components you need.

More information about server patterns is available in “[OES Services Pattern Descriptions](#)” in the [OES 11 SP2: Installation Guide](#)

3.11.4 If You Want to Get Acquainted with SP2 First

Many administrators prefer to install products on and experiment on a smaller scale prior to formal deployment feasibility testing. The [OES 11 SP2: Getting Started with OES 11 and Virtualized NetWare](#) walks you through installing and exploring all the basic OES 11 SP2 services.

4 Getting and Preparing OES 11 SP2 Software

This section contains instructions for getting and preparing Open Enterprise Server 11 SP2 software and discusses the following topics:

- ♦ [Section 4.1, “Do You Have Upgrade Protection?,” on page 109](#)
- ♦ [Section 4.2, “64-Bit Only,” on page 109](#)
- ♦ [Section 4.3, “Do You Want to Purchase OES 11 SP2 or Evaluate It?,” on page 109](#)
- ♦ [Section 4.4, “Evaluating OES 11 SP2 Software,” on page 110](#)
- ♦ [Section 4.5, “Downloading and Preparing OES Software,” on page 111](#)
- ♦ [Section 4.6, “Licensing,” on page 113](#)

If you have not already done so, we recommend that you review the information in [Section 3.11, “Understand Your Installation Options,” on page 106](#).

4.1 Do You Have Upgrade Protection?

If you have Novell Upgrade Protection, you can upgrade to OES 11 SP2 and the associated support packs, free of charge until your upgrade protection expires. After your protection expires, the OES 11 SP2 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 \(https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp\)](https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp).
- 2 Follow the instructions on the page to obtain the upgrade to Open Enterprise Server 11 SP2.

4.2 64-Bit Only

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

OES 11 SP2 is a set of services or an “add-on product” that runs on SUSE Linux Enterprise Server (SLES 11 SP3) and is available in 64-bit only.

4.3 Do You Want to Purchase OES 11 SP2 or Evaluate It?

If you want to evaluate OES prior to purchasing it, skip to the next section, [Evaluating OES 11 SP2 Software](#).

If you have decided to purchase OES 11 SP2, visit the Novell [How to Buy OES 11 Web page \(http://www.novell.com/products/openenterpriseserver/howtobuy.html\)](http://www.novell.com/products/openenterpriseserver/howtobuy.html).

When you purchase OES 11 SP2, you receive two activation codes for OES 11 SP2 (one for OES 11 services and one for SUSE Linux Enterprise Server 11). Both codes are required for registering an OES 11 SP2 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 11 SP2 licensing model. For a brief description, see [Section 4.6, “Licensing,” on page 113](#).

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 106](#) and then skip to [Chapter 5, “Installing OES 11 SP2,” on page 115](#).

4.4 Evaluating OES 11 SP2 Software

This section walks you through the OES 11 SP2 software evaluation process and discusses the following topics:

- [Section 4.4.1, “Understanding OES 11 SP2 Software Evaluation Basics,” on page 110](#)
- [Section 4.4.2, “Evaluating OES 11 SP2,” on page 110](#)
- [Section 4.4.3, “Installing OES 11 for Evaluation Purposes,” on page 111](#)

4.4.1 Understanding OES 11 SP2 Software Evaluation Basics

You can evaluate the full OES 11 SP2 product. The evaluation software is the complete, fully functional OES 11 SP2 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 11 SP2 product are limited to the rights set forth in the EULA.

Briefly, the evaluation period for OES 11 SP2 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 11 and SLES 11 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 Evaluating OES 11 SP2

During the evaluation period, we recommend that you fully explore the many services available in OES 11 SP2.

To help you get started with the process, we have prepared a [Getting Started Guide](#) for OES 11 SP2 that explores both OES 11 SP2 and virtualized NetWare on a second OES 11 SP2 virtual machine host server. The sections in this guide introduce eDirectory, walk you through server installations, and provide brief exercises that you can complete to get started using OES 11 SP2 Services. After completing the exercises in the guide, you can use the environment you’ve created to further explore OES 11 SP2 and learn about its many powerful services.

For more information, see the [OES 11 SP2: Getting Started with OES 11 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 11 SP2 and the planning and implementation processes you will follow to fully leverage its network services.

4.4.3 Installing OES 11 for Evaluation Purposes

After completing the instructions in [Section 4.5.1, “Downloading OES 11 SP2 Software from the Novell Web Site,” on page 111](#), you will have two activation/evaluation codes: one for OES 11 and another for SLES 11. As you install OES 11 SP2, you should register with the Novell Customer Center and use these codes to enable your server for online updates from the OES 11 and SLES 11 patch channels.

IMPORTANT: Always download the current patches during an installation.

Instructions for using the activation codes during an installation are found in “[Specifying Novell Customer Center Configuration Settings](#)” in the *OES 11 SP2: Installation Guide*.

The evaluation period begins when the codes are issued. Use the same activation codes for each OES 11 server you install during the evaluation period.

4.5 Downloading and Preparing OES Software

- ♦ [Section 4.5.1, “Downloading OES 11 SP2 Software from the Novell Web Site,” on page 111](#)
- ♦ [Section 4.5.2, “Preparing the Installation Media,” on page 112](#)
- ♦ [Section 4.5.3, “Installing Purchased Activation Codes after the Evaluation Period Expires,” on page 112](#)

4.5.1 Downloading OES 11 SP2 Software from the Novell Web Site

If you already have OES 11 SP2 ISO image files, skip to [Section 4.5.2, “Preparing the Installation Media,” on page 112](#).

If you have OES 11 SP2 product media (CDs and DVDs), skip to [Section 4.4.3, “Installing OES 11 for Evaluation Purposes,” on page 111](#).

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 11 SP2*.
- 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 11 SP2 previously and received your OES 11 and SLES 11 activation codes, skip to [Step 15](#).

Otherwise, in the *Evaluating Open Enterprise Server 11 SP2* section, click the *Get Activation Codes* link in the *Novell Open Enterprise Server 11 SP2* 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 11 and the SLES 11 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 11 SP2 from files on your network, see the instructions in [“Setting Up a Network Installation Source”](#) in the *OES 11 SP2: Installation Guide*.

4.5.2 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 112](#). 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 a Network Installation Source”](#) in the *OES 11 SP2: Installation Guide*.

4.5.3 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 Using the Command Line”](#) in the *OES 11 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.

4.6 Licensing

This section explains the following:

- ♦ [Section 4.6.1, “The OES 11 SP2 Licensing Model,” on page 113](#)
- ♦ [Section 4.6.2, “OES Doesn’t Support NLS,” on page 113](#)

4.6.1 The OES 11 SP2 Licensing Model

The only OES 11 SP2 licensing restriction is the number of user connections allowed to use OES 11 SP2 services on your network. You are authorized to install as many OES 11 SP2 servers as you need to provide OES 11 SP2 services to those users.

For example, if your OES 11 SP2 license is for 100 user connections, you can install as many OES 11 SP2 servers as desired. Up to 100 users can then connect to and use the services provided by those OES 11 SP2 servers. When you install OES 11 SP2, you must accept an end user license agreement (EULA). Your rights to use the OES 11 SP2 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.

For more information on OES licensing, see the [Novell Licensing EULA page on the Novell Web site](http://www.novell.com/licensing/eula/) (<http://www.novell.com/licensing/eula/>).

4.6.2 OES Doesn’t Support NLS

Novell Licensing Services (NLS) are not available on OES, nor does an OES installation require a license/key file pair (*.nlf and *.nfk). Therefore, in a mixed OES 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 Trees” on page 101](#).

5 Installing OES 11 SP2

IMPORTANT: Before you install Open Enterprise Server 11 SP2, be sure to review the information in [Chapter 3, “Planning Your OES 11 SP2 Implementation,”](#) on page 83, especially [Section 3.9, “Caveats to Consider Before You Install,”](#) on page 92.

This section briefly covers the following:

- ♦ [Section 5.1, “Installing OES 11 SP2 on Physical Servers,”](#) on page 115
- ♦ [Section 5.2, “Installing OES 11 SP2 Servers in a Xen VM,”](#) on page 116
- ♦ [Section 5.3, “Installing OES 11 SP2 Servers in a KVM Virtual Machine,”](#) on page 116

5.1 Installing OES 11 SP2 on Physical Servers

The OES 11 SP2 installation leverages the SUSE Linux YaST graphical user interface. You can install OES 11 SP2 services on an existing SUSE Linux Enterprise Server 11 SP2 server, or you can install both OES 11 SP2 and SLES 11 SP3 at the same time, making the installation of SLES 11 and OES 11 services a seamless process.

To ensure a successful installation:

1. Read and follow all instructions in the [OES 11 SP2: Readme](#).
2. Carefully follow the instructions in the [OES 11 SP2: Installation Guide](#), especially those found in
 - ♦ [“Preparing to Install OES 11 SP2”](#)
 - ♦ [“Installing OES 11 SP2 as a New Installation”](#)
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, you are prompted for the root password.

This happens because the server reboots as part of the update process and the `root` password is no longer in memory.

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 11 SP2 on an Existing Server”](#) in the [OES 11 SP2: Installation Guide](#).

5.1.1 What's Next

After installing OES 11 SP2 and before starting to use your new server, be sure to review the information in [Chapter 6, “Caveats for Implementing OES 11 SP2 Services,”](#) on page 117.

The various service sections in this guide contain information about completing your OES 11 SP2 services implementation. See the sections for the services you have installed, beginning with [Chapter 11, “Managing OES 11 SP2,”](#) on page 143.

5.2 Installing OES 11 SP2 Servers in a Xen VM

Installing OES 11 SP2 servers on a Xen virtual machine involves installing an OES 11 SP2 or SUSE Linux Enterprise Server (SLES) 11 SP3 VM host server, creating a VM, and then installing a NetWare or OES server in the VM.

To get started with Xen virtualization in OES 11 SP2, see the following:

- ♦ “Introduction to Xen Virtualization (http://www.suse.com/documentation/sles11/book_xen/data/cha_xen_basics.html)” in the *Virtualization with Xen* (http://www.suse.com/documentation/sles11/book_xen/data/book_xen.html) guide.
- ♦ “Installing OES as a VM Host Server” in the *OES 11 SP2: Installation Guide*.
- ♦ “Installing, Upgrading, or Updating OES on a VM” in the *OES 11 SP2: Installation Guide*.
- ♦ “Installing and Managing NetWare on a Xen-based VM” in the *OES 11 SP2: Installation Guide*.

5.3 Installing OES 11 SP2 Servers in a KVM Virtual Machine

Installing OES 11 SP2 servers on a KVM virtual machine involves installing an OES 11 SP2 or SUSE Linux Enterprise Server (SLES) 11 SP2 VM host server, creating a VM, and then installing an OES server in the VM.

To get started with KVM virtualization in OES 11 SP2, see the following:

- ♦ The *Virtualization with KVM* (http://www.suse.com/documentation/sles11/book_kvm/data/book_kvm.html) guide.
- ♦ “Installing OES as a VM Host Server” in the *OES 11 SP2: Installation Guide*.
- ♦ “Installing, Upgrading, or Updating OES on a VM” in the *OES 11 SP2: Installation Guide*.

6 Caveats for Implementing OES 11 SP2 Services

This section presents a few pointers for avoiding common Open Enterprise Server 11 SP2 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 118](#)
- ♦ [Section 6.2, “Avoiding POSIX and eDirectory Duplications,” on page 118](#)
- ♦ [Section 6.3, “CIFS,” on page 120](#)
- ♦ [Section 6.4, “CUPS on OES 11 SP2,” on page 121](#)
- ♦ [Section 6.5, “DSfW: MMC Password Management Limitation,” on page 121](#)
- ♦ [Section 6.6, “eDirectory,” on page 121](#)
- ♦ [Section 6.7, “iFolder 3.9.22,” on page 123](#)
- ♦ [Section 6.8, “iPrint,” on page 123](#)
- ♦ [Section 6.9, “LDAP—Preventing “Bad XML” Errors,” on page 125](#)
- ♦ [Section 6.10, “LUM Cache Refresh No Longer Persistent,” on page 125](#)
- ♦ [Section 6.11, “Management,” on page 125](#)
- ♦ [Section 6.12, “McAfee Antivirus Requires Additional Configuration,” on page 127](#)
- ♦ [Section 6.13, “NCP,” on page 127](#)
- ♦ [Section 6.14, “Novell-tomcat Is for OES Use Only,” on page 128](#)
- ♦ [Section 6.15, “NSS,” on page 128](#)
- ♦ [Section 6.16, “OpenLDAP on OES,” on page 129](#)
- ♦ [Section 6.17, “Samba,” on page 129](#)
- ♦ [Section 6.18, “SLP Registrations Are Not Retrieved from a Novell SLP DA,” on page 129](#)
- ♦ [Section 6.19, “Synchronizing NMAS Login Methods Is Required to Avoid Login Failures,” on page 129](#)
- ♦ [Section 6.20, “Using NLVM with Linux Software RAIDs,” on page 130](#)
- ♦ [Section 6.21, “Virtualization,” on page 131](#)

6.1 AFP

- ♦ [Section 6.1.1, “Anti-Virus Solutions and AFP,” on page 118](#)

6.1.1 Anti-Virus Solutions and AFP

The Apple Filing Protocol (AFP) support for NSS files on OES 11 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 11 SP2 server or by real-time and on-demand scanning on the Apple client.

6.2 Avoiding POSIX and eDirectory Duplications

OES 11 SP2 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 118](#)
- ♦ [Section 6.2.2, “Three Examples,” on page 118](#)
- ♦ [Section 6.2.3, “Avoiding Duplication,” on page 119](#)

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 11 SP2 server.

6.2.2 Three Examples

The following examples illustrate the issue.

- ♦ [“The shadow Group” on page 119](#)
- ♦ [“The users Group” on page 119](#)
- ♦ [“Other Non-System Groups” on page 119](#)

The shadow Group

There is a default [system-created group](#) named `shadow` that is used by certain Web-related services, including the 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 11 SP2 services but is nevertheless created on all SLES 11 (and therefore, OES 11) 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 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 120](#)
- ♦ [“Create Only eDirectory Users and Groups” on page 120](#)

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 H, “System User and Group Management in OES 11 SP2,” on page 335](#) is not exhaustive. For example, the `users` group is not listed.

Create Only eDirectory Users and Groups

For OES 11 SP2 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 120](#)
- ♦ [Section 6.3.2, “Renaming CIFS Share Names on NSS Volumes Results in Two Share Names,” on page 120](#)

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.

6.3.2 Renaming CIFS Share Names on NSS Volumes Results in Two Share Names

When NSS volumes are added to an OES 11 SP2 server, they are automatically added as CIFS shares.

If you rename these shares and restart CIFS, the original share names appear in addition to the new share names you specified.

6.4 CUPS on OES 11 SP2

iPrint is the print solution for OES 11 SP2 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 11 SP2 server.

6.5 DSfW: MMC Password Management Limitation

After creating a user, you cannot then force a password change through the Microsoft Management Console (MMC) because the *User must change password at next logon* option is disabled. You can work around this issue while creating the user by selecting the option as part of the creation task. For existing users, you can reset the password and select the same option as part of the reset task.

6.6 eDirectory

- [Section 6.6.1, "Avoid Uninstalling eDirectory When Possible," on page 121](#)
- [Section 6.6.2, "Avoid Renaming Trees and Containers," on page 122](#)
- [Section 6.6.3, "Default Static Cache Limit Might Be Inadequate," on page 122](#)
- [Section 6.6.4, "eDirectory Not Restarting Automatically," on page 122](#)
- [Section 6.6.5, "One Instance Only," on page 122](#)
- [Section 6.6.6, "Special Characters in Usernames and Passwords," on page 122](#)

6.6.1 Avoid Uninstalling eDirectory When Possible

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

The process of uninstalling and reinstalling eDirectory is documented in "[Reconfiguring eDirectory and OES Services](#)" in the *OES 11 SP2: Installation Guide*. However, you should carefully consider the potential ramifications of doing this. The documented solution has been thoroughly tested, but it is impossible for Novell to anticipate all customer scenarios and the complications that might arise in them.

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

IMPORTANT: Although the eDirectory 8.8 documentation describes how to remove and reinstall eDirectory, the processes described in that documentation do not cleanly decouple OES services, nor do they restore service connections. Therefore, they do not apply to OES servers.

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 11 sets a default static cache of 200 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 Not Restarting Automatically

After a system crash or power failure, eDirectory services (ndsd) might not automatically restart in some situations. To start eDirectory again, do the following:

- 1 Delete the `/var/opt/novell/eDirectory/data/ndsd.pid` file.
- 2 At a terminal prompt, enter `/etc/init.d/ndsd start`.

6.6.5 One Instance Only

OES 11 SP2 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 11.

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 3.9.22

Implementation caveats for iFolder 3.9.2 are documented in [“Caveats for Implementing iFolder Services”](#) in the *Novell iFolder 3.9.2 Administration Guide*.

6.8 iPrint

iPrint has the following implementation caveats:

- ♦ [Section 6.8.1, “Advanced Printing Options,” on page 123](#)
- ♦ [Section 6.8.2, “Authentication Dialog Not Displaying for Secure Printers from Terminal Servers,” on page 123](#)
- ♦ [Section 6.8.3, “Cluster Failover Between Mixed Platforms Not Supported,” on page 123](#)
- ♦ [Section 6.8.4, “iManager Plug-Ins Are Platform-Specific,” on page 124](#)
- ♦ [Section 6.8.5, “iPrint Client for Linux Doesn't Install Automatically,” on page 124](#)
- ♦ [Section 6.8.6, “iPrint Disables CUPS Printing on the OES Server,” on page 124](#)
- ♦ [Section 6.8.7, “Linux and Macintosh Client Printer Installation Fails When Communicating via Proxy,” on page 124](#)
- ♦ [Section 6.8.8, “Printer Driver Uploading on OES 11 SP2 Might Require a CUPS Administrator Credential,” on page 124](#)
- ♦ [Section 6.8.9, “Printer Driver Uploading Support,” on page 124](#)

6.8.1 Advanced Printing Options

Some drivers, such as HP and Lexmark UPDs, have problems handling advanced printing options, such as watermarks and n-up printing when they are used from user workstations.

6.8.2 Authentication Dialog Not Displaying for Secure Printers from Terminal Servers

When you perform an automatic driver or profile update for secure printers from terminal servers, the authentication dialog box is not displayed.

6.8.3 Cluster Failover Between Mixed Platforms Not Supported

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

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 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 11 SP2: iPrint Linux Administration Guide*.

6.8.6 iPrint Disables CUPS Printing on the OES Server

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

6.8.7 Linux and Macintosh Client Printer Installation Fails When Communicating via Proxy

Linux and Macintosh iPrint clients fail to install printers when communicating with the iPrint server through a proxy server.

6.8.8 Printer Driver Uploading on OES 11 SP2 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. 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.

6.8.9 Printer Driver Uploading Support

Uploading drivers from SUSE Linux Enterprise Desktop (SLED) 10 supports PPD upload using *Add From System* but SLED 11 supports PPD upload using both *Add From System* and *Add From file*.

Uploading PPD printer drivers from a Windows workstation requires Internet Explorer 5.5 or later and supports only *Add From File*."

Windows printer drivers can be uploaded only by using Internet Explorer running on Windows.

6.9 LDAP—Preventing “Bad XML” Errors

If you are using NetIQ 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 *NetIQ eDirectory 8.8 SP8 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 release with the addition of the AncestorID feature.

6.10 LUM Cache Refresh No Longer Persistent

In response to customer requests for improved LDAP performance, persistent searching for new Linux-enabled users and groups was disabled in OES 2 and has been carried forward in OES 11. This means that when a user or group is enabled for Linux access, it is not immediately listed in some of the interfaces, such as the GUI file browser.

For most installations this is not an issue. However, persistent searching can be turned on by editing the `/etc/nam.conf` file and changing the `persistent-search` parameter from `no` to `yes`.

Alternatively, you can shorten the LUM cache refresh period (default is 8 hours). You can adjust the refresh period by editing the `persistent-cache-refresh-period` parameter in the `/etc/nam.conf` file and restarting LUM using the `rcnamcd restart` command.

You can also refresh the cache immediately by using the `namconfig cache_refresh` command.

For more information, see [“The namcd Linux User Management Caching Daemon”](#) in the *OES 11 SP2: Novell Linux User Management Administration Guide*.

6.11 Management

- ♦ [Section 6.11.1, “iManager RBS Configuration with OES 11,” on page 126](#)
- ♦ [Section 6.11.2, “Storage Error in iManager When Accessing a Virtual Server,” on page 126](#)
- ♦ [Section 6.11.3, “Truncated DOS-Compatible Short Filenames Are Not Supported at a Terminal Prompt,” on page 127](#)
- ♦ [Section 6.11.4, “LUM-Enabling Required for Full Administrative Access,” on page 127](#)

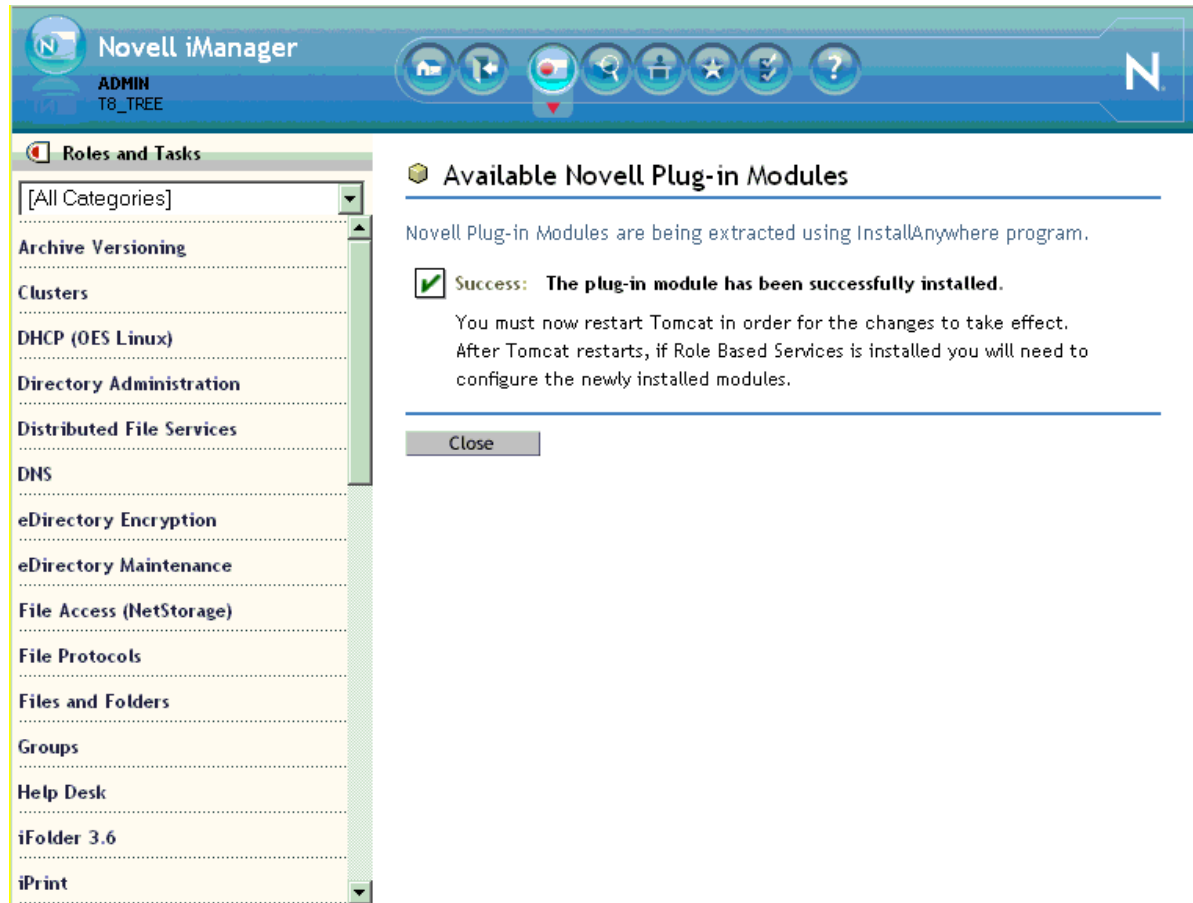
6.11.1 iManager RBS Configuration with OES 11

In “Installing RBS” in the [NetIQ® iManager Administration Guide](#), you are instructed to run the iManager Configuration Wizard before using iManager.

When iManager is installed in connection with OES 11, 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 [NetIQ® iManager Administration Guide](#).

6.11.2 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.

6.11.3 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.

6.11.4 LUM-Enabling Required for Full Administrative Access

The current LUM architecture requires that administrators, administrator equivalents, and RBS-enabled managers be LUM-enabled to have full management capabilities.

6.12 McAfee Antivirus Requires Additional Configuration

After installing McAfee Antivirus support on an OES server with NSS and/or NCP volumes, various problems might be seen, including clustered volumes going comatose because of mount failures with an error code of 150.

This happens because the antivirus software is locking `.trustee_database.xml` files on NSS and NCP volumes.

To prevent these problems, make sure you do the following, as described in the McAfee documentation. (References to OES 2 apply to OES 11 as well.)

- 1 Exclude the `._NETWARE` and `/_admin/*` folders on all NSS and NCP volumes as documented in Chapter 5 > Anti-virus Exclusions in the [McAfee VirusScan Enterprise for Linux 1.7.0 Best Practices Guide](#), except that the `/_admin/*` path is documented incorrectly as `._ADMIN` in the McAfee guide.

For example:

- ♦ `/_admin/*` (for NSS)
 - ♦ `/admin/*` (for NCS)
 - ♦ `/media/nss/volume_name/._NETWARE`
- 2 Using iManager, create a `nails` user and a `nailsgroup` group in eDirectory and assign them administrative privileges on all NSS and/or NCP volumes as documented in Chapter 2 > Prerequisites in the [McAfee VirusScan Enterprise for Linux 1.7.0 Software Configuration Guide](#).

IMPORTANT: Be sure to configure any new NSS or NCP volumes you add to the server.

6.13 NCP

- ♦ [Section 6.13.1, “NCP Doesn’t Equal NSS File Attribute Support,” on page 128](#)
- ♦ [Section 6.13.2, “Opening MS Office Files Using Novell Client for Windows 7,” on page 128](#)

6.13.1 NCP Doesn't Equal NSS File Attribute Support

NSS file attributes and NCP services tend to get mixed together in the minds of OES administrators, especially those with a lot of NetWare experience. 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 (Ext3, XFS, and so on) 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.

6.13.2 Opening MS Office Files Using Novell Client for Windows 7

To open MS Office files through an NCP (Novell Client) connection, Windows 7 workstations must be running Novell Client 2 SP1 for Windows, version IR 9a or later. Otherwise, file open requests are denied. See [TID 7009540 \(http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7009540&sliceId=1&docTypeID=DT_TID_1_1&dialogID=273023280&statId=0%200%20273025163\)](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7009540&sliceId=1&docTypeID=DT_TID_1_1&dialogID=273023280&statId=0%200%20273025163).

Windows XP workstations do not experience the problem. The latest version of Novell Client for Windows XP is version 4.91 SP5 (IR1).

6.14 Novell-tomcat Is for OES Use Only

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

The `novell-tomcat` package, and its associated configuration file and JRE (`novell-tomcat.conf` and IBM 1.6.0 Java), must not be manually modified, updated, or changed in any way. Otherwise, OES services and tools, such as iManager, do not work as expected.

If you want to deploy a Tomcat-dependant Web application on an OES server, use the open source Tomcat package that comes with SLES 11. Installing and configuring the open source Tomcat package will not affect the `novell-tomcat` package.

6.15 NSS

- [Section 6.15.1, "For GroupWise, Change the Default Name Space to UNIX," on page 129](#)
- [Section 6.15.2, "Junction Target Support," on page 129](#)

6.15.1 For GroupWise, Change the Default Name Space to UNIX

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 11 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.

6.15.2 Junction Target Support

If a junction's source and target are both on OES, then subdirectory targets are fully supported.

Junctions from OES to NetWare only support targets at the root of a volume.

NetWare junctions cannot target OES servers.

6.16 OpenLDAP on OES

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

6.17 Samba

For Samba implementation caveats, see "Samba Caveats" in the *OES 11 SP2: Novell Samba Administration Guide*.

6.18 SLP Registrations Are Not Retrieved from a Novell SLP DA

By default, the OpenSLP DA cannot retrieve SLP registrations from the Novell SLP DA during startup. For information on resolving this issue, see [TID 7009783 \(http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7009783&sliceId=1&docTypeID=DT_TID_1_1&dialogID=281740290&statId=0%200%20281736877\)](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7009783&sliceId=1&docTypeID=DT_TID_1_1&dialogID=281740290&statId=0%200%20281736877).

6.19 Synchronizing NMAS Login Methods Is Required to Avoid Login Failures

NMAS (NetIQ Modular Authentication Service) provides flexible login options, including support for smart cards, proximity cards, passwords, etc.

OES services, such as Novell AFP and Novell CIFS include NMAS login methods that are installed in eDirectory at the same time as the services. Macintosh and Windows users can then log into OES just as they would log into a native AFP or CIFS server.

After an NMAS login method is installed in eDirectory, it must be synchronized to all of the eDirectory replicas in the tree. Replica synchronization is, of course, a high system priority. However, it is not guaranteed to be immediate, and on networks with many servers and multiple-replica trees, normal delays in synchronization can result in authentication failures.

For example, when an AFP user requests a connection to an OES server running Novell AFP, NMAAS can direct the login request to any eDirectory server that has a writable replica of a partition containing the User object. If the AFP login method is not yet synchronized to that particular eDirectory server, the authentication request fails.

To avoid login failures and user frustration, you should make sure that all of your eDirectory servers that hold replicas are synchronized as soon as possible after OES services are installed.

For more information on synchronization, see “[Synchronization](#)” in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

6.20 Using NLVM with Linux Software RAIDs

Linux Software RAIDs are intended to be used with Linux tools and file systems. Consider the caveats in this section before implementing Linux Software RAIDs on your OES server.

- ♦ [Section 6.20.1, “Linux Software RAIDs,” on page 130](#)
- ♦ [Section 6.20.2, “Linux Software RAIDs Are Not Cluster Aware,” on page 130](#)
- ♦ [Section 6.20.3, “Linux Software RAIDs Are Not Recommended for the System Device,” on page 131](#)

6.20.1 Linux Software RAIDs

We recommend that you do not use Linux software RAIDs (such as MD RAIDs and Device Mapper RAIDs) for devices that you plan to use for storage objects that are managed by NSS management tools. The Novell Linux Volume Manager (NLVM) utility and the NSS Management Utility (NSSMU) list Linux software RAID devices that you have created by using Linux tools. Beginning with Linux Kernel 3.0 in OES 11 SP1, NLVM and NSSMU can see these devices, initialize them, and allow you to create storage objects on them. However, this capability has not yet been fully tested.

IMPORTANT: In OES 11, a server hang or crash can occur if you attempt to use a Linux software RAID when you create storage objects that are managed by NSS management tools.

For NSS pools, you can use hardware RAID devices or NSS Software RAID devices to achieve disk fault tolerance.

For Linux POSIX volumes, LVM volume groups, and cLVM volume groups, you can use hardware RAID devices on your storage subsystem to achieve disk fault tolerance.

6.20.2 Linux Software RAIDs Are Not Cluster Aware

Do not use Linux Software RAIDs for devices that you plan to use for shared storage objects. Linux Software RAID devices do not support concurrent activation on multiple nodes; that is, they are not cluster aware. They cannot be used for shared-disk storage objects, such as the OCFS2 file system, cLVM volume groups, and Novell Cluster Services SBD (split-brain-detector) partitions.

For shared disks, you can use hardware RAID devices on your storage subsystem to achieve fault tolerance.

6.20.3 Linux Software RAID's Are Not Recommended for the System Device

We recommend that you do not use Linux software RAID's (such as MD RAID's and Device Mapper RAID's) on the system device if you plan to use free space on the device later for storage objects managed by NSS tools. During the SLES and OES installation, if you create a Linux software RAID device to use as the system device for the root (/) file system, the free space on the system device cannot be used later for NSS pools because the configuration of NSS storage objects on Linux software RAID's has not yet been fully tested.

IMPORTANT: In OES 11, a server hang or crash can occur if you attempt to use a Linux software RAID when you create storage objects that are managed by NSS management tools.

For the Linux system device, you can use a hardware RAID device to achieve fault tolerance. This allows NSS tools to see and use any available free space on the system device for unshared NSS pools.

6.21 Virtualization

The following are caveats for setting up OES 11 server in Xen VMs:

- [Section 6.21.1, "Always Close Virtual Machine Manager When Not in Use," on page 131](#)
- [Section 6.21.2, "Always Use Timesync Rather Than NTP," on page 131](#)
- [Section 6.21.3, "Backing Up a Xen Virtual Machine," on page 131](#)
- [Section 6.21.4, "Time Synchronization and Virtualized OES," on page 132](#)
- [Section 6.21.5, "NSS Considerations," on page 132](#)

6.21.1 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.

6.21.2 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.

6.21.3 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.

6.21.4 Time Synchronization and Virtualized OES

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 \(http://www.suse.com/documentation/sles11/book_xen/data/sec_xen_guests_suse_time.html\)](http://www.suse.com/documentation/sles11/book_xen/data/sec_xen_guests_suse_time.html) in the *Virtualization with Xen* (http://www.suse.com/documentation/sles11/book_xen/data/book_xen.html) guide.

6.21.5 NSS Considerations

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

- ♦ **OES:** Data shredding is not supported.

7 Upgrading to OES 11 SP2

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

- ♦ [Section 7.1, “Caveats to Consider Before Upgrading,” on page 133](#)
- ♦ [Section 7.2, “OES 11 SP2 Upgrade Paths,” on page 134](#)
- ♦ [Section 7.3, “NetWare 6.5 SP8 Upgrade Paths,” on page 134](#)

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 133](#)
- ♦ [Section 7.1.2, “Only One eDirectory Instance Is Supported on OES Servers,” on page 133](#)
- ♦ [Section 7.1.3, “Before Upgrading to OES 11 SP2 You Must Update Sentinel,” on page 133](#)

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 and OES 11:** Applications installed on OES 2 and later servers 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 11 SP2”](#) in the *OES 11 SP2: Installation Guide*.

7.1.2 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 122](#).

7.1.3 Before Upgrading to OES 11 SP2 You Must Update Sentinel

Before upgrading to OES 11 SP2 from OES 2 SP 3, you must update the system with the [latest Sentinel agent](#) (<http://support.novell.com/products/sentinel/secure/sentinelplugins.html>).

Otherwise, the SLES 11 server might experience problems booting.

For more information, see the SLES 10 SP3 entry in [“Preparing the Server You Are Upgrading”](#) in the *OES 11 SP2: Installation Guide*.

7.2 OES 11 SP2 Upgrade Paths

The following are supported upgrade paths for OES 11 SP2:

Table 7-1 Supported OES 11 Upgrade Paths

Source	Destination
OES 2 SP3 (64-bit)	OES 11 SP2
OES 11	OES 11 SP2
OES 11 SP1	OES 11 SP2

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 11 SP2](#)” in the *OES 11 SP2: Installation Guide*.

In addition to upgrading the server itself, data and service migrations are also supported. For more information, see “[Planning for Migration](#)” in the *OES 11 SP2: Migration Tool Administration Guide*.

7.3 NetWare 6.5 SP8 Upgrade Paths

For help upgrading from NetWare to OES 11 SP2, see the *OES 11 SP2: Upgrading to OES—Best Practices Guide*.

8 Migrating Existing Servers and Data

This section briefly outlines the following migration topics:

- ♦ [Section 8.1, “Supported OES 11 SP2 Migration Paths,” on page 135](#)
- ♦ [Section 8.2, “Migration Tools and Purposes,” on page 135](#)

8.1 Supported OES 11 SP2 Migration Paths

For a complete list of Open Enterprise Server migration scenarios and paths, see “[Migration Scenarios](#)” in the *OES 11 SP2: Migration Tool Administration Guide*.

8.2 Migration Tools and Purposes

The OES 11 SP2 Migration Tool lets you migrate and/or consolidate data and services from one or more NetWare, OES 1, OES 2, or OES 11 source servers to an OES 11 SP2 target server. See “[Source Platform Support for OES 11 SP2 Services](#)” in the *OES 11 SP2: Migration Tool Administration Guide*.

You can also transfer a complete server identity, including its IP address, hostname, eDirectory identity, NCI keys, and certificates. For more information, see “[Transfer ID](#)” in the *OES 11 SP2: Migration Tool Administration Guide*.

9 Virtualization in OES 11 SP2

Open Enterprise Server 11 SP2 runs as a VM guest on any virtual machine host server that is certified for running Suse Linux Enterprise Server 11 SP3 (SLES 11 SP3) as a paravirtualized guest. Because Xen and KVM are distributed with SLES 11 SP3, they are mentioned more particularly in the OES documentation.

For a list of the VM host platforms that are certified for SLES 11 SP3, see [Section 2.4.4, “Supported Virtualization Hosts”](https://www.suse.com/documentation/sles11/book_sle_deployment/data/sec_x86_sysreqs.html) (https://www.suse.com/documentation/sles11/book_sle_deployment/data/sec_x86_sysreqs.html) in the *SLES 11 Deployment Guide* (https://www.suse.com/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html).

NetWare guest servers are supported only on Xen host servers. NetWare is not supported as a guest on a KVM virtual machine host server.

For information about installing and running OES 11 SP2 services on virtual machines, see the links on the [Virtualization page of the OES 11 Online Documentation](http://www.novell.com/documentation/oes11/index.html#cat_virtualization) (http://www.novell.com/documentation/oes11/index.html#cat_virtualization).

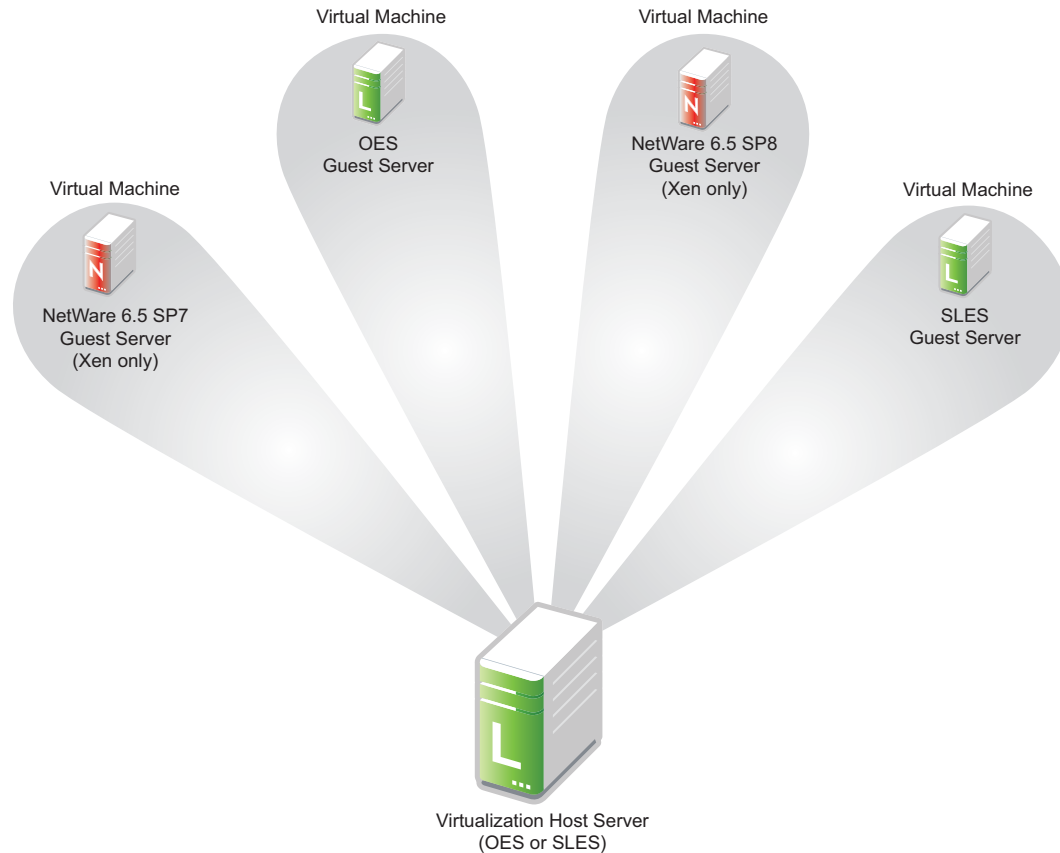
- ♦ [Section 9.1, “Graphical Overview of Virtualization in OES 11 SP2,” on page 137](#)
- ♦ [Section 9.2, “Why Install OES Services on Your VM Host?,” on page 138](#)
- ♦ [Section 9.3, “Services Supported on VM Hosts and Guests,” on page 139](#)
- ♦ [Section 9.4, “Xen VMs Need Ext2 for the System /Boot Volume,” on page 140](#)

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

9.1 Graphical Overview of Virtualization in OES 11 SP2

[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 Virtualization in OES 11 SP2



9.2 Why Install OES Services on Your VM Host?

Novell supports three OES services running on a Xen VM host server: Novell Linux User Management, Novell Storage Management Services, and Novell Cluster Services.

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 [“Section 11.5.2, “Setting Up SSH Access for LUM-enabled eDirectory Users,” on page 157.”](#)
- ♦ **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.

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 3.9.20](#), “Unsupported Service Combinations,” on page 102).

Table 9-1 Services Supported on VM Hosts and Guests

OES 11 SP2 Service	Linux VM Host	OES 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		✓ (3.9)	✓ (2.1x)
iManager		✓	✓
iPrint	✓	✓	✓
Linux User Management	✓	✓	
NCP Server/Dynamic Storage Technology		✓	
NetStorage		✓	✓
Novell Remote Manager (NRM)		✓	✓
Novell Storage Services (NSS)		✓	✓
QuickFinder		✓	✓
Samba		✓	

IMPORTANT: Adding OES services to a Xen VM host requires that you boot the server with the regular kernel prior to adding the services. See the instructions in the Important note in [“Adding/Configuring OES Services on an Existing Server”](#) in the *OES 11 SP2: Installation Guide*.

9.4 Xen VMs Need Ext2 for the System /Boot Volume

It is recommended that operating systems running in paravirtual mode set up their kernel on a separate partition that uses a non-journaling file system, such as ext2.

Before a paravirtualized operating system can boot, the management domain must construct a virtual machine and place the paravirtualized kernel in it. Then, the paravirtualized operating system boots. To retrieve the kernel during the bootstrapping process, the virtual machine's boot disk is mounted in read-only mode, the kernel is copied to the virtual machine's memory, and then the boot disk is unmounted.

When a virtual machine's operating system crashes, its disks are not shut down in an orderly manner. This should not pose a problem to a virtual machine running in full virtualization mode because the pending disk entries are checked and corrected the next time the operating system starts. If the disk is using a journaling file system, the journal is replayed to update and coordinate any pending disk entries.

This type of system crash poses a potential problem for paravirtualized operating systems. If a paravirtualized operating system using a journaled file system crashes, any pending disk entries cannot be updated and coordinated because the file system is initially mounted in read-only mode.

Therefore, it is recommended that you set virtual machine boot files, such as the kernel and ramdisk, on a separate partition that is formatted with a non-journaling file system, such as ext2.

10 Clustering and High Availability

Open Enterprise Server 11 SP2 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 OES during the migration to OES.
For more information, see the [OES 11 SP2: Novell Cluster Services NetWare to Linux Conversion Guide](#).
- ♦ 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 [OES 11 SP2: Novell Cluster Services for Linux Administration Guide](#).

11 Managing OES 11 SP2

This section includes the following topics:

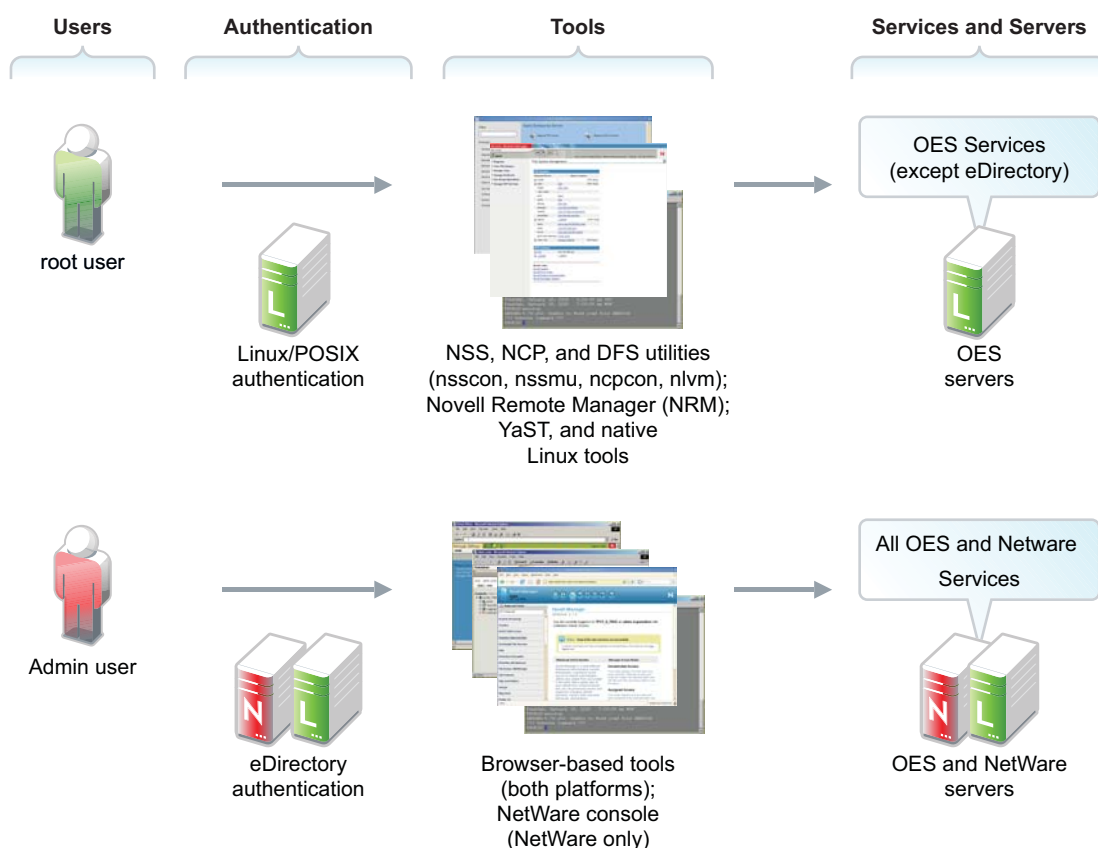
- ♦ [Section 11.1, “Overview of Management Interfaces and Services,”](#) on page 143
- ♦ [Section 11.2, “Using OES 11 SP2 Welcome Pages,”](#) on page 144
- ♦ [Section 11.3, “OES Utilities and Tools,”](#) on page 145
- ♦ [Section 11.4, “iManager Differences on OES,”](#) on page 155
- ♦ [Section 11.5, “SSH Services on OES 11 SP2,”](#) on page 155

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 11 servers, require local authentication.

For more information, see [Section 11.3, “OES Utilities and Tools,”](#) on page 145.

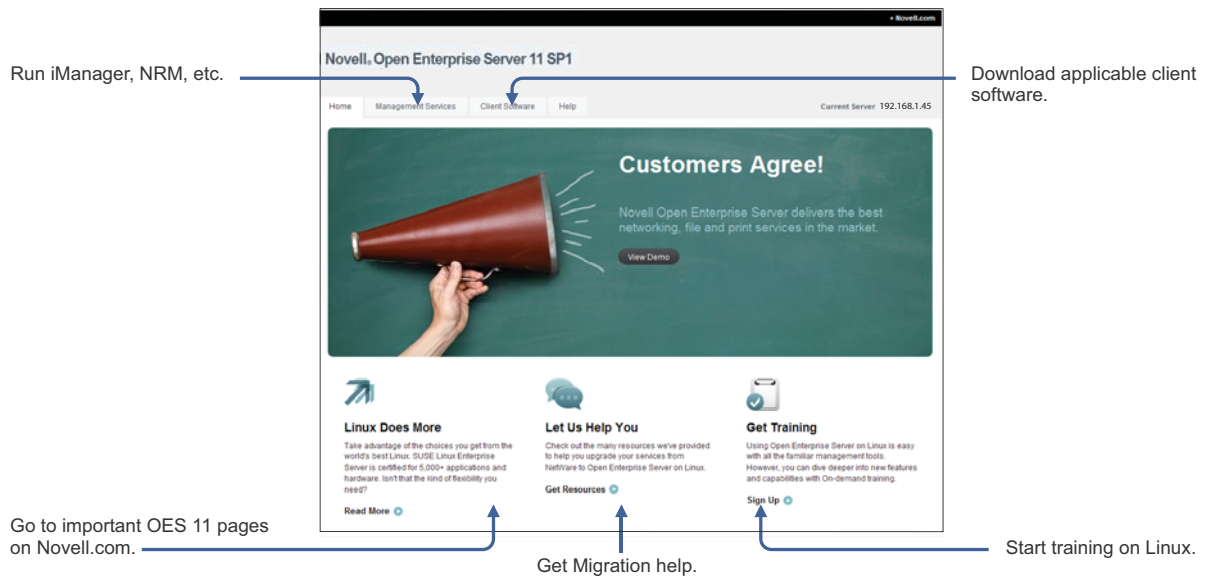
Figure 11-1 Management Interfaces and Services



11.2 Using OES 11 SP2 Welcome Pages

After you install an OES 11 SP2 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 144](#)
- ♦ [Section 11.2.2, “Accessing the Welcome Web Site,” on page 145](#)
- ♦ [Section 11.2.3, “The Welcome Web Site Is Available to All Users,” on page 145](#)
- ♦ [Section 11.2.4, “Administrative Access from the Welcome Web Site,” on page 145](#)

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 11 SP2 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 11 SP2 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 11 SP2 server.

11.2.2 Accessing the Welcome Web Site

Anyone with browser access to an OES 11 SP2 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 11 SP2 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, it 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 11 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 “[OES 11 SP2: Linux Tips for NetWare Administrators](#),” a reference that outlines the OES equivalents for most of the familiar CLI tools on NetWare.

Novell OES 11 SP2 includes several administration utilities that let you manage everything in your network, from configuring and managing eDirectory to setting up network services and open source software. This section lists and briefly explains the most common utilities.

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

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

Table 11-1 OES Management Tool Quick Reference

Tool	Tasks	Access Method or URL/ Username	Notes
bash	<ul style="list-style-type: none">♦ Manage the Linux server.♦ Manage many services running on the server.	Access a command prompt on the Linux server.	For more information or help understanding and using bash, search the Web for any of the numerous articles and tutorials on using the shell.

Tool	Tasks	Access Method or URL/ Username	Notes
Health Monitoring Services	<ul style="list-style-type: none"> Monitor the health of OES servers. 	<p>OES 11 SP2 uses Ganglia and Nagios to provide health monitoring. The NRM Health Monitor is no longer available. Ganglia and Nagios do not depend on SFCB.</p> <p>Access for Ganglia:</p> <ol style="list-style-type: none"> Go to <code>http://server_ip_address:8008</code>. Log in to NRM as the root user. Select <i>Diagnose Server > Server Health Values</i>. <p>Access for Nagios:</p> <ol style="list-style-type: none"> Go to <code>http://server_ip_address:8008</code>. Log in to NRM as the root user. On the first access, you must set up a password for the Nagios user <code>nagiosadmin</code>. <p>Click the Configuration icon in the NRM toolbar.</p> <p>On the Configuration Options page under <i>Nagios Configuration Options</i>, click <i>Nagios User Management</i>.</p> <p>Type <code>nagiosadmin</code>, type and confirm the password, then click <i>Create User</i>.</p> <ol style="list-style-type: none"> Select <i>Diagnose Server > Server Health Services</i>. Click <i>Nagios Service Detail</i>. When you are prompted, authenticate with the <code>nagiosadmin</code> user and password, then click <i>OK</i>. 	<p>Log in as the root user to access health metrics. When you access Nagios details, you must additionally log in as a Nagios user that you configure for your Nagios monitoring system.</p> <p>Ganglia and Nagios provide health monitoring capabilities that match or exceed those provided by the Health Monitor on OES 11 SP1 and earlier. The interfaces do not mimic the old Health Monitor; rather, they are specific to Ganglia and Nagios.</p> <p>For more information, see the OES 11 SP2: Novell Remote Manager Administration Guide.</p> <p>For information about monitoring services in Ganglia, see the Ganglia open source project Web site (http://ganglia.sourceforge.net/).</p> <p>For information about monitoring services in Nagios, see the Nagios open source project Web site (http://www.nagios.org/).</p> <p>Health Monitoring Services on OES 11 SP2 use a Common Information Model (CIM) provided by the SFCB Initiative. For more information on WBEM, visit the DMTF Web site (http://www.dmtf.org/standards/wbem).</p>

Tool	Tasks	Access Method or URL/ Username	Notes
iManager 2.7	<ul style="list-style-type: none"> ♦ Access various other management tools and plug-ins. ♦ Configure OES network services. ♦ Create and manage users, groups, and other objects. ♦ Delegate administration through Role-Based Services (RBS). ♦ Manage eDirectory objects, schema, partitions, and replicas. ♦ Manage OES 11 SP2 services ♦ Set up and manage your NetIQ eDirectory tree. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: <code>http://IP_or_DNS/iManager.html</code> 2. Specify the eDirectory Admin username and password. 	<p>Requires an SSL connection (HTTPS).</p> <p>Both HTTP and HTTPS requests establish the SSL connection.</p> <p>For more information on using iManager, see the NetIQ® iManager Administration Guide.</p> <p>See also iManager Workstation.</p>
iManager Workstation (formerly Mobile iManager)	<ul style="list-style-type: none"> ♦ Manage eDirectory. ♦ Create and manage users, groups, and other objects. ♦ Manage OES 11 SP2 services. ♦ Access various other management tools and plug-ins. 	<p>On a Linux workstation:</p> <ol style="list-style-type: none"> 1. At the <code>bin</code> directory of the expanded <code>iMan_25_Mobile_iManager_linux.tar</code> directory, run <code>imanager.sh</code>. 2. Log in, using the eDirectory Admin username, password, and eDirectory tree name. <p>On a Windows workstation:</p> <ol style="list-style-type: none"> 1. At the <code>bin</code> directory of the unzipped <code>iMan_25_Mobile_iManager_win</code> directory, run <code>imanager.bat</code>. 2. Log in, using the eDirectory Admin username, password, and eDirectory tree name. 	<p>Requires an SSL connection (HTTPS).</p> <p>Both HTTP and HTTPS requests establish the SSL connection.</p> <p>For more information on using iManager Workstation, see “Accessing iManager Workstation” in the NetIQ® iManager Administration Guide.</p> <p>See also iManager.</p>

Tool	Tasks	Access Method or URL/ Username	Notes
iMonitor	<ul style="list-style-type: none"> ♦ Monitor and diagnose all the servers in your eDirectory tree. ♦ Examine eDirectory partitions, replicas, and servers. ♦ Examine current tasks taking place in the tree. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter one of the following URLs: (On NetWare) <code>http://IP_or_DNS:81/nds</code> (On Linux) <code>https://IP_or_DNS:8030/nds</code> 2. Specify the eDirectory Admin username and password. 	<p>iMonitor provides a Web-based alternative to tools such as DSBrowse, DSTrace, DSDiag, and the diagnostic features available in DSRepair.</p> <p>Because of this, iMonitor's features are primarily server focused, meaning that they report the health of individual eDirectory agents (running instances of the directory service) rather than the entire eDirectory tree.</p> <p>For more information, see "Using NetIQ iMonitor" in the <i>NetIQ eDirectory 8.8 SP8 Administration Guide</i>.</p>
iPrint Map Designer	<ul style="list-style-type: none"> ♦ Create a printer map to aid in printer selection/installation. ♦ Edit an existing printer map. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: <code>http://IP_or_DNS/ippdocs/maptool.htm</code> 2. Specify the eDirectory Admin username and password. 	<p>For OES 11 SP2 server instructions, see "Setting Up Location-Based Printing" in the <i>OES 11 SP2: iPrint Linux Administration Guide</i>.</p>
NetStorage Web Interface	<ul style="list-style-type: none"> ♦ Manage file system access. ♦ Manage file system space restrictions. ♦ Salvage and purge deleted files. 	Use the NetStorage Web interface.	<p>As an Admin user (or equivalent), you can set directory and user quotas for NSS data volumes. You can also set file system trustees, trustee rights, and attributes for directories and files on NSS volumes. And you can salvage and purge deleted files.</p> <p>For more information, see "Viewing or Modifying Directory and File Attributes and Rights" in the <i>OES 11 SP2: NetStorage Administration Guide for Linux</i>.</p>

Tool	Tasks	Access Method or URL/ Username	Notes
Novell Client	<ul style="list-style-type: none"> ♦ Manage file system access. ♦ Manage File System Space Restrictions. ♦ Salvage and purge deleted files. 	Use the Novell N icon to access these and other tasks.	<p>As an Admin user (or equivalent), you can set directory and user quotas for NSS data volumes. You can also set file system trustees, trustee rights, and attributes for directories and files on NSS volumes. And you can salvage and purge deleted files.</p> <p>For more information, see “Managing File Security and Passwords” in the <i>Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide</i>.</p>
Novell iFolder 3.9.2	<ul style="list-style-type: none"> ♦ Manage various aspects of iFolder 3.9.2. 	1. In iManager 2.7, click <i>iFolder 3.9.2 > Launch iFolder Admin Console</i> .	<p>For more information on managing iFolder 3.9.2, see the following in the <i>Novell iFolder 3.9.2 Administration Guide</i>:</p> <ul style="list-style-type: none"> ♦ “Managing an iFolder Enterprise Server” ♦ “Managing iFolder Services via Web Admin ” ♦ “Managing iFolder Users” ♦ “Managing an iFolder Web Access Server” ♦ “Managing iFolders”
Novell Linux Volume Manager	<ul style="list-style-type: none"> ♦ Manage the NSS file system using console commands or script files. ♦ Create NCP volumes on existing POSIX volumes. 	1. Use the <code>nlvm</code> command at the command line.	For more information, see the OES 11 SP2: NLVM Reference .

Tool	Tasks	Access Method or URL/ Username	Notes
Novell Remote Manager (NRM)	<ul style="list-style-type: none"> ♦ Manage file system attributes for the NSS File System ♦ Manage the NCP Server ♦ Manage NCP connections and open files for NSS and NCP volumes ♦ Manage CIFS connections and open files for NSS volumes ♦ Manage AFP connections and open files NSS volumes ♦ Manage Dynamic Storage Technology ♦ Manage OES 11 SP2 servers from a remote location ♦ Monitor the server health metrics, status, and alert notifications ♦ Change server configurations ♦ Perform diagnostic and debugging tasks ♦ View file system inventories ♦ View NCP volume inventories ♦ View trustee reports for NSS volumes 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: https:// IP_or_DNS:8009 2. Specify the root user and password. 	<p>Functionality is limited for non-root users.</p> <p>NRM on Linux doesn't include all the functionality of NRM on NetWare.</p> <p>For more information, see the OES 11 SP2: Novell Remote Manager Administration Guide.</p>

Tool	Tasks	Access Method or URL/ Username	Notes
NSS Management Utility (NSSMU)	<ul style="list-style-type: none"> ♦ Manage the Novell Storage Services file system. ♦ Manage Linux POSIX volumes for native Linux file systems. 	<p>At a terminal prompt:</p> <ol style="list-style-type: none"> 1. Load NSSMU by entering <code>/opt/novell/nss/sbin/nssmu</code> 	<p>NSS Management Utility (NSSMU) is a server console application used to manage the Novell Storage System (NSS) file system. It also allows you to create and manage Linux POSIX volumes for native Linux file systems, and it includes support for NCP volumes and Novell Cluster Services.</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 <i>OES 11 SP2: NSS File System Administration Guide for Linux</i>.</p>
OpenSSH (client access)	<ul style="list-style-type: none"> ♦ Securely run commands on remote servers. ♦ Securely copy files and directories to and from other servers using SSH utilities. 	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 Section 11.5, “SSH Services on OES 11 SP2,” on page 155.
OpenSSH (Linux)	<ul style="list-style-type: none"> ♦ Manage a SLES 11 SP3 (OES 11 SP2) server by using OpenSSH. 	<ol style="list-style-type: none"> 1. Use standard SSH connection and management options. 	<p>Requirements:</p> <ul style="list-style-type: none"> ♦ The firewall must allow for SSH access. ♦ eDirectory users must be enabled for SSH access. For more information, see Section 11.5, “SSH Services on OES 11 SP2,” on page 155.

Tool	Tasks	Access Method or URL/ Username	Notes
Perl	<p>A programming language developed by Larry Wall that</p> <ul style="list-style-type: none"> ♦ Runs faster than shell script programs. ♦ Reads and writes binary files. ♦ Processes very large files. ♦ Lets you quickly develop CGI applications. 	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.
QuickFinder Server Manager	<ul style="list-style-type: none"> ♦ Create search indexes for any Web site or attached file systems. ♦ Modify the search dialog look-and-feel to match your corporate design. Create full-text indexes of HTML, XML, PDF, Word, OpenOffice.org, and many other document formats. ♦ Configure and maintain your indexes remotely from anywhere on the Net. 	<ol style="list-style-type: none"> 1. In a supported Web browser, enter the following URL: http://IP_or_DNS/qfsearch/admin 2. Specify the <code>root</code> or other user as documented. 	<p>Local users and any eDirectory users that are enabled for Linux access (LUM) can be assigned rights to manage QuickFinder.</p> <p>For more information, see the QuickFinder 5.0 Server Administration Guide.</p>
Remote Manager			See Novell Remote Manager .

Tool	Tasks	Access Method or URL/ Username	Notes
SNMP for eDirectory	<p>Lets you use standard SNMP tools to</p> <ul style="list-style-type: none"> ♦ Monitor an eDirectory server. ♦ Track the status of eDirectory to verify normal operations. ♦ Spot and react to potential problems when they are detected. ♦ Configure traps and statistics for selective monitoring. ♦ Plot a trend on the access of eDirectory. ♦ Store and analyze historical data that has been obtained through SNMP. ♦ Use the SNMP native master agent on all eDirectory platforms. 	<ol style="list-style-type: none"> 1. Configure SNMP for eDirectory as documented for your platform. 2. Access SNMP for eDirectory services using the SNMP management interface of your choice. 3. Specify the eDirectory Admin username and password. 	<p>SNMP support is installed with eDirectory.</p> <p>For more information on SNMP for eDirectory, see “SNMP Support for NetIQ eDirectory” in the <i>NetIQ eDirectory 8.8 SP8 Administration Guide</i>.</p>
SUSE Linux Monitoring Utilities	<ul style="list-style-type: none"> ♦ Manage the Linux server and standard Linux services from the command prompt. 	Enter the desired command at the command prompt.	For more information, see “ System Monitoring ” (http://www.suse.com/documentation/sles11/book_sle_tuning/data/part_tuning_monitoring.html) in the <i>SLES 11 SP3: System Analysis and Tuning Guide</i> (http://www.suse.com/documentation/sles11/book_sle_tuning/data/book_sle_tuning.html).
YaST (SUSE Linux)	<ul style="list-style-type: none"> ♦ Install OES 11 SP2. ♦ Configure the server and standard Linux services. ♦ Install OES components and services. 	<p>To access YaST from the GNOME interface, start the YaST Control Center by clicking <i>Computer > YaST</i>.</p> <p>To access YaST at a command prompt, enter <code>yast</code>.</p>	For more information, see “ Installation with YaST ” (http://www.suse.com/documentation/sles11/book_sle_deployment/data/cha_inst.html) in the <i>SLES 11 SP3: Deployment Guide</i> (https://www.suse.com/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html), and the <i>SLES 11: Administration Guide</i> (http://www.suse.com/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html) .

11.4 iManager Differences on OES

Self-Signed Certificates

As explained in the *NetIQ iManager Installation Guide*, the iManager instructions for dealing with self-signed certificates don't apply to OES Linux.

OES installs Tomcat and Apache versions that are specific to OES (see [Section 6.14, "Novell-tomcat Is for OES Use Only," on page 128](#)). For instructions on replacing the self-signed Apache/Tomcat certificate on OES, see [Section 23.2, "Setting Up Certificate Management," on page 309](#).

11.5 SSH Services on OES 11 SP2

This section documents the following topics:

- ♦ [Section 11.5.1, "Overview," on page 155](#)
- ♦ [Section 11.5.2, "Setting Up SSH Access for LUM-enabled eDirectory Users," on page 157](#)

11.5.1 Overview

SSH services on SLES 11 are provided by [OpenSSH \(http://www.openssh.org\)](http://www.openssh.org), a free version of SSH connectivity tools developed by the [OpenBSD Project \(http://www.openbsd.org/\)](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 11 SP2 services can be managed at a command prompt via an SSH session, it is important to understand how SSH access is controlled in OES 11 SP2.

This section discusses the following topics:

- ♦ ["When Is SSH Access Required?" on page 155](#)
- ♦ ["How SSH Access for eDirectory Users Works" on page 156](#)
- ♦ ["SSH Security Considerations" on page 156](#)

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 11 SP2 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 if 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 11 SP2 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 PAM-enabled service:** In OES 11 SP2, 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 as a PAM-enabled service on each server.
- ♦ **PAM-enabling:** After SSH is included as a PAM-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 a group of users.

11.5.2 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 157](#)
- ♦ [“Adding SSH as an Allowed Service in LUM” on page 157](#)
- ♦ [“Enabling Users for LUM” on page 158](#)
- ♦ [“Restricting SSH Access to Only Certain LUM-Enabled Users” on page 158](#)
- ♦ [“Providing SSH Access for Samba Users” on page 159](#)

Allowing SSH Access Through the Firewall

NOTE: This section assumes you are allowing SSH access on an installed server.

SSH can also be enabled during an OES installation by clicking the *SSH Port Is Blocked* button on the Firewall screen.

- 1 On the OES 11 SP2 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 (PAM-enabled) service for Linux User Management on the server, skip to [“Enabling Users for LUM” on page 158](#).
or
If SSH is not an allowed (PAM-enabled) service for Linux User Management on the server, continue with [Step 2](#).
- 2 On the OES 11 SP2 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 finished loading, 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 11 SP2: Novell Linux User Management Administration 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 159](#).

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 158](#).

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 11 SP2 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 `uamPosicPAMServiceExcludeList` 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 158](#) as a general guide.

12 Network Services

The term “network services” as used in this section, refers to the 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 161](#)
- ♦ [Section 12.2, “DNS and DHCP,” on page 162](#)
- ♦ [Section 12.3, “Time Services,” on page 164](#)
- ♦ [Section 12.4, “Discovery Services,” on page 175](#)
- ♦ [Section 12.5, “SLP,” on page 176](#)

For links to more information and tasks, see the “[network protocols \(http://www.novell.com/documentation/oes11/index.html#cat_network-protocols-services\)](http://www.novell.com/documentation/oes11/index.html#cat_network-protocols-services)” links in the OES 11 SP2 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 11 SP2 includes the standard Linux TCP/IP support on SUSE Linux Enterprise Server 11 SP3.

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 11 SP2 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 11 SP2,” on page 162](#)
- ♦ [Section 12.2.2, “DHCP Differences Between NetWare and OES 11 SP2,” on page 163](#)

12.2.1 DNS Differences Between NetWare and OES 11 SP2

As you plan to upgrade from NetWare to OES 11 SP2, consider the following differences between DNS on NetWare and OES 11 SP2:

Table 12-1 DNS: NetWare 6.5 SP8 vs. OES 11 SP2

Feature or Command	NetWare 6.5 SP8	OES 11 SP2
Auditing	Yes	No
Console commands:		
♦ Check Status	♦ <code>named status</code>	♦ <code>rcnovell-named status</code>
♦ Force Zone-in	♦ <code>-zi zone_name</code>	N/A
♦ Purge All Cache	♦ <code>-pa</code>	N/A
♦ Screen Logging	♦ <code>-s</code>	N/A
♦ Start the server	♦ <code>named</code>	♦ <code>rcnovell-named start</code> or ♦ <code>/etc/init.d/novell-named start</code>
♦ Stop the server	♦ <code>named stop</code>	♦ <code>rcnovell-named stop</code>
♦ Unsupported <code>named</code> command parameters	♦ N/A	♦ <code>[-dc categories]</code> ♦ <code>[-mstats]</code> ♦ <code>[-nno_of_cpus]</code> ♦ <code>[-qstats]</code>
♦ Zone Information	♦ <code>-info file_name</code>	N/A
DNSMaint	Yes	Yes - <code>dns-maint</code>
Fault Tolerance	Yes	Yes
Filenames and paths:		

Feature or Command	NetWare 6.5 SP8	OES 11 SP2
♦ Server binary	♦ <code>sys:/system/named.nlm</code>	♦ <code>/opt/novell/named/bin/novell-named</code>
♦ .db, .jnl 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>
Journal log size	Specify at the command prompt by using the <code>jsize</code> argument.	Specify using Java Console, <i>DNS Server Object>Advanced tab > max-journal-size field</i> .
Management	iManager Command Line Interface	Java Console Command Line Interface Unlike the Netware implementation, command line parameters cannot be passed when loading and unloading.
SNMP Support	Yes	No

12.2.2 DHCP Differences Between NetWare and OES 11 SP2

As you plan to upgrade from NetWare to OES 11 SP2, consider the following differences between DHCP on NetWare and OES 11 SP2:

Table 12-2 DHCP: NetWare 6.5 SP8 vs. OES 11 SP2

Feature or Command	NetWare 6.5 SP8	OES 11 SP2
Auditing	Yes	No
Filenames and paths:		
♦ Conf file	♦ N/A	♦ <code>/etc/dhcpd.conf</code>
♦ Leases	♦ Stored in eDirectory	♦ <code>/var/lib/dhcp/db/dhcpd.leases</code>
♦ Log file	♦ <code>sys:/etc/dhcp/dhcpd.log</code>	♦ <code>/var/log/dhcpd.log</code>
♦ Startup log	♦ N/A	♦ <code>/var/log/dhcp-ldap-startup.log</code> This is a dump of DHCP configurations read from eDirectory when the DHCP server starts.
Management	iManager 2.7 (Wizard-based)	Java Console Unlike the NetWare implementation, command line parameters cannot be passed when loading and unloading.

Feature or Command	NetWare 6.5 SP8	OES 11 SP2
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:

- [Section 12.3.1, “Overview of Time Synchronization,” on page 164](#)
- [Section 12.3.2, “Planning for Time Synchronization,” on page 168](#)
- [Section 12.3.3, “Coexistence and Migration of Time Synchronization Services,” on page 171](#)
- [Section 12.3.4, “Implementing Time Synchronization,” on page 172](#)
- [Section 12.3.5, “Configuring and Administering Time Synchronization,” on page 174](#)
- [Section 12.3.6, “Daylight Saving Time,” on page 175](#)

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 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 164](#)
- [“OES Servers as Time Providers” on page 167](#)
- [“OES Servers as Time Consumers” on page 167](#)

Understanding Time Synchronization Modules

During the upgrade to OES 11 SP2, your eDirectory tree might contain servers running different versions of OES, NetWare 6.5 SP8, and/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 vs. NetWare 6.5” on page 165](#)
- [“OES Servers Use the Network Time Protocol \(NTP\) to Communicate” on page 165](#)
- [“Compatibility with Earlier Versions of NetWare” on page 165](#)

OES 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 by using NTP on port 123. However, when installing virtualized NetWare, Timesync should always be used (see [Section 6.21.2, “Always Use Timesync Rather Than NTP,” on page 131](#)).

OES must use the NTP daemon (xntpd).

Figure 12-1 Time Synchronization for Linux and NetWare



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

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

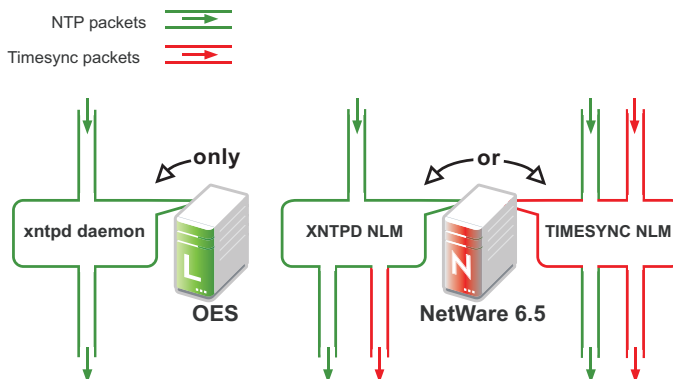
However, this doesn't limit your options on NetWare.

[Figure 12-2](#) illustrates that OES 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



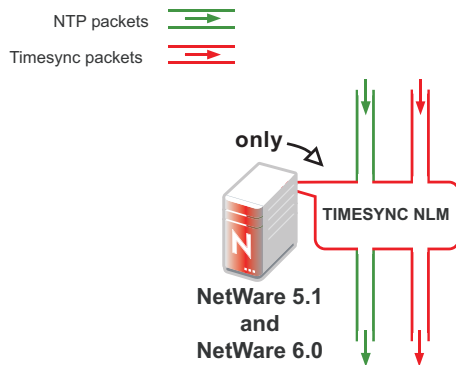
Compatibility with Earlier Versions of NetWare

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.

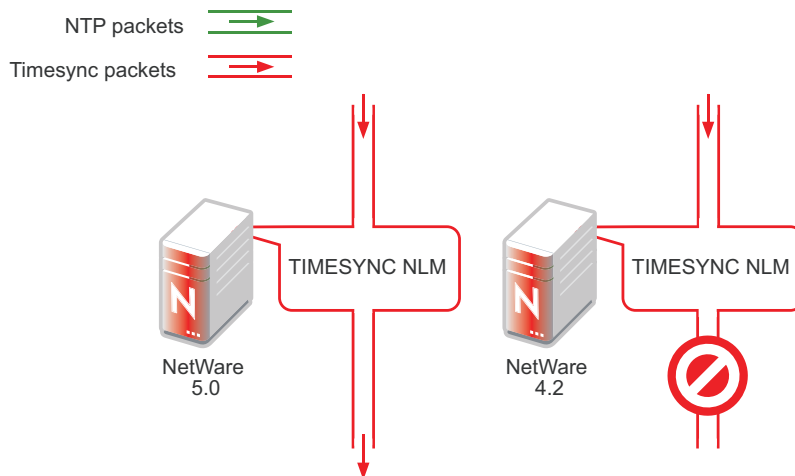
Figure 12-3 NTP Compatibility of NetWare 5.1 and 6.0



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



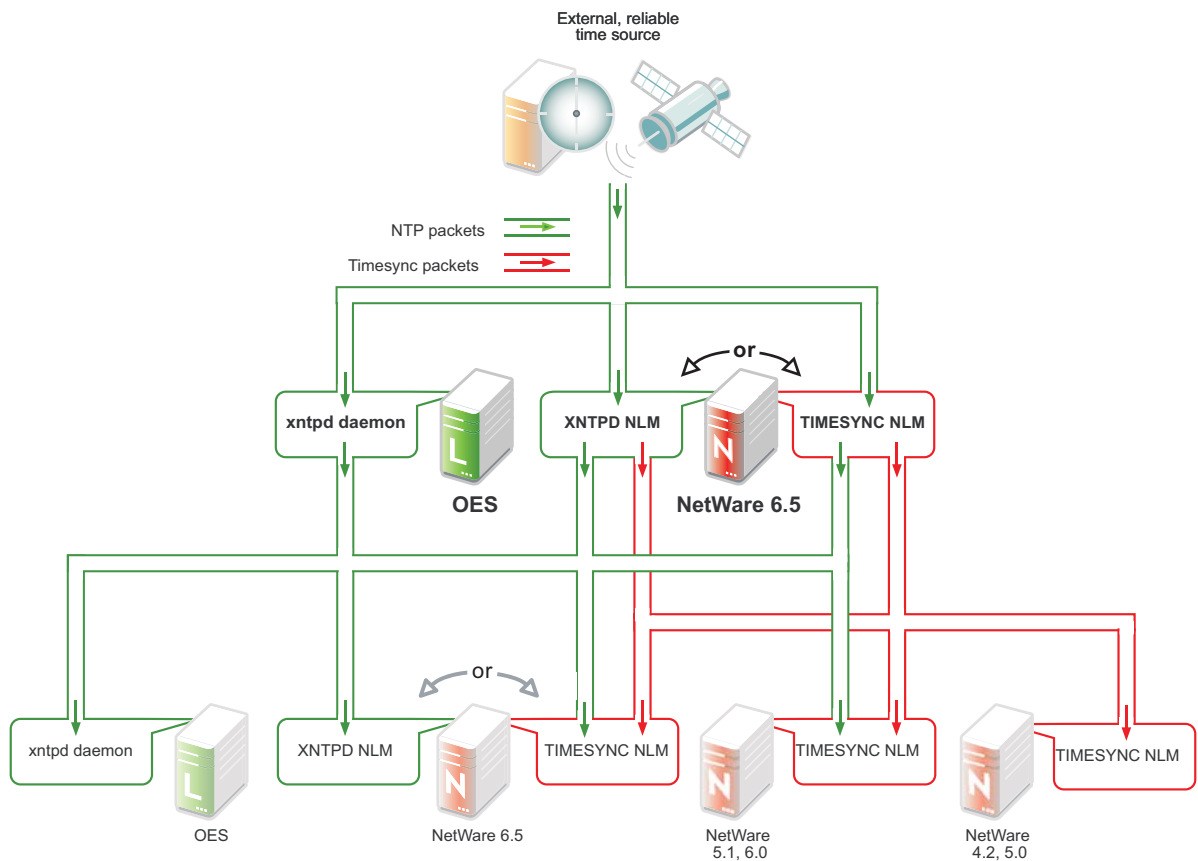
Therefore, if you have NetWare 4.2 or 5.0 servers in your eDirectory tree, and you want to install an OES server, you must have at least one NetWare 5.1 or later server to provide a “bridge” between NTP and Timesync time packets. Figure 12-5 on page 167 illustrates that these earlier server versions 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 Servers as Time Providers

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

Figure 12-5 OES Servers as Time Providers

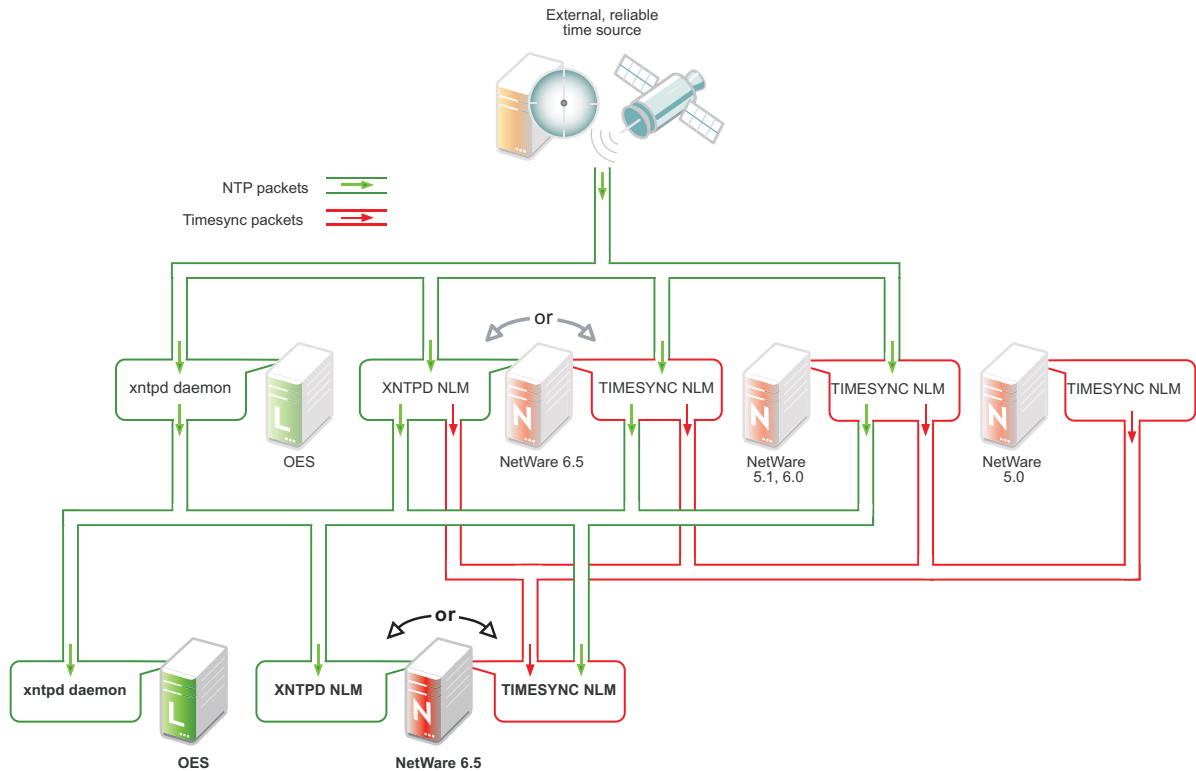


OES Servers as Time Consumers

Figure 12-6 shows the time sources that OES 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 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 168
- ♦ “Choose Timesync for Virtualized NetWare Only” on page 169
- ♦ “Planning a Time Synchronization Hierarchy before Installing OES” on page 169

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 169
- ♦ “Time Synchronization for Trees with More Than Thirty Servers” on page 169
- ♦ “Time Synchronization across Geographical Boundaries” on page 169

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 169.)

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 169.

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

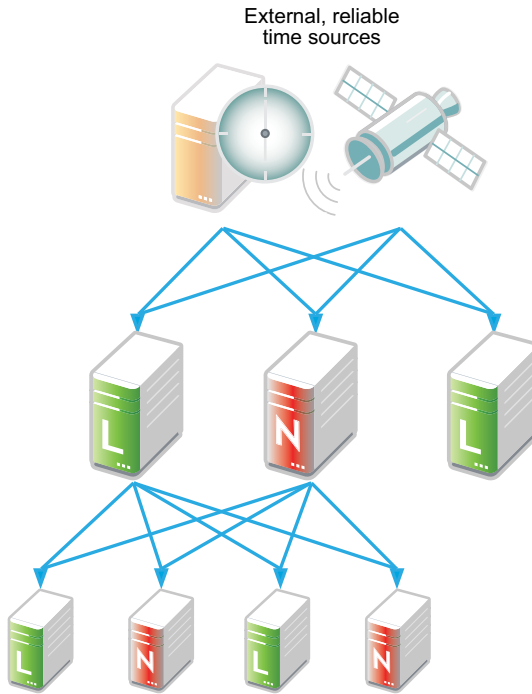
When you install a virtualized NetWare 6.5 server, you should always use Timesync and configure it to communicate using NTP. For more information, see “[You Must Use Timesync for Time Synchronization](#)” in the *OES 11 SP2: Installation Guide*.

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 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 \(http://support.ntp.org/bin/view/Servers/WebHome\)](http://support.ntp.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 166.](#))
- 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 11 SP2 server in /usr/share/doc/packages/xntp and on the Web (<http://www.cis.udel.edu/~mills/ntp.html>)

12.3.3 Coexistence and Migration of Time Synchronization Services

The time synchronization modules in OES have been designed to ensure that new OES 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 171](#)
- ♦ [“Upgrading from NetWare to OES 11 SP2” on page 172](#)

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 servers into your current network.

- ♦ [“Compatibility” on page 171](#)
- ♦ [“Coexistence Issues” on page 172](#)

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 167](#) and [Figure 12-6 on page 168](#).

Table 12-3 Time Synchronization Compatibility

Module	Compatibility
TIMESYNC NLM (NetWare)	Can consume time from
	♦ All previous versions of Timesync. However, the NetWare 4.2 TIMESYNC NLM should not be used as a time source.
	♦ Any TIMESYNC or NTP daemon.
	Can provide time to
	♦ All previous versions of Timesync.
	♦ Any TIMESYNC or NTP daemon.

Module	Compatibility
XNTPD NLM (NetWare)	<p>Can consume time from</p> <ul style="list-style-type: none"> ♦ Any NTP daemon. <p>Can provide time to</p> <ul style="list-style-type: none"> ♦ All previous versions of Timesync. ♦ Any NTP daemon.
xntpd daemon (SLES 11)	<p>Can consume time from</p> <ul style="list-style-type: none"> ♦ Any NTP daemon. <p>Can provide time to</p> <ul style="list-style-type: none"> ♦ Any NTP daemon.
eDirectory	eDirectory gets its time synchronization information from the host OS (Linux or NetWare), not from the time synchronization modules.

Coexistence Issues

If you have NetWare servers earlier than version 5.1, you need to install at least one later version NetWare server to bridge between the TIMESYNC NLM on the earlier server and the OES 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 165](#).

Upgrading from NetWare to OES 11 SP2

The OES 11 SP2 Migration Tool can migrate time synchronization services from NetWare to Linux. For more information, see [“Migrating NTP to OES 11 SP2”](#) in the *OES 11 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 11 SP2 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 173](#)
- ♦ [“Existing Tree” on page 173](#)

New Tree

By default, both the OES 11 SP2 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://support.ntp.org/bin/view/Servers/WebHome) (<http://support.ntp.org/bin/view/Servers/WebHome>) on the Web.

- ♦ “OES 11 SP2” on page 173
- ♦ “NetWare 6.5 SP8” on page 173

OES 11 SP2

When you configure your eDirectory installation, the OES 11 SP2 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 169](#) 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 11 SP2” on page 174
- ♦ “NetWare 6.5 SP8” on page 174

OES 11 SP2

If you are installing into an existing tree, the OES 11 SP2 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 any version of OES.
- ♦ 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 169](#).

The OES 11 SP2 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 11 Server” on page 174](#).

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 169](#)) 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 11 Server” on page 174](#)
- ♦ [“Changing Time Synchronization Settings on a NetWare Server” on page 175](#)

Changing Time Synchronization Settings on a SLES 11 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 11 server by either navigating to the application on the desktop or typing `yast` at the command prompt.
- 2 Click *Network Services > NTP Configuration*.
- 3 In the *Advanced NTP Configuration* dialog box, 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), go to the [Novell Support Knowledgebase \(http://www.novell.com/support/kb/\)](http://www.novell.com/support/kb/) and search for Daylight Saving Time.

12.4 Discovery Services

Various discovery mechanisms are usually available on an OES network.

- ♦ DNS/DHCP
- ♦ Directory services
- ♦ Local host configuration files
- ♦ Service Location Protocol (SLP services)

NOTE: 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 176](#).

- ♦ 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.

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 176](#).

12.5 SLP

The OpenSLP services on OES 11 SP2 are compatible and comparable with NetWare SLP services.

This section discusses the following topics:

- ♦ [Section 12.5.1, “Overview,” on page 176](#)
- ♦ [Section 12.5.2, “Comparing Novell SLP and OpenSLP,” on page 178](#)
- ♦ [Section 12.5.3, “Setting Up OpenSLP on OES 11 SP2 Networks,” on page 179](#)
- ♦ [Section 12.5.4, “Using Novell SLP on OES 11 SP2 Networks,” on page 184](#)
- ♦ [Section 12.5.5, “TIDs and Other Help,” on page 188](#)

12.5.1 Overview

The Service Location Protocol (SLP) was developed so that clients and other software modules can dynamically discover and use services on the network without knowing the IP address or the hostname of the server offering the service.

- ♦ [“Why SLP Is Needed” on page 176](#)
- ♦ [“About the Three SLP Agents and Their Roles” on page 176](#)
- ♦ [“Overcoming the Subnet Limitation” on page 177](#)
- ♦ [“An eDirectory Example” on page 177](#)
- ♦ [“What Happens When a DA Goes Down?” on page 177](#)

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: On the other hand, for OES 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 11 SP2 installation or manually.

About the Three SLP Agents and Their Roles

Three software “agents” provide the infrastructure for SLP-based service discovery:

- ♦ **Service Agents (SAs):** Are a required component of any SLP infrastructure. They act on behalf of a network service that is running on a server by advertising that the service is available.
- ♦ **User Agents (UAs):** Are also required. They act on behalf of clients or other software modules that need network services by searching for the needed services.

- ♦ **Directory Agents (DAs):** Are technically optional, but they are used in most SLP infrastructures. They collect service information from Service Agents so that User Agents can more easily locate the services. DAs are like a phone book directory listing of services on the network.

DAs are not needed when all of the SAs and UAs are on the same subnet. This is because the UAs and SAs can find each other within the subnet using multicast packets, provided that there are no firewalls that are set to block multicast traffic.

Overcoming the Subnet Limitation

Novell recommends against routing multicast packets across subnet boundaries, and most network configurations conform with that recommendation. Therefore, when SAs and UAs are on different subnets, they need an alternative to multicasting for advertizing and locating services on the other subnets.

Network administrators use DAs to solve this problem by setting up organizational or geographical DAs and then configuring the SAs and UAs within the organization or geographical area to use them. Many administrators further subdivide the DA workload by defining multiple SLP scopes based on different kinds of network services, and then configuring the SAs and UAs to communicate with the DAs servicing the scope that pertains to them.

An eDirectory Example

When you configure eDirectory during an OES server installation, you have the option of specifying one or more SLP DAs for the server to communicate with. Each time eDirectory starts and every hour thereafter, the server's SA will send a unicast packet to the server's assigned DAs, advertising that its eDirectory services are available.

IMPORTANT: Prior to eDirectory 8.8.2, the eDirectory SA advertised service availability every 10 minutes by default. Starting with eDirectory 8.8.2, the refresh interval changed to one hour. This has caused some confusion for network administrators who couldn't figure out why it took so long for eDirectory to register as a service

For information on how to set the refresh interval to a smaller value, see [TID 7001449 \(http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7001449&sliceId=2&docTypeID=DT_TID_1_1&dialogID=104660609&statId=0%200%20209665064\)](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7001449&sliceId=2&docTypeID=DT_TID_1_1&dialogID=104660609&statId=0%200%20209665064) in the Novell Support Knowledgebase.

What Happens When a DA Goes Down?

As you can imagine, a directory agent in a large organization can accumulate many service listings after it has been running for a while. Unfortunately, because DAs are inherently cache-only repositories, if they go down for some reason, when they come back up their list of services is initially blank.

Novell SLP solved this problem on NetWare 5.x and later through eDirectory Modified Event notifications. These notifications keep all of the NetWare DA's that are servicing the same scope in sync with each other. After going down and coming back up, a NetWare DA can quickly recover its directory listings.

OpenSLP DA's, on the other hand, have historically been completely independent from each other. Because they are not eDirectory-aware, they have had no means of recovering the directory listings they had prior to going down.

This changed, beginning in OES 2 SP3.

OpenSLP DAs can now

- ♦ Retrieve and/or push service information to and/or from other DAs. For more information, see [“Synchronizing Data Between OpenSLP DAs and/or Novell SLP DAs” on page 181](#).
- ♦ Back up their service registrations so that when the DA service is started up it can read the backup file and pre-populate its cache. For more information, see [“Backing Up Registrations and Managing Persistence” on page 182](#).

These changes provide, in effect, the same type of DA to DA communication for OES that has traditionally been available only on NetWare.

12.5.2 Comparing Novell SLP and OpenSLP

Table 12-4 SLP Solutions

Platform	NetWare	OES 11 SP2
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 11.</p> <p>In OES 11 SP2, 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 11 SP2 server is the fourth or later server added to a tree and doesn't have an eDirectory replica automatically installed.</p>

Platform	NetWare	OES 11 SP2
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> <p>NOTE: Novell SLP DAs do not directly share information with each other as many administrators have assumed. But they do maintain well synchronized caches through eDirectory as described above.</p>	<p>OpenSLP directory agents (DAs) are able to share service registrations as described in “Synchronizing Data Between OpenSLP DAs and/or Novell SLP DAs” on page 181.</p> <p>OpenSLP is also capable of ensuring data persistence when DAs go down, as explained in “Backing Up Registrations and Managing Persistence” on page 182.</p>
Compatibility	Novell SLP user agents (UAs) or service agents (SAs) can access both Novell SLP DAs and OpenSLP DAs.	OpenSLP-based user agents or service agents can access both Novell SLP DAs and OpenSLP DAs.
Documentation	Setting Up SLP on NetWare (https://www.netiq.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/ba6406j.html) .	“Configuring OpenSLP for eDirectory” in the <i>NetIQ eDirectory 8.8 SP8 Administration Guide</i> .

12.5.3 Setting Up OpenSLP on OES 11 SP2 Networks

SLP services are always installed as part of both NetWare and SLES 11 SP3 (the underlying OES 11 SP2 platform). On NetWare and on OES, SLP services run automatically in multicast mode. Setting up directory agents and multiple scopes, etc. requires a manual configuration of SLP, either during the installation or by modifying the `slpd.conf` file afterward.

- ♦ [“When Is OpenSLP Required?”](#) on page 180
- ♦ [“Setting Up an OpenSLP DA Server”](#) on page 180
- ♦ [“Synchronizing Data Between OpenSLP DAs and/or Novell SLP DAs”](#) on page 181
- ♦ [“Backing Up Registrations and Managing Persistence”](#) on page 182
- ♦ [“Configuring OES 11 SP2 Servers to Access the OpenSLP DA”](#) on page 182
- ♦ [“Configuring NetWare Servers to Use the OpenSLP Service”](#) on page 183

When Is OpenSLP Required?

The OES install automatically starts OpenSLP on your OES 11 SP2 server in case any of the following applies:

- You install more than three servers into a new tree
- You create a new eDirectory partition on an OES 11 SP2 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 in more than multicast mode 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 11 SP2 server is recommended.

Setting Up an OpenSLP DA Server

The default SLP configuration in the YaST-based install doesn't include having a Directory Agent. This approach is far less robust, requires multicasting, and involves disabling the firewall.

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 11 SP2 server in your tree as an OpenSLP DA. The simplest way to do this is during server installation by selecting the *Configure as Directory Agent* option in the YaST-based installation.

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.

To set up an OpenSLP DA on an existing OES 11 SP2 server, do the following.

- 1 On the OES 11 SP2 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 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 11 SP2 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:
 - ♦ [Synchronizing Data Between OpenSLP DAs and/or Novell SLP DAs \(page 181\)](#)
 - ♦ [Backing Up Registrations and Managing Persistence \(page 182\)](#)
 - ♦ [Configuring OES 11 SP2 Servers to Access the OpenSLP DA \(page 182\)](#)
 - ♦ [Configuring NetWare Servers to Use the OpenSLP Service \(page 183\)](#)

Synchronizing Data Between OpenSLP DAs and/or Novell SLP DAs

If you didn't set up DA synchronization during server installation, you can set it up later by using the following parameters in the `slp.conf` file:

```
net.slp.dasyncreg = true/false
```

```
slp.DAaddresses = IP_address_1,IP_address_2
```

If the `net.slp.dasyncreg` parameter value is set to `true`, then synchronization is achieved by the DA pushing or pulling SLP registrations from the DAs listed for the `slp.DAaddresses` parameter, as follows:

1. When the DA starts up, it pulls the registration information from all of the server DAs listed in the `slp.DAaddresses` parameter, including any Novell SLP DAs listed.
2. When the DA receives a service registration, it forwards the information to the OpenSLP DAs that are listed.

IMPORTANT: Service registrations cannot be pushed to Novell SLP DA's.

Backing Up Registrations and Managing Persistence

If you didn't set up registration back-up during server installation, you can set it up later by using the following parameters in the `slp.conf` file:

```
net.slp.isDABackup = true/false

net.slp.DABackupInterval = time_in_seconds
```

If the `net.slp.isDABackup` parameter is set to `true`, service registrations are backed up in the `/etc/slp.reg.d/slpd/DABackup` file at the interval specified for the `net.slp.DABackupInterval` parameter. By default, the interval is 900 seconds (15 minutes).

Configuring OES 11 SP2 Servers to Access the OpenSLP DA

If you created the OpenSLP DA on an OES 11 SP2 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 11 SP2 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 11 SP2 Installation” on page 182](#)
- ♦ [“Configuring for DA Access Before or After Installing OES 11 SP2” on page 182](#)

Configuring for DA Access During the OES 11 SP2 Installation

As you install OES 11 SP2 by using the instructions in the [“NetIQ eDirectory Services”](#) section of the [OES 11 SP2: Installation Guide](#), do the following:

- 1 When you reach the [“eDirectory Configuration - NTP and SLP”](#) section of the installation, select *Configure SLP to Use an Existing Directory Agent*.
The first 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 180](#). 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 180](#). You can also list additional DA addresses, separated by commas.
- 4 Return to the [“NetIQ Modular Authentication Services”](#) instructions in the [OES 11 SP2: Installation Guide](#).

Configuring for DA Access Before or After Installing OES 11 SP2

Whether you configure DA access before installing OES 11 SP2 on a SLES 11 SP3 server or after a simultaneous install of SLES 11 SP3 and OES 11 SP2, 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 180](#).

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 180](#).

```
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 183](#)
- [“Configuring for DA Access After Installing the NetWare Server” on page 184](#)

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 11 SP2 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 11 SP2 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 11 SP2 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 11 SP2 until you are ready to switch to OpenSLP.

This section discusses the following:

- ♦ [“NetWare Is Configured with Novell SLP By Default” on page 184](#)
- ♦ [“Configuring OES 11 SP2 Servers to Access the Novell SLP DA” on page 184](#)
- ♦ [“Checking the Status of Novell SLP Services” on page 187](#)

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.

Configuring OES 11 SP2 Servers to Access the Novell SLP DA

For each of the OES 11 SP2 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 11 SP2 Installation” on page 184](#)
- ♦ [“Configuring for DA Access Before or After Installing the OES 11 SP2 Server” on page 185](#)

Configuring for DA Access During the OES 11 SP2 Installation

As you install OES 11 SP2, in the [“NetIQ eDirectory Services”](#) section of the [OES 11 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, *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.

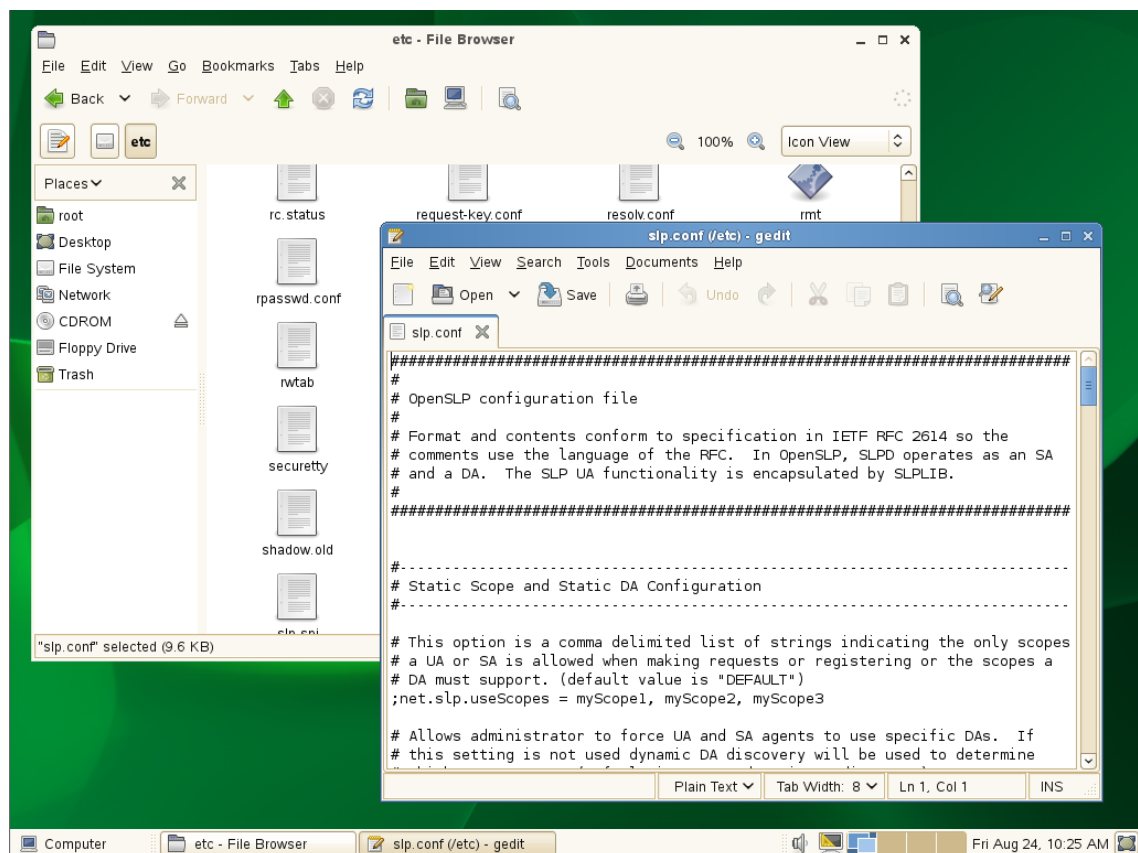
You can also list additional DA addresses, separated by commas.

- 4 Return to the "[NetIQ eDirectory Services](#)" instructions in the [OES 11 SP2: Installation Guide](#).

Configuring for DA Access Before or After Installing the OES 11 SP2 Server

Whether you configure DA access before installing OES 11 SP2 on a SLES 11 SP3 server or after a simultaneous install of SLES 11 SP3 and OES 11, 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.

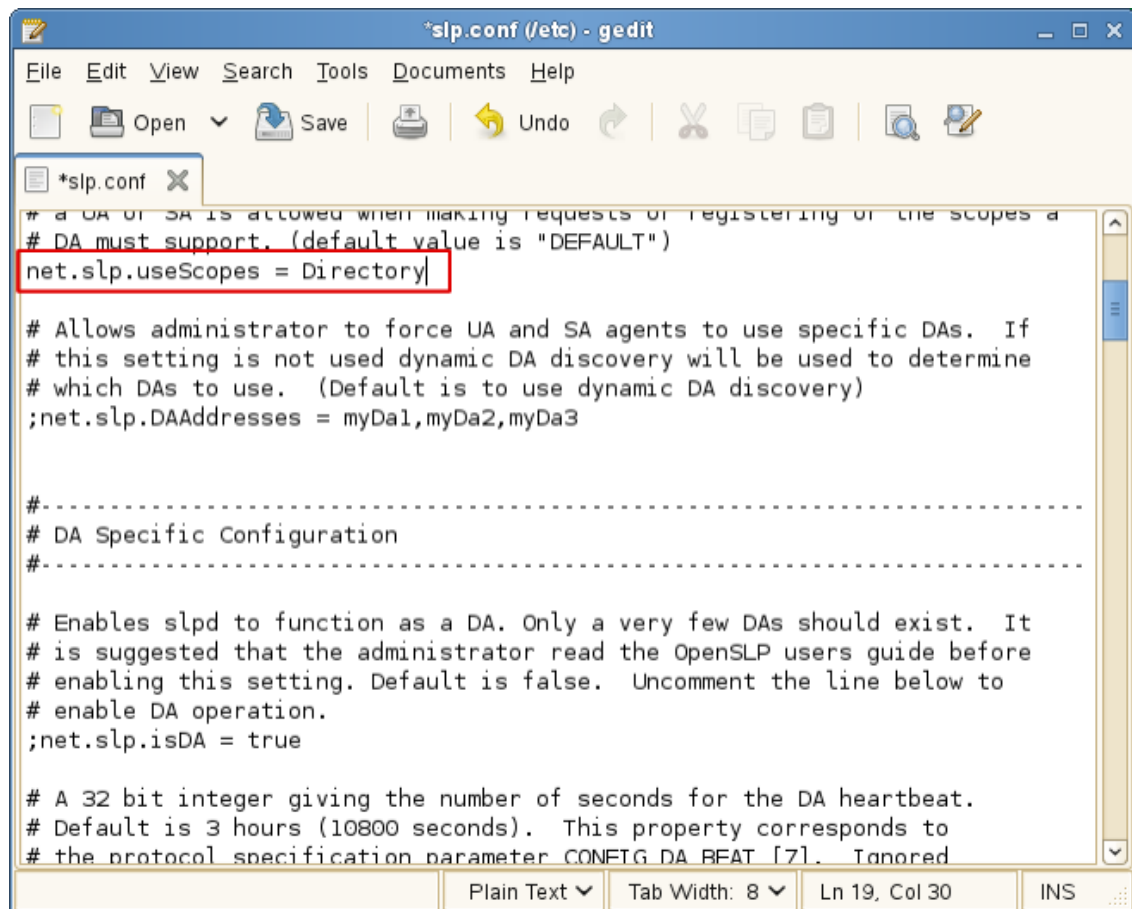
- 3 Modify the line by removing the semicolon and typing the name or names of the scopes you want this server to have access to.

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
```

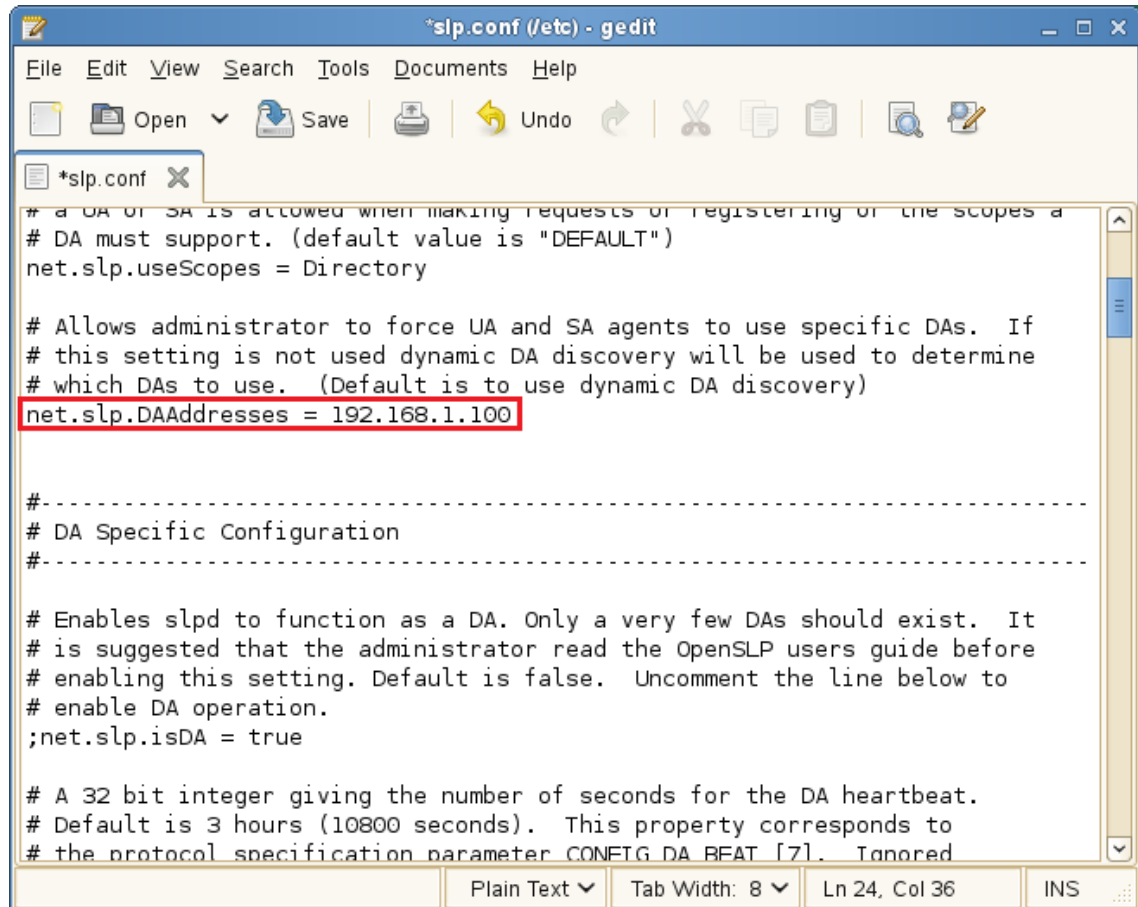


- 4 Find the following line:

```
;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 11 SP2, enter the following 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.

12.5.5 TIDs and Other Help

The SLP configuration file (`etc/slp.conf`) is self-documented regarding each of the configuration parameters. Novell support has also provided the following TIDS:

- ♦ [OpenSLP vs. Novell SLP](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004574&sliceId=1&docTypeID=DT_TID_1_1&dialogID=246569372&stateId=0%200%20246565813) (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004574&sliceId=1&docTypeID=DT_TID_1_1&dialogID=246569372&stateId=0%200%20246565813) answers questions about the differences between the two SLP solutions.
- ♦ [eDir not registering bindery or NDAP services with OpenSLP](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7001449&sliceId=1&docTypeID=DT_TID_1_1&dialogID=246569372&stateId=0%200%20246565813) (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7001449&sliceId=1&docTypeID=DT_TID_1_1&dialogID=246569372&stateId=0%200%20246565813) answers questions about how the SLP solutions register ndap and bindery services.
- ♦ [NetWare SLP fails to populate service registrations to an openSLP DA on OES](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7009783&sliceId=1&docTypeID=DT_TID_1_1&dialogID=281740290&stateId=0%200%20281736877) (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7009783&sliceId=1&docTypeID=DT_TID_1_1&dialogID=281740290&stateId=0%200%20281736877) explains how to solve the communication problem.
- ♦ [OpenSLP Documentation on the Web](http://www.openslp.org/documentation.html) (<http://www.openslp.org/documentation.html>) provides complete documentation of the OpenSLP services that OES leverages.

13 Storage and File Systems

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

Use this section to understand the file storage solutions available in Open Enterprise Server 11 SP2 and then to plan a storage solution that meets your file system management needs.

The “[storage and file systems \(http://www.novell.com/documentation/oes11/index.html#cat_stor-file-systems-databases\)](http://www.novell.com/documentation/oes11/index.html#cat_stor-file-systems-databases)” links in the OES 11 SP2 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 11 SP2 Storage,” on page 189](#)
- ♦ [Section 13.2, “Planning OES File Storage,” on page 194](#)
- ♦ [Section 13.3, “Coexistence and Migration of Storage Services,” on page 201](#)
- ♦ [Section 13.4, “Configuring and Maintaining Storage,” on page 203](#)

Other storage-related topics in this guide are:

- ♦ [Chapter 16, “Access Control and Authentication,” on page 231](#)
- ♦ [Section 16.2, “Authentication Services,” on page 242](#)
- ♦ [Appendix 17, “Backup Services,” on page 247](#)
- ♦ [Chapter 18, “File Services,” on page 249](#)

13.1 Overview of OES 11 SP2 Storage

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

- ♦ [Section 13.1.1, “Databases,” on page 189](#)
- ♦ [Section 13.1.2, “iSCSI,” on page 190](#)
- ♦ [Section 13.1.3, “File System Support in OES,” on page 190](#)
- ♦ [Section 13.1.4, “Storage Basics by Platform,” on page 192](#)
- ♦ [Section 13.1.5, “Storage Options,” on page 192](#)
- ♦ [Section 13.1.6, “NetWare Core Protocol Support \(Novell Client Support\) on Linux,” on page 194](#)

13.1.1 Databases

See the [MySQL documentation \(http://dev.mysql.com/doc\)](http://dev.mysql.com/doc) on the Web.

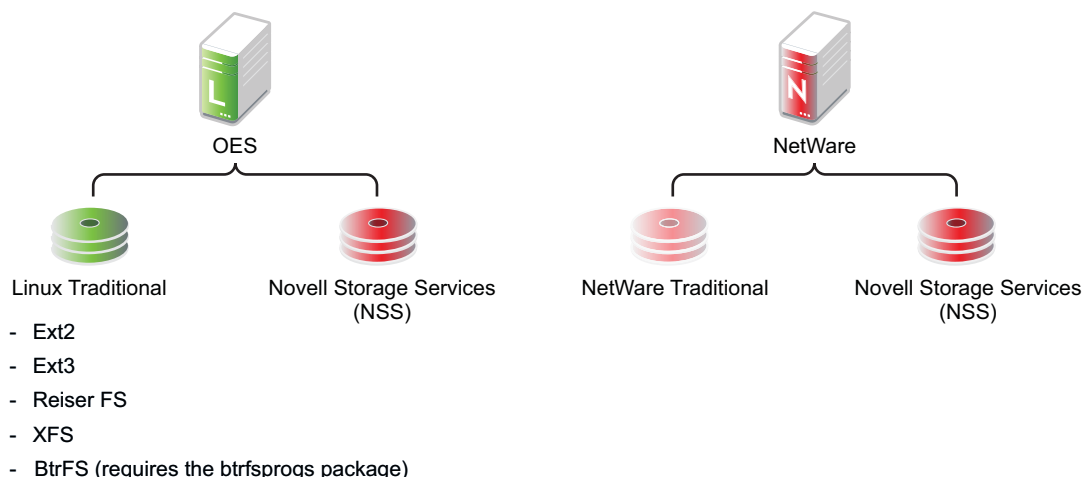
13.1.2 iSCSI

See the topics in “iSCSI for Linux (http://www.suse.com/documentation/sles11/stor_admin/data/cha_inst_system_iscsi.html)” in the SLES online documentation.

13.1.3 File System Support in OES

As shown in [Figure 13-1](#), both OES and NetWare support Novell Storage Services as well as their traditional file systems.

Figure 13-1 File System Choices on OES and NetWare Servers



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

Table 13-1 File Systems Available on OES and NetWare Servers

File System Type	OES	NetWare	Summary	Link for More Information
Linux POSIX File Systems	Y	N	<p>SLES 11 SP3 includes a number of different file systems, the most common of which are Ext3, Reiser, XFS, and Btrfs (requires the btrfsprogs package).</p> <p>OES 11 SP2 services are supported on Ext3, Reiser, XFS, and Btrfs.</p>	<p>For an overview of the supported file systems in OES 11, see “File Systems Overview” in the <i>OES 11 SP2: File Systems Management Guide</i>.</p> <p>For an overview of Linux POSIX file systems, see Overview of File Systems in Linux in the <i>SLES 11 SP3: Storage Administration Guide</i>.</p>
NetWare Traditional File System	N	Y	<p>This is a legacy file system on NetWare servers that supports the Novell file service trustee access control model.</p>	<p>For more information, see the <i>NW6.5 SP8: Traditional File System Administration Guide</i>.</p>

File System Type	OES	NetWare	Summary	Link for More Information
Novell Storage Services (NSS)	Y	Y	<p>NSS lets you manage your shared file storage for any size organization.</p> <p>On Netware, NSS features include visibility, a trustee access control model, multiple simultaneous name space support, native Unicode, user and directory quotas, rich file attributes, multiple data stream support, event file lists, and a file salvage subsystem.</p> <p>Most of these features are also supported on NSS on Linux. For a feature comparison, see “Comparison of NSS on NetWare and NSS on Linux” in the <i>OES 11 SP2: NSS File System Administration Guide for Linux</i>.</p>	For an overview of NSS, see “ Overview of NSS ” in the <i>OES 11 SP2: NSS File System Administration Guide for Linux</i> .

Novell Storage Services (NSS)

The following sections summarize key points regarding NSS:

- ♦ “[Understanding NSS Nomenclature](#)” on page 191
- ♦ “[Comparing NSS with Other File Systems](#)” on page 191
- ♦ “[NSS and Storage Devices](#)” on page 191

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 11 SP2: NSS File System Administration Guide for Linux*.

Comparing NSS with Other File Systems

Because OES 11 supports a variety of file systems, you might want to compare their features and benefits as outlined in the following sections of the *OES 11 SP2: NSS File System Administration Guide for Linux*:

- ♦ **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 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 11 SP2: NSS File System Administration Guide for Linux*.

13.1.4 Storage Basics by Platform

The following sections summarize storage basics for Linux and NetWare.

- ♦ [“Linux and File Systems” on page 192](#)
- ♦ [“NetWare Directories” on page 192](#)
- ♦ [“NetWare Storage Devices” on page 192](#)

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 11 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 File System”](#) in the *OES 11 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 192](#)
- ♦ [“Direct-Attached Storage Options \(NSS and Traditional\)” on page 193](#)
- ♦ [“Advanced Storage Options” on page 193](#)

Dynamic Storage Technology

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

NCP client users and Novell CIFS users automatically see a merged view of the files and subdirectories on the shadow volume when they access a share on the primary volume. All the actions they take--renaming, deleting, moving, etc.--are synchronized by Dynamic Storage Technology across the two volumes. If you use supported native Linux file access protocols, such as Novell Samba, SSH, or Novell FTP (PureFTP-d), to access the DST volume, you can enable ShadowFS to provide a merged view location for LUM-enabled users of those protocols. Novell CIFS and Novell Samba cannot be used on the same server.

Backup tools can access the volumes directly and separately, instead of via the merged view shown to NCP and CIFS users. You can apply one backup policy to the primary volume 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.

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 11 SP2: Dynamic Storage Technology Administration Guide](#).

Direct-Attached Storage Options (NSS and Traditional)

As shown in [Figure 13-1 on page 190](#), 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 11 SP2: Storage and File Services Overview](#).

Advanced Storage Options

NSS volumes support the following advanced storage solutions, as documented in the [OES 11 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.

- ◆ [iSCSI SAN](#)

You can create a SAN using Linux iSCSI.

- ◆ [Fault-Tolerant and High-Availability Architectures](#)

Use one or more of the following technologies:

- ◆ [Multiple Path I/O](#): The Linux Device Mapper Multipath I/O tool helps prevent failure in the connection between the CPU and the storage device by automatically identifying multiple paths between each Linux server and its storage devices.

- ◆ [Software RAIDs](#): NSS supports software RAIDs to improve storage availability and performance by enhancing data fault tolerance and I/O performance.

For more information, see “[Managing NSS Software RAID Devices](#)” in the [OES 11 SP2: NSS File System Administration Guide for Linux](#).

- ◆ [Server Clusters](#): With Novell Cluster Services, you can configure up to 32 servers into a high-availability cluster where resources and services are dynamically allocated to any server in the cluster and automatically switched to another server if the hosting server fails.

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

For more information, see the [OES 11 SP2: Novell Cluster Services for Linux Administration Guide](#). To convert a NetWare cluster to an OES cluster, see the [OES 11 SP2: Novell Cluster Services NetWare to Linux Conversion 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 lets you attach to Linux POSIX volumes that are defined as NCP volumes using Novell Client software. For more information, see [Section 18.6, “NCP Implementation and Maintenance,” on page 276](#).

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 194](#)
- ♦ [Section 13.2.2, “File Service Support Considerations,” on page 194](#)
- ♦ [Section 13.2.3, “General Requirements for Data Storage,” on page 195](#)
- ♦ [Section 13.2.4, “OES 11 SP2 Storage Planning Considerations,” on page 195](#)
- ♦ [Section 13.2.5, “NSS Planning Considerations,” on page 201](#)

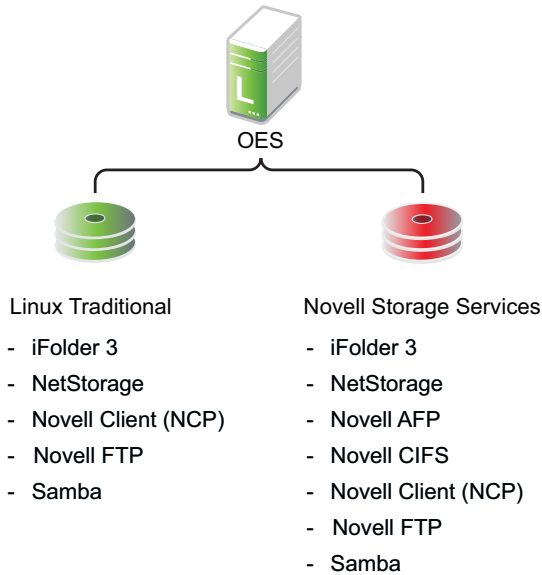
13.2.1 Directory Structures

To plan the directory structures you need on OES 11 SP2, see “[Understanding Directory Structures in Linux POSIX File Systems](#)” in the [OES 11 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 11 SP2: Storage and File Services Overview](#).

13.2.4 OES 11 SP2 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 11 SP2 servers, and includes the following topics:

- ♦ “[The Workgroup Environment](#)” on page 195
- ♦ “[File System Support](#)” on page 196
- ♦ “[File Access Protocol Support](#)” on page 198
- ♦ “[OES 11 SP2 Workloads](#)” on page 199

The Workgroup Environment

When selecting a file system, it is important to understand the environment in which it operates. For OES 11 SP2, 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 11 offers support for five file systems: Novell Storage Services (NSS), Ext 2, Ext3, Reiser, and XFS. Following is an explanation of each file system and the pros and cons of using them in the workloads supported by OES 11.

- ♦ [“Novell Storage Services \(NSS\)” on page 196](#)
- ♦ [“Btrfs” on page 197](#)
- ♦ [“Ext2” on page 197](#)
- ♦ [“Ext3” on page 198](#)
- ♦ [“Reiser” on page 198](#)
- ♦ [“XFS” on page 198](#)

Novell Storage Services (NSS)

- ♦ Supported only through NSS management tools; not supported through native Linux Management tools.
- ♦ Best for shared LAN file serving; excellent scalability in the number of files
- ♦ Journaled
- ♦ Novell Trustee Model and NSS directory and file attributes (such as Rename Inhibit) provide access control that is much richer than POSIX and Linux access control lists (ACLs)

The Novell Storage Services file system is used in NetWare 5.0 and above, is included in the Novell Open Enterprise Server.

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.

Btrfs

- ♦ Writable snapshots that allow you to easily roll back your system if needed after applying updates, or to back up files.
- ♦ Multiple device support that allows you to grow or shrink the file system.
- ♦ Compression to efficiently use storage space.
- ♦ Different RAID levels for metadata and user data.
- ♦ Different checksums for metadata and user data to improve error detection.
- ♦ Integration with Linux Logical Volume Manager (LVM) storage objects.
- ♦ Integration with the YaST Partitioner on SUSE Linux.

BtrFS creates a default subvolume in its assigned pool of space. It allows you to create additional subvolumes that act as individual file systems within the same pool of space. The number of subvolumes is limited only by the space allocated to the pool.

If BtrFS is used for the root (/) file system, you can cover any subdirectory as a subvolume as you might normally do. You should also consider covering the following subdirectories in separate subvolumes because they contain files that you might prefer not to snapshot for the reasons given:

Path	Reason to Cover as a Subvolume
/opt	Contains third-party add-on application software packages.
/srv	Contains <code>http</code> and <code>ftp</code> files.
/tmp	Contains temporary files.
/var/log	Contains log files.
/var/opt	Contains run-time variable data for <code>/opt</code> .
/var/run	Contains run-time variable data.
/var/spool	Contains data that is awaiting processing by a program, user, or administrator, such as news, mail, and printer queues.
/var/tmp	Contains temporary files or directories that are preserved between system reboots.

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 a paravirtualized server is running as a Xen VM guest, you should format the `/boot` partition with Ext2 as explained in [Section 9.4, “Xen VMs Need Ext2 for the System /Boot Volume,” on page 140](#).

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 the default file system for SUSE Linux 11 distributions. 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.

Reiser

- ♦ Best performance and scalability when the number of files is great and/or files are small
- ♦ Journaled
- ♦ POSIX extended access control

Reiser 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.

XFS

- ♦ Best for extremely large file systems, large files, and lots of files
- ♦ Journaled (an asymmetric parallel cluster file system version is also available)
- ♦ POSIX extended access controls

The XFS file system is open source and is included in major Linux distributions. It originated from SGI (Irix) and was designed specifically for large files and large volume scalability.

Video and multimedia files are best handled by this file system. Scaling to petabyte volumes, it also handles very large amounts of data. It is one of the few file systems on Linux that supports HSM data migration.

File Access Protocol Support

OES 11 SP2 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 Novell 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. It supports Novell Trustee model access for NSS volumes and Dynamic Storage Technology shadow volumes

Novell Samba is a Novell's customized version of an open source software version of CIFS developed after 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. OES provides FTP functionality similar to that available on NetWare. For more information, see [Section 18.5, “Novell FTP \(Pure-FTPd\) and OES 11 SP2,” on page 268](#).
- ♦ **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 that was developed by Novell for supporting DOS, Windows, OS/2, Macintosh, UNIX (UnixWare), and Linux for shared file services.

The NCP Server included in OES features emulation of the Novell Trustee Model and inheritance plus visibility when it runs on traditional POSIX file systems such as Ext3, Reiser, and XFS. When it runs on NSS, these capabilities are synchronized with the NSS File system and its extended directory and file attributes, such as Rename Inhibit.

OES 11 SP2 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	Btrfs	Ext3 File System	Reiser File System	XFS File System
AFP (Novell AFP)	Supported	Not Supported	Not Supported	Not Supported	Not Supported
CIFS (Novell CIFS)	Supported	Not Supported	Not Supported	Not Supported	Not Supported
Cluster Services	Recommended	Supported	Recommended	Recommended	Recommended
Collaboration (GroupWise)	Supported	Supported	Recommended	Supported	Supported
Dynamic Storage Technology	Supported	Not Supported	Not Supported	Not Supported	Not Supported
File serving – Application server	Supported	Supported	Supported	Recommended	Recommended
iFolder	Recommended	Supported	Supported	Recommended	Recommended
NCP (Novell Client)	Recommended	Supported	Supported	Supported	Supported
NetStorage	Recommended	Supported	Recommended	Recommended	Recommended
Printing (iPrint)	Recommended	Supported	Recommended	Recommended	Recommended
PureFTP	Recommended	Supported	Recommended	Recommended	Recommended

The following sections provide a brief summary of considerations for the workload types listed in [Table 13-2](#).

- ♦ [“Collaboration \(GroupWise\)” on page 200](#)
- ♦ [“Dynamic Storage Technology” on page 200](#)
- ♦ [“File Serving” on page 200](#)
- ♦ [“iFolder” on page 200](#)
- ♦ [“Novell Cluster Services” on page 200](#)
- ♦ [“Printing \(iPrint\)” on page 201](#)

Collaboration (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. GroupWise recommends the Ext3 file system. NSS and Reiser are also supported.

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.

File Serving

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 AFP, 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.

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.

Novell Cluster Services

Novell Cluster Services does not depend on a particular file system. For shared storage, the file systems software must be available 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.

Printing (iPrint)

iPrint is file system agnostic. There is no noticeable difference in performance or reliability on any of the file systems.

13.2.5 NSS Planning Considerations

To plan for NSS volumes—including prerequisites and security considerations—see “[Planning NSS Storage Solutions](#)” in the *OES 11 SP2: NSS File System Administration Guide for Linux*.

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, “Databases,” on page 201](#)
- ♦ [Section 13.3.2, “NetWare 6.5 SP8,” on page 202](#)
- ♦ [Section 13.3.3, “OES 11 SP2 File System Options,” on page 202](#)

13.3.1 Databases

The SUSE Linux Enterprise Server 11 (SLES 11) SP2 platform on which OES 11 SP2 services are installed, includes two open source databases:

- ♦ [“MySQL” on page 201](#)
- ♦ [“PostgreSQL” on page 201](#)

NOTE: Full Novell support of these databases requires a product-specific Novell support contract. Documentation and support are available through open source communities as outlined below.

MySQL

The SLES 11 platform includes the open source MySQL database server and client. 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. See the [documentation on the Web \(http://dev.mysql.com/doc/\)](http://dev.mysql.com/doc/).

For overview of MySQL and for information about configuring it with Novell Cluster Services, see “[Configuring MySQL with Novell Cluster Services](#)” in the *OES 11 SP2: Web Services and Applications Guide*.

PostgreSQL

The more powerful PostgreSQL database server also comes with SLES 11. See the [PostgreSQL documentation on the Web \(http://www.postgresql.org/docs/8.3/interactive/index.html\)](http://www.postgresql.org/docs/8.3/interactive/index.html).

Novell Archive and Version Services uses PostgreSQL for its Archive database.

13.3.2 NetWare 6.5 SP8

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

- ♦ [“NetWare Traditional File System” on page 202](#)
- ♦ [“NSS Volumes” on page 202](#)

NetWare Traditional File System

Although NetWare 6.5 SP8 supports Traditional volumes, you must upgrade them to NSS before upgrading from NetWare to OES.

NSS Volumes

To support data migration, NSS volumes are cross-compatible between NetWare and OES servers. During a cluster conversion from NetWare 6.5 SP8 to OES, clustered NSS pools 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 OES. For information, see the [OES 11 SP2: Novell Cluster Services NetWare to Linux Conversion Guide](#).

For additional information about coexistence and migration of NSS volumes, as well as access control issues for NSS on OES, see “[Migrating NSS Devices to OES 11 SP2](#)” in the [OES 11 SP2: NSS File System Administration Guide for Linux](#).

13.3.3 OES 11 SP2 File System Options

OES 11 SP2 provides support for Novell Storage Services (NSS) as well as Linux POSIX file systems.

- ♦ [“NSS Volumes” on page 202](#)
- ♦ [“Linux POSIX File Systems” on page 203](#)

NSS Volumes

To support migration from NetWare to OES, NSS volumes are cross-compatible between NetWare and Linux.

On OES, you can use NSS volumes only as data volumes.

You configure NSS pools and volumes in iManager or NSSMU after the server installation completes successfully. You can also use the Novell Linux Volume Manager (NLVM) command line interface.

Starting with NetWare 6.5 SP4 (and OES 1), a new metadata structure provided enhanced support for hard links. After you upgrade your operating system to OES, 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 11 SP2: NSS File System Administration Guide for Linux](#).

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

Linux POSIX File Systems

IMPORTANT: Users can access data storage on OES 11 SP2 servers through a number of methods. For more information, see [“Overview of File Services” on page 249](#).

OES 11 SP2 includes tools and services that help bridge the gap between traditional Novell file services and Linux POSIX file services.

- ♦ [“Management Tools” on page 203](#)
- ♦ [“NCP Server” on page 203](#)
- ♦ [“Novell Cluster Services” on page 203](#)

Management Tools

Using NSSMU and the Novell Linux Volume Manager (NLVM) command line interface, you can create native Linux POSIX volumes and standalone or clustered Linux Logical Volume Manager 2 (LVM2) volume groups and logical volumes.

NCP Server

OES 11 SP2 includes NCP Server for Linux. After you create native Linux POSIX volumes, you can use NCP Server to create NCP shares on them. You can then manage the shares as NCP volumes.

This lets Novell Client users map drives to Linux POSIX file system data, with access controls being enforced by NCP. For more information on using NCP Server for Linux in OES, see the [OES 11 SP2: NCP Server for Linux Administration Guide](#).

Novell Cluster Services

For information about clustering LVM2 volume groups with Novell Cluster Services, see [“Configuring and Managing Cluster Resources for Shared LVM Volume Groups”](#) in the [OES 11 SP2: Novell Cluster Services for Linux Administration Guide](#).

13.4 Configuring and Maintaining Storage

- ♦ [Section 13.4.1, “Managing Directories and Files,” on page 203](#)
- ♦ [Section 13.4.2, “Managing NSS,” on page 203](#)
- ♦ [Section 13.4.3, “Optimizing Storage Performance,” on page 205](#)

13.4.1 Managing Directories and Files

To learn about managing directories and files on an OES 11 SP2 server, see [“Understanding Directory Structures in Linux POSIX File Systems”](#) in the [OES 11 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.	OES 11 SP2: Novell Archive and Version Services Administration Guide
Compression	Conserve disk space and increase the amount of data a volume can store.	“Managing Compression on NSS Volumes” in the OES 11 SP2: NSS File System Administration Guide for Linux
Console Commands	<p>Manage NSS volumes in an OES terminal console via the NSS Console (nsscon) utility.</p> <p>You can also issue Novell Linux Volume Manager (NLVM) command line commands at the console prompt and in scripts.</p>	“NSS Commands” and “NSS Utilities” in the OES 11 SP2: NSS File System Administration Guide for Linux
Distributed File Services (DFS)	Use DFS junctions to transparently redirect data requests, split volumes while maintaining transparent access, and quickly move volume data to another volume.	OES 11 SP2: Novell Distributed File Services Administration Guide for Linux
Encryption	Create and manage encrypted NSS volumes that make data inaccessible to software that circumvents normal access control.	“Managing Encrypted NSS Volumes” in the OES 11 SP2: NSS File System Administration Guide for Linux
Hard Links	Create multiple names for a single file in the same or multiple directories in an NSS volume.	“Managing Hard Links” in the OES 11 SP2: NSS File System Administration Guide for Linux
Monitoring	Monitor NSS file systems.	“Monitoring the Status of the NSS File System and Services” in the OES 11 SP2: NSS File System Administration Guide for Linux
Multipath Support on Linux	Use Linux Device Mapper Multipath I/O tools to manage the dynamic, multiple, redundant connection paths between a Linux server and its external storage devices.	“Managing Multipath I/O to Devices” in the OES 11 SP2: NSS File System Administration Guide for Linux
Novell Linux Volume Manager	NLVM provides a command line interface that lets you manage the NSS file system at a terminal console or by using a script. It also provides APIs that are used by the NSSMU and iManager storage management tools.	OES 11 SP2: NLVM Reference
Partitions	Manage partitions on NSS volumes.	“Managing Partitions” in the OES 11 SP2: NSS File System Administration Guide for Linux
Pools	Create and manage NSS pools.	“Managing NSS Pools” in the OES 11 SP2: NSS File System Administration Guide for Linux

Category/Feature	Description	Link
Pool Move	You can move the contents of a pool from one location to another on the same system. The destination location can be made up of one or multiple devices. If the new location is larger than the original location, the pool is automatically expanded after the move is complete.	“Mount” in the OES 11 SP2: NLVM Reference “Moving a Pool” in the OES 11 SP2: NSS File System Administration Guide for Linux
Quotas	Set space restrictions for users and directories to control storage usage.	“Managing Space Quotas for Volumes, Directories, and Users” in the OES 11 SP2: NSS File System Administration Guide for Linux
Salvage subsystem	Use the salvage subsystem to make deleted files and directories available for undelete or purge actions.	“Salvaging and Purging Deleted Volumes, Directories, and Files” in the OES 11 SP2: NSS File System Administration Guide for Linux
Tools	Learn about the various tools available to manage NSS volumes, the tool capabilities, and how to use them.	“Management Tools for NSS” in the OES 11 SP2: NSS File System Administration Guide for Linux
Troubleshooting	Troubleshoot NSS on OES and NetWare 6.5 SP8.	“Troubleshooting the NSS File System” in the OES 11 SP2: NSS File System Administration Guide for Linux
File System Trustees and Attributes	Control user access to data by setting trustees, trustee rights, and inherited rights filters for files. Control file behavior by setting file and folder attributes.	“Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes” in the OES 11 SP2: NSS File System Administration Guide for Linux
Volumes	Create and manage NSS volumes in NSS pools.	“Managing NSS Volumes” in the OES 11 SP2: NSS File System Administration Guide for Linux

13.4.3 Optimizing Storage Performance

See [“Tuning NSS Performance”](#) in the *OES 11 SP2: NSS File System Administration Guide for Linux*.

14 eDirectory, LDAP, and Domain Services for Windows

This section discusses the following topics:

- ♦ [Section 14.1, “Overview of Directory Services,” on page 207](#)
- ♦ [Section 14.2, “eDirectory,” on page 208](#)
- ♦ [Section 14.3, “LDAP \(eDirectory\),” on page 209](#)
- ♦ [Section 14.4, “Domain Services for Windows,” on page 210](#)

14.1 Overview of Directory Services

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

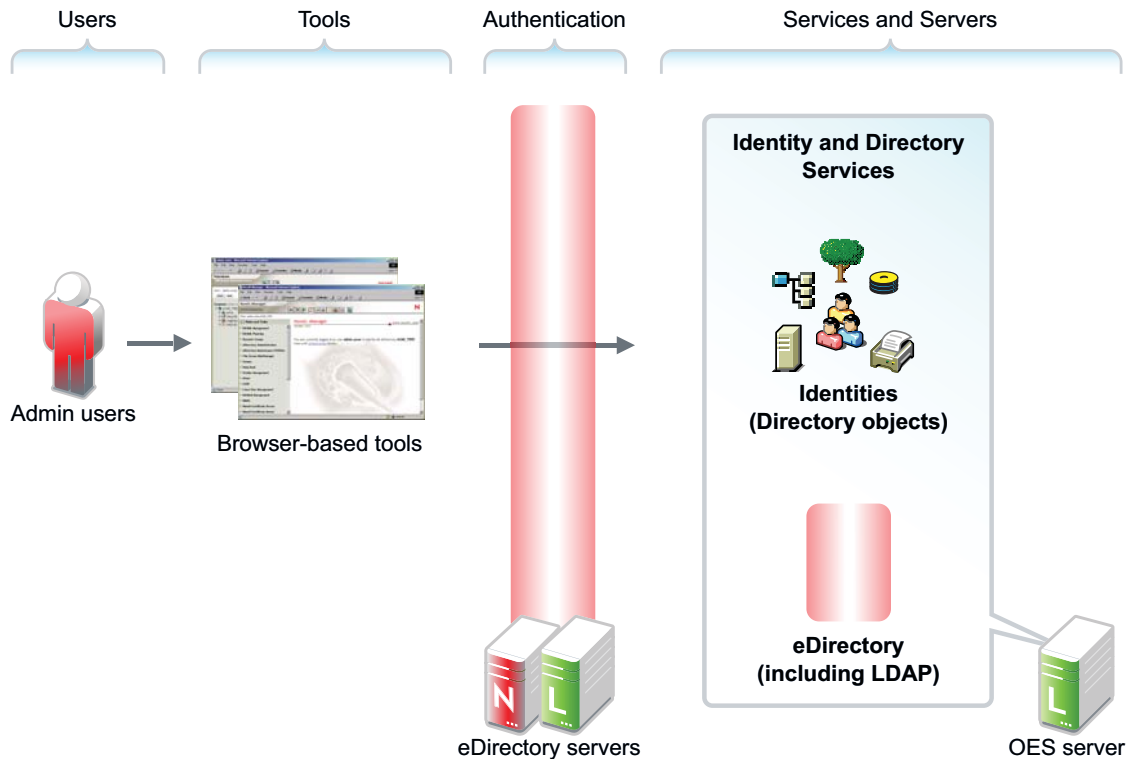
In the simplest terms, NetIQ eDirectory is a tree structure containing a list of objects (or identities) that represent network resources, such as the following:

- ♦ 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 207](#).

Figure 14-1 eDirectory Overview



14.2 eDirectory

NetIQ 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 208](#)
- ♦ [Section 14.2.2, “Planning Your eDirectory Tree,” on page 209](#)
- ♦ [Section 14.2.3, “eDirectory Coexistence and Migration,” on page 209](#)

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 208](#)
- ♦ [“iManager” on page 209](#)

OES Installation Programs

OES requires that eDirectory be installed by using the YaST-based OES install.

IMPORTANT: Other utilities, such as `ndsconfig` and `ndsmanage`, are not supported for installing or removing eDirectory on OES servers, unless explicitly called for in OES-specific instructions.

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 [NetIQ® iManager 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.

If you are new to eDirectory, the [OES 11 SP2: Getting Started with OES 11 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 NetIQ eDirectory Network” in the [NetIQ eDirectory 8.8 SP8 Installation Guide](#).

To learn what's new in eDirectory 8.8, see the [NetIQ eDirectory 8.8 SP8 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, NetIQ 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 11 SP2 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 SP8” in the [NetIQ eDirectory 8.8 SP8 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 210](#)
- ♦ [Section 14.3.2, “Planning eDirectory LDAP Services,” on page 210](#)

- ♦ [Section 14.3.3, “Migration of eDirectory LDAP Services,” on page 210](#)
- ♦ [Section 14.3.4, “eDirectory LDAP Implementation Suggestions,” on page 210](#)

14.3.1 Overview of eDirectory LDAP Services

Lightweight Directory Access Protocol (LDAP) Services for NetIQ eDirectory is a server application that lets LDAP clients access information stored in eDirectory.

Most OES 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 NetIQ eDirectory”](#) in the *NetIQ eDirectory 8.8 SP8 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 [“NetIQ eDirectory Management Utilities”](#) in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

14.3.4 eDirectory LDAP Implementation Suggestions

OES service LDAP support requires no additional setup or configuration beyond the OES install.

For help with setting up and using LDAP for eDirectory for other purposes, you can refer to [“Configuring LDAP Services for NetIQ eDirectory”](#) in the *NetIQ eDirectory 8.8 SP8 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 NetIQ 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 211](#)
- ♦ [Section 14.4.2, “Planning Your DSfW Implementation,” on page 214](#)
- ♦ [Section 14.4.3, “Implementing DSfW on Your Network,” on page 214](#)

14.4.1 Graphical Overview of DSfW

- ♦ “File Access” on page 211
- ♦ “User Management” on page 212
- ♦ “Storage Management” on page 213

File Access

Figure 14-2 DSfW File Access Overview

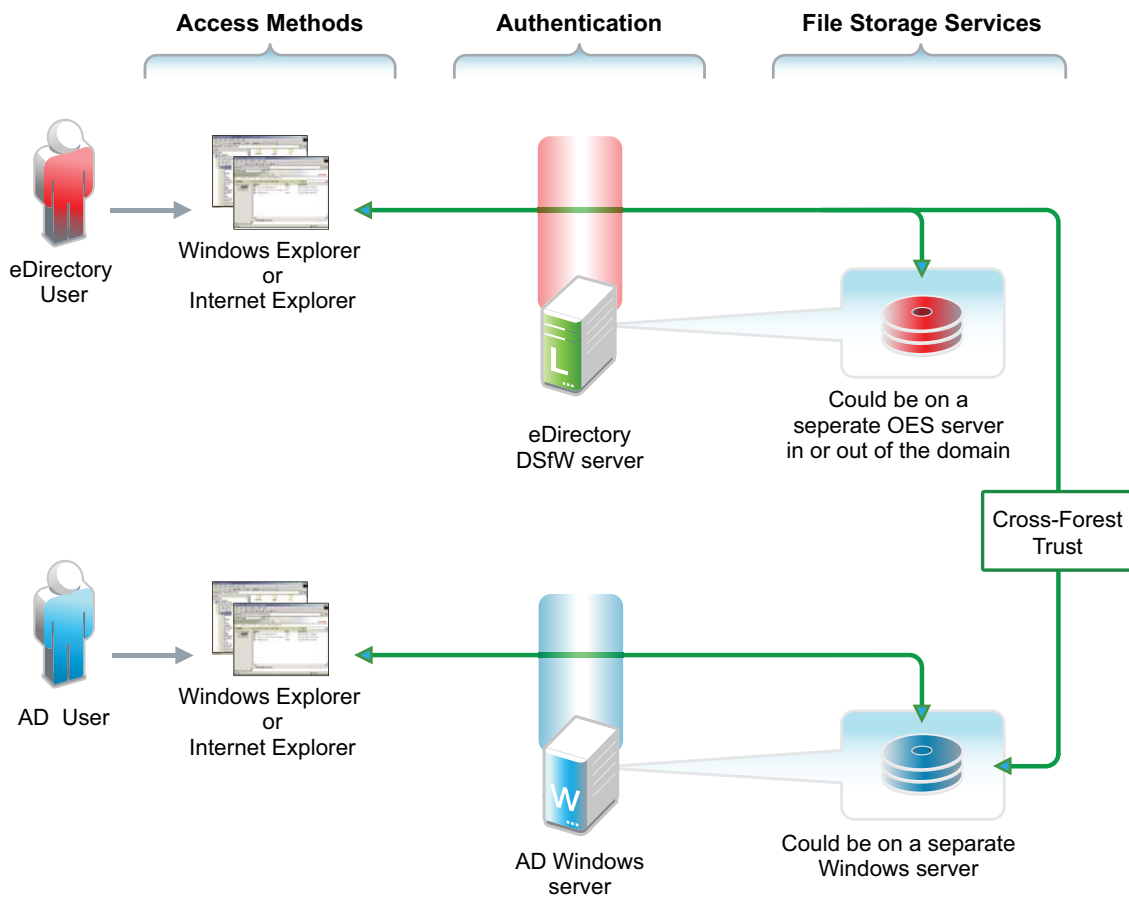


Table 14-1 DSfW File Access

Access Methods	Authentication	File Storage Services
<p>eDirectory and Active Directory users on Windows workstations can access files through Windows Explorer (CIFS) or Internet Explorer (WebDAV Web Folders). No Novell Client is needed on the machine.</p> <p>Unlike Windows workgroup or Novell Samba, the user doesn't need to have a matching username and password on the local workstation.</p> <p>Although not shown, Novell Client users can also access files through a normal NCP connection.</p>	<p>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.</p> <p>For AD users, file service access is controlled by authentication through the AD server.</p>	<p>On OES servers, file storage services are provided by Samba to NSS or traditional Linux file systems.</p> <p>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.</p>

User Management

Figure 14-3 DSfW User Management Overview

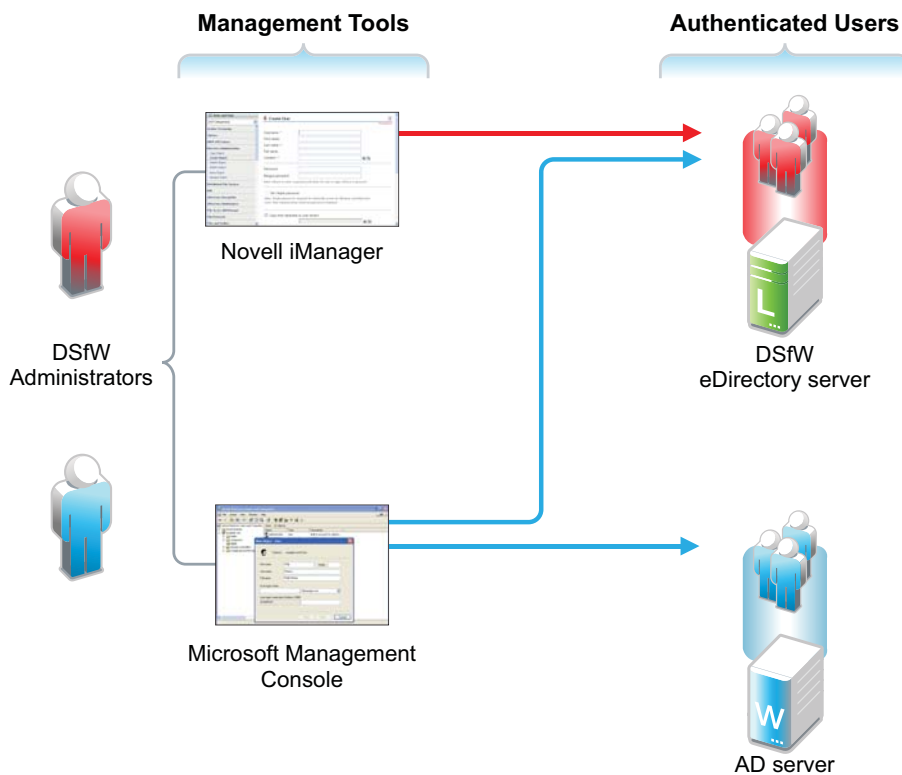


Table 14-2 DSfW User Management

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

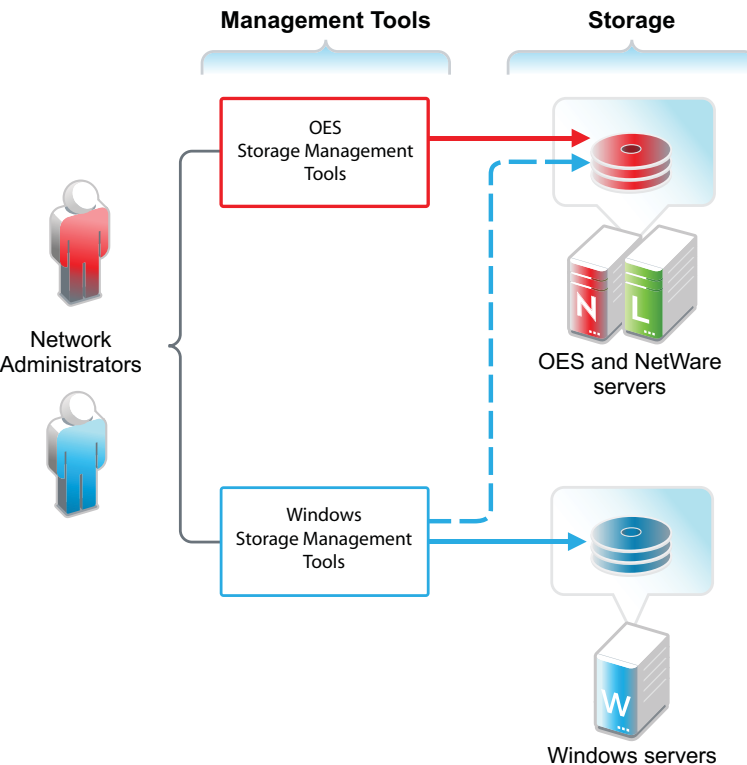


Table 14-3 DSfW Storage Management

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 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 11 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 11 SP2: Domain Services for Windows Administration Guide](#), especially the “[Troubleshooting DSfW](#)” section.

- ♦ [“Implement Universal Password Before DSfW in a Name-Mapped Scenario” on page 214](#)
- ♦ [“DSfW Must Be Installed at the Root of an eDirectory Partition” on page 214](#)
- ♦ [“Hierarchical Placement of Users in the eDirectory Tree” on page 214](#)
- ♦ [“OES 11 Service Limitations” on page 214](#)
- ♦ [“Install DSfW on a New OES 11 Server When Possible” on page 214](#)
- ♦ [“DNS Configuration” on page 215](#)

Implement Universal Password Before DSfW 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.

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 11 Service Limitations

Only designated OES 11 services can be installed on a DSfW server. For more information, see “[Unsupported Service Combinations](#)” in the [OES 11 SP2: Domain Services for Windows Administration Guide](#).

Install DSfW on a New OES 11 Server When Possible

Because of the service limitations mentioned in [OES 11 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.

15 Users and Groups

Networks exist to serve users and groups of users. Open Enterprise Server 11 SP2 provides strong user and group management through eDirectory and its associated technologies.

- ♦ [Section 15.1, “Creating Users and Groups,” on page 217](#)
- ♦ [Section 15.2, “Linux User Management: Access to Linux for eDirectory Users,” on page 217](#)
- ♦ [Section 15.3, “Identity Management Services,” on page 226](#)
- ♦ [Section 15.4, “Using the Identity Manager 4.0.2 Bundle Edition,” on page 226](#)

15.1 Creating Users and Groups

All OES services require that you create User objects to represent the users on your system. The Linux User Management (LUM) and Samba components on OES 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 [OES 11: Getting Started Guide](#) provides introductory exercises 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 [OES 11 SP2: Novell Samba Administration Guide](#).

For detailed information on understanding, creating, and managing the various objects your organization might require, see the [NetIQ eDirectory 8.8 SP8 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 218](#)
- ♦ [Section 15.2.2, “LUM Changes,” on page 223](#)
- ♦ [Section 15.2.3, “Planning,” on page 223](#)
- ♦ [Section 15.2.4, “LUM Implementation Suggestions,” on page 223](#)

15.2.1 Overview

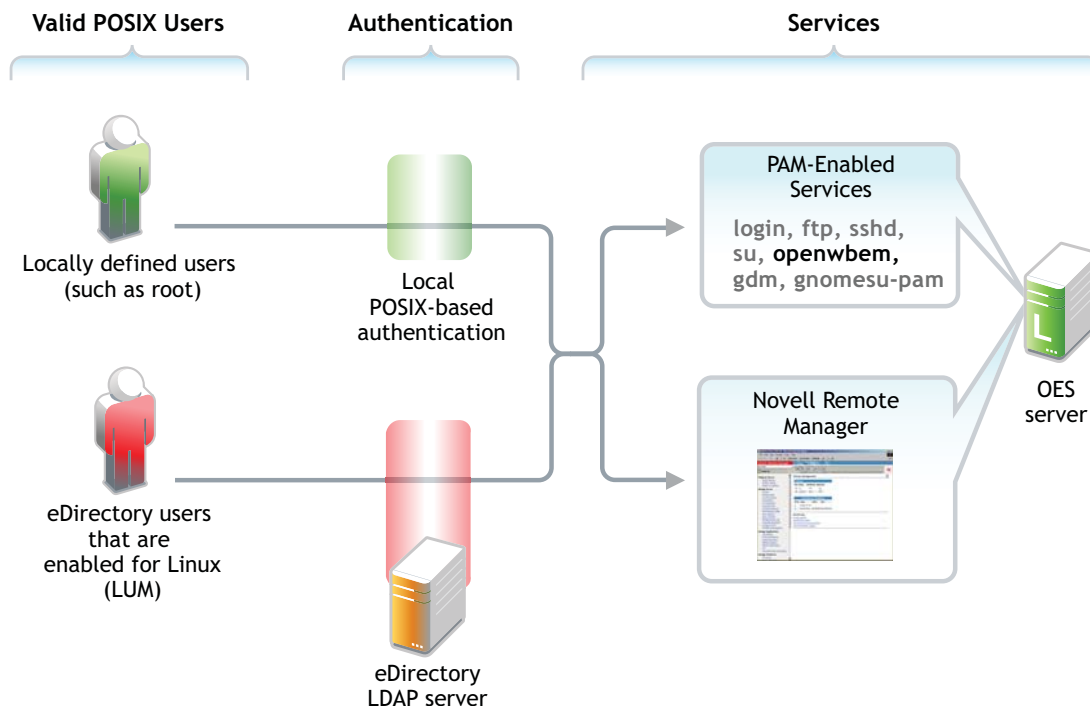
The topics in this section are designed to help you understand when LUM-enabled access is required so that your network services are accessible and work as expected. For more information about Linux User Management, see “[Overview](#)” in the *OES 11 SP2: Novell Linux User Management Administration Guide*.

- ♦ “[A Graphical Preview of Linux User Management](#)” on page 218
- ♦ “[Linux Requires POSIX Users](#)” on page 219
- ♦ “[Linux Users Can Be Local or Remote](#)” on page 219
- ♦ “[The root User Is Never LUM-Enabled](#)” on page 219
- ♦ “[About Service Access on OES](#)” on page 220
- ♦ “[OES Services That Require LUM-Enabled Access](#)” on page 220
- ♦ “[OES Services That Do Not Require LUM-Enabled Access But Have Some LUM Requirements](#)” on page 221
- ♦ “[OES Services That Do Not Require LUM-enabled Access](#)” on page 222
- ♦ “[LUM-Enabling Does Not Provide Global Access to ALL OES Servers](#)” on page 222
- ♦ “[LUM-Enabling Required for Full Administrative Access](#)” on page 222

A Graphical Preview of Linux User Management

Figure 15-1 illustrates how Linux User Management controls access to the OES 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 servers must be accessed by POSIX users.	When the system receives an action request, it can authenticate both local POSIX users and users who have been enabled for Linux access.	Users can potentially access PAM-enabled services, Samba shares, and Novell Remote Manager as either local or eDirectory users.
eDirectory users can function as POSIX users if they are enabled for Linux access (LUM).		By default, only the <code>sfcbl</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 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 118](#).

-
- ♦ **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 user management tools prevent you from creating an eDirectory user named `root`, thus replacing the `root` user on an OES 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

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

In other words, LUM lets eDirectory users function as local (POSIX) users on an OES 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 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 224](#).

OES Services That Require LUM-Enabled Access

Some services on an OES server require that eDirectory users be LUM-enabled to use them:

- ♦ **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 an OES server through Samba does not create a home directory on the server.

- ♦ **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 or services.

IMPORTANT: Before you accept the default PAM-enabled service settings, be sure you understand the security implications explained in [Section 22.2.2, “User Restrictions: Some OES Limitations,” on page 297](#).

The core utilities available for PAM-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 server which, in this case, is a remote host.
gdm	♦ Local host ♦ Remote host	Run and manage the X servers using XDMCP.
gnomesu-pam	Local host	Required for GNOME applications that need superuser access.
login	♦ OES server ♦ SSH session with OES server	Log in to the OES server, either directly or in an SSH session with the server.

Command	Where Executed	Task
sfcfb	Local host	Required for iPrint, NSS, SMS, Novell Remote Manager, and iManager.
sshd	Another host	Establish a secure encrypted connection with the OES server which, in this case, is a remote host.
su	<ul style="list-style-type: none"> ♦ OES server ♦ SSH session with OES server 	<p>Temporarily become another user.</p> <p>This is most often used to temporarily become the <code>root</code> user, who is not a LUM user and is, therefore, not affected by LUM.</p>

NOTE: Logging in to the OES server through a PAM-enabled service for the first time causes the creation of a home directory in `/home` 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 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, who has rights to see everything on the Linux server, including NSS volumes.
 - ♦ A local Linux user with access governed by POSIX access rights. (Having local users in addition to `root` is not recommended on OES servers.)
 - ♦ A LUM-enabled eDirectory user, such as the Admin user created during the install.

OES 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 means they are then LUM-enabled), and they begin using Samba as a file service, their NetStorage uploaded files are not accessible through Samba until you make them the file owners from a POSIX perspective. 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 (proxy) User (initially a local user on the OES 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 11 SP2 installation program configures this correctly by default.

For more information, see [Appendix H, "System User and Group Management in OES 11 SP2," on page 335](#).

- ♦ **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.

OES Services That Do Not Require LUM-enabled Access

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

- ♦ iFolder 3.9.2
- ♦ 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 Servers

As you plan to LUM-enable users for access to the services that require it, keep in mind that each OES 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 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 each server must be formed by using iManager. This can be accomplished for multiple servers by using the process described in ["Enabling eDirectory Groups and Users for Linux Access" on page 224](#).

For more information on LUM, see the [OES 11 SP2: Novell Linux User Management Administration Guide](#).

LUM-Enabling Required for Full Administrative Access

The current LUM architecture requires that administrators, administrator equivalents, partition administrators, and RBS-enabled managers be LUM-enabled to have full management capabilities.

15.2.2 LUM Changes

In response to customer requests for improved LDAP performance, persistent searching for new Linux-enabled users and groups has been disabled in OES 2 SP3 and later.

For more information, see [Section 6.10, “LUM Cache Refresh No Longer Persistent,”](#) on page 125 and [“What’s New or Changed in Linux User Management”](#) in the *OES 11 SP2: Novell Linux User Management Administration Guide*.

15.2.3 Planning

The following sections summarize LUM planning considerations.

- ♦ [“eDirectory Admin User Is Automatically Enabled for Linux Access”](#) on page 223
- ♦ [“Planning Which Users to Enable for Access”](#) on page 223
- ♦ [“Be Aware of System-Created Users and Groups”](#) on page 223

eDirectory Admin User Is Automatically Enabled for Linux Access

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

This can be easily determined by doing the following:

1. Review the information in [“OES Services That Require LUM-Enabled Access”](#) on page 220.
2. Identify the servers that will run the services mentioned.
3. Note the users and groups that need access and then configure their objects and the target servers/services for that 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 H, “System User and Group Management in OES 11 SP2,”](#) on page 335.

15.2.4 LUM Implementation Suggestions

The following sections summarize LUM implementation considerations.

- ♦ [“About Enabling eDirectory Users for Linux Access”](#) on page 224
- ♦ [““UNIX Workstation” and “Linux Workstation” Are the Same Thing”](#) on page 224
- ♦ [“Enabling eDirectory Groups and Users for Linux Access”](#) on page 224

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 also lets you associate the group with one or more OES servers or Linux workstations.

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 11 SP2: Novell Linux User Management Administration Guide](#).

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

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

When OES servers are created, a “UNIX Workstation - *server_name*” object is created in eDirectory, where *server_name* is the DNS name of the OES 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 eDirectory Groups and Users for Linux Access

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 servers by associating the LUM-enabled groups to which the users belong with the UNIX Workstation objects you want users to have access to.

There are four methods for enabling eDirectory groups and users for Linux access:

- ♦ [“Using iManager to Enable Groups and any Users Assigned to Them” on page 224](#)
- ♦ [“Using iManager to Bulk-Enable Users in a LUM Group” on page 225](#)
- ♦ [“Using iManager to Bulk-Enable Users in a Container” on page 225](#)
- ♦ [“Using LUM Utilities at the Command Prompt” on page 225](#)

Using iManager to Enable Groups and any Users Assigned to Them

The following steps assume that the eDirectory Group objects already exist and that any User objects you want to enable for Linux at the same time 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 groups to be enabled for Linux, make sure the *Linux-Enable All Users in These Groups* option is selected.

- 5 Click *Next*.
- 6 If the groups contain users, click *Next* to confirm that you want them enabled.
- 7 Browse to and select a UNIX Workstation (OES server) object, then click *OK*.
- 8 Browse to and select the Unix Config Object for the workstation, then click *OK*.
- 9 Click *Next*, click *Finish*, then click *OK*.

Using iManager to Bulk-Enable Users in a LUM Group

The following steps assume that the eDirectory LUM-enabled Group objects already exist and that they have assigned non-LUM-enabled User objects that you want to enable for Linux access.

- 1 Log in to iManager as the eDirectory Admin user or equivalent.
- 2 Click *Linux User Management > Bulk-Enable Users in a LUM Group*.
- 3 Browse to and select one or more LUM-enabled Group objects, then click *OK*.
- 4 Browse to and select the Unix Config Object, then click *OK*.
- 5 Click *Next*.
- 6 Click *Finish* to confirm that you want the listed users enabled for Linux.
- 7 Click *OK*.

Using iManager to Bulk-Enable Users in a Container

The following steps assume that eDirectory non-LUM-enabled User objects exist inside an eDirectory container (OU object) and that you want to enable these User objects for Linux access.

- 1 Log in to iManager as the eDirectory Admin user or equivalent.
- 2 Click *Linux User Management > Bulk-Enable Users in a Container*.
- 3 Browse to and select the Container (OU) object, then click *OK*.
- 4 Browse to and select the Unix Config Object, then click *OK*.
- 5 Browse to and select the LUM-enabled group that you want the users associated with for Linux access.
- 6 Click *Next*.
- 7 Observe that all user objects in the container are listed for assignment to the group you have selected as the primary group. If you don't want already enabled user objects that are currently assigned to a different primary group to have that assignment changed, you must deselect them at this point.
- 8 Click *Finish* to confirm that you want the selected users enabled for Linux (if not already) and assigned to the select group.
- 9 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 11 SP2: Novell Linux User Management Administration 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 11 SP2: Novell Linux User Management Administration 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 NetIQ 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 provide seamless file and print access to OES servers by using the NCP server for Linux and iPrint services. For more information, see [Section 18.6, “NCP Implementation and Maintenance,” on page 276](#) and [Chapter 19, “Print Services,” on page 283](#).
- ♦ If you want eDirectory users to have access to OES 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 217](#).
- ♦ 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 NetIQ Identity Manager. For more information, see [Section 15.4, “Using the Identity Manager 4.0.2 Bundle Edition,” on page 226](#).

15.4 Using the Identity Manager 4.0.2 Bundle Edition

NetIQ 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.

This section discusses the following:

- ♦ [Section 15.4.1, “What Am I Entitled to Use?,” on page 227](#)
- ♦ [Section 15.4.2, “System Requirements,” on page 227](#)
- ♦ [Section 15.4.3, “Installation Considerations,” on page 227](#)
- ♦ [Section 15.4.4, “Getting Started,” on page 227](#)
- ♦ [Section 15.4.5, “Activating the Bundle Edition,” on page 228](#)

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:

- ♦ Legacy Identity Manager Driver for eDirectory (eDir2eDir)

IMPORTANT: The Bi-directional eDirectory driver is not included in the Bundle Edition entitlement.

- ♦ 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 *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 4.0.2 Framework Installation Guide](#).

The Bundle Edition does not include Solaris or AIX support. To run the Identity Manager engine or Integration Modules on these platforms, you must purchase Identity Manager.

15.4.3 Installation Considerations

NetIQ 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 228](#).

15.4.4 Getting Started

The following sections from the [Identity Manager 4.0.2 documentation](#) will help you plan, install, and configure your Identity Manager 4.0.2 Bundle Edition.

- ♦ [Overview](#)
- ♦ [Planning](#)
- ♦ [Installing Identity Manager](#)
- ♦ [Installing Active Directory and eDirectory Drivers](#)
- ♦ [Password Synchronization across Connected Systems](#)

See [Policy Builder and Driver Customization Guide](#) for information about customizing your Identity Manager implementation.

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 *Identity Manager*. See [Activating Identity Manager Products Using a Credential](#) 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](#) 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, then choose *Identity Manager > Identity Manager Overview* and select the driver set or browse to a driver set, then click *Next*.
- 5 On the Identity Manager Overview page, locate the driver set, click the red *Activation required by* link, then click *Install Activation*.
- 6 Select the driver set where you want to activate an Identity Manager component.
- 7 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*.
- 8 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 OES, and create a driver set on the server.

I installed the Bundle Edition but it's not activated. Why?

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 Identity Manager Engine (on your OES server) and a remote driver (on the Windows server.)

In order to run Identity Manager on a Windows server, you need to purchase *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 Identity Engine and a remote driver (on the Solaris or AIX server.)

In order to run Identity Manager on Solaris or AIX, you need to purchase *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 OES server where OES exists. If Identity Manager is installed on a non-OES platform, activation cannot work. After 90 days, your drivers 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 *Identity Manager*. The Integration Module cannot activate until you purchase *Identity Manager*.

If I purchase licenses for NetIQ Identity Manager and an additional Integration Module, must I re-install?

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 for Identity Manager and for Drivers](#).

16 Access Control and Authentication

Access Control and Authentication are the keys to:

- ♦ Providing services for users.
- ♦ Ensuring that the network is secure.

This section discusses the following:

- ♦ [Section 16.1, “Controlling Access to Services,” on page 231](#)
- ♦ [Section 16.2, “Authentication Services,” on page 242](#)

16.1 Controlling Access to Services

OES 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 you 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 231](#)
- ♦ [Section 16.1.2, “Planning for Service Access,” on page 237](#)
- ♦ [Section 16.1.3, “Coexistence and Migration of Access Services,” on page 240](#)
- ♦ [Section 16.1.4, “Access Implementation Suggestions,” on page 240](#)
- ♦ [Section 16.1.5, “Configuring and Administering Access to Services,” on page 240](#)

16.1.1 Overview of Access Control

The following sections present overviews of methods for accessing Open Enterprise Server 11 SP2 services.

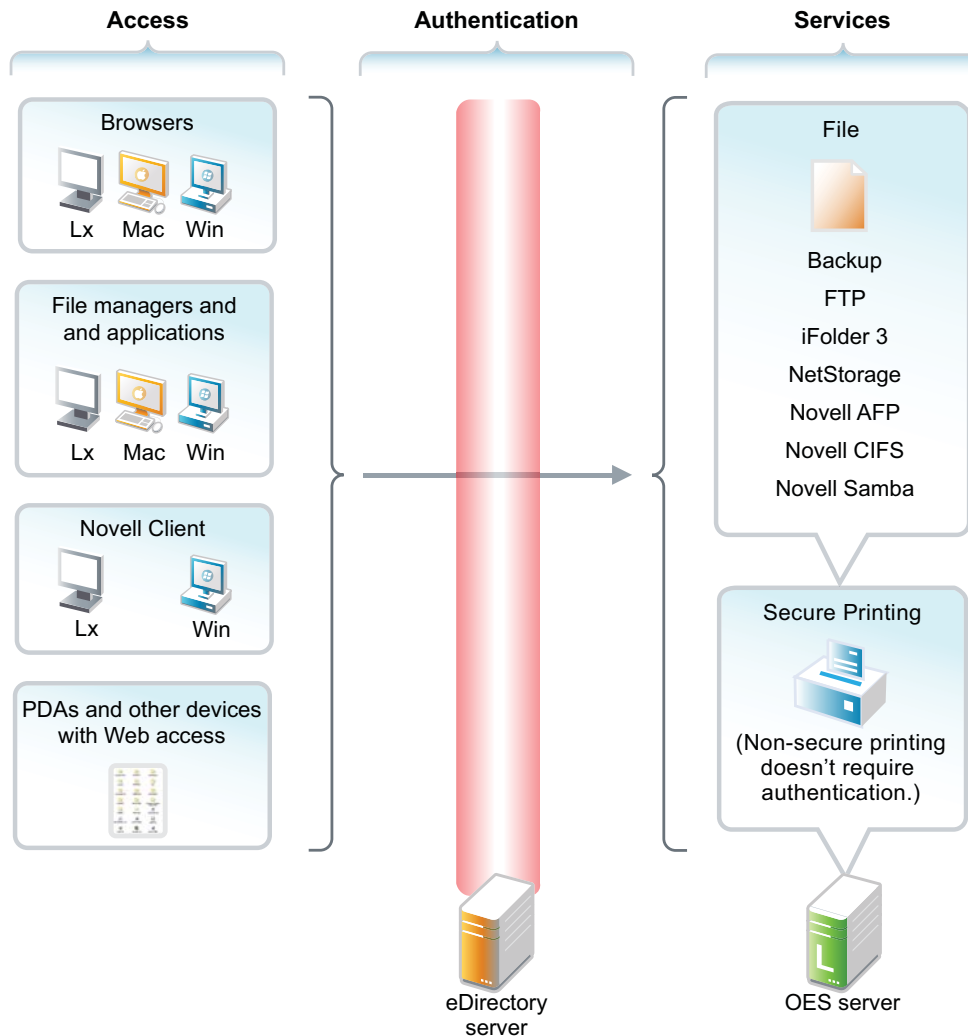
- ♦ [“Access to OES 11 SP2 Services” on page 232](#)
- ♦ [“Access Control Options in OES” on page 233](#)
- ♦ [“The Traditional Novell Access Control Model” on page 234](#)
- ♦ [“NSS Access Control on OES” on page 235](#)

- ♦ “Novell Client (NCP File Services) Access” on page 236
- ♦ “eDirectory User Access to OES Servers” on page 237

Access to OES 11 SP2 Services

Figure 16-1 illustrates the access methods supported by OES 11 SP2 services. NetIQ 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 services can help you begin to plan your OES implementation. For more information, see [“Matching Protocols and Services to Check Access Requirements” on page 239](#).

Access Control Options in OES

Because OES 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 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 how they let you assign file and directory permissions to users and groups who do not own the files or directories.	“Access Control Lists in Linux” (http://www.suse.com/documentation/sles11/book_security/data/cha_acls.html) in the <i>SLES 11 SP3: Security Guide</i> (http://www.suse.com/documentation/sles11/index.html)
Aligning NCP and POSIX access rights	How to approximate the Novell access control model on POSIX file systems.	“Section 18.4, “Aligning NCP and POSIX File Access Rights,” on page 264”
Directory and file attributes	Directory and file attributes on NSS volumes.	“Understanding Directory and File Attributes for NSS Volumes” in the <i>OES 11 SP2: File Systems Management Guide</i>
File system trustee rights	File system trustee rights on NetWare (NSS and traditional volumes), including how file system trustee rights work.	“Understanding the Novell Trustee Model for File System Access” in the <i>OES 11 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.	“Understanding File System Access Control Using Trustees” in the <i>OES 11 SP2: File Systems Management Guide</i>
POSIX file system rights and attributes on Linux	How to configure file system attributes on OES 11 SP2 servers.	“Access Control Lists in Linux” (http://www.suse.com/documentation/sles11/book_security/data/cha_acls.html) in the <i>SLES 11 SP3: Security Guide</i> (http://www.suse.com/documentation/sles11/index.html)
Security Equivalence in eDirectory	The concept of Security Equivalence in eDirectory.	“Security Equivalence” in the <i>OES 11 SP2: File Systems Management Guide</i>

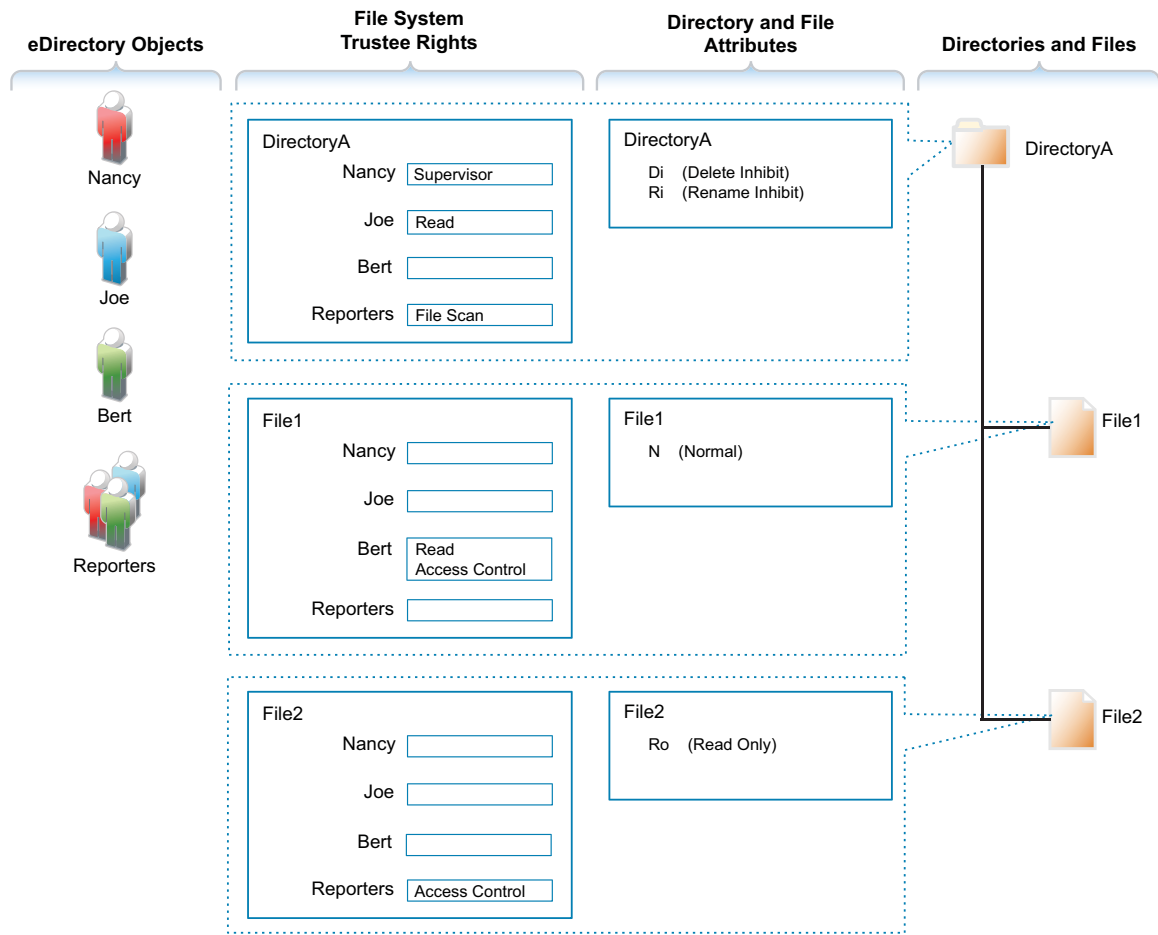
The Traditional Novell Access Control Model

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 volume access controls are not equivalent to NSS because they are constrained by Linux POSIX access controls, which 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, because she has the Supervisor right, Nancy could modify the file attributes so that File2 could then be deleted.</p>	<p>Each directory and file has attributes associated with it. These attributes apply universally to all trustees regardless of the trustee rights an object might have.</p> <p>For example, a file that has the Read Only attribute is Read Only for all users.</p> <p>Attributes can be set by any trustee that has the Modify trustee right to the directory or file.</p>	<p>The possible actions by the eDirectory users and group shown in this example are as follows:</p> <ul style="list-style-type: none"> ◆ Nancy has the Supervisor trustee right at the directory level, meaning that she can perform any action not blocked by a directory or file attribute. <p>The Di (Delete Inhibit) and Ri (Rename Inhibit) Attributes on Directory A prevent Nancy from deleting or renaming the directory unless she modifies the attributes first. The same principle applies to her ability to modify File2.</p> <ul style="list-style-type: none"> ◆ Because Joe is a member of the Reporters group, he can view file and directory names inside DirectoryA and also see the directory structure up to the root directory. <p>Joe also has rights to open and read any files in DirectoryA and to execute any applications in DirectoryA.</p> <ul style="list-style-type: none"> ◆ Because Bert is a member of the Reporters group, he can view file and directory names inside DirectoryA and also see the directory structure up to the root directory. <p>Bert also has rights to open and read File1 and to execute it if it's an application.</p> <p>And Bert has rights to grant any eDirectory user access to File1.</p> <ul style="list-style-type: none"> ◆ Because all three users are members of the Reporters group, they can grant any eDirectory user access to File2. <p>Of course, for Nancy this is redundant because she has the Supervisor right at the directory level.</p>

NSS Access Control on OES

Table 16-3 provides links to documentation that discusses the various NSS-specific access control features.

Table 16-3 Summary of NSS Access Control Documentation Links

Feature	To Understand	See
Independent Mode vs. NetWare Mode This applies only to OES servers, not NetWare.	The difference between Independent Mode access and NetWare Mode access.	“Access Control for NSS on Linux” in the <i>OES 11 SP2: File Systems Management Guide</i>
POSIX directory and file attributes on NSS volumes on OES This describes what is displayed. POSIX permissions are not actually used for access control to NSS volumes.	How NSS file attributes are reflected in Linux directory and file permissions viewable through POSIX.	“Viewing Key NSS Directory and File Attributes as Linux POSIX Permissions” in the <i>OES 11 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 236](#)
- ♦ [“Is the Novell Client Right for Your Network?” on page 236](#)
- ♦ [“Differences between Linux and Windows” on page 237](#)

About the Novell Client

The Novell Client extends the capabilities of Windows and Linux desktops with access to NetWare and OES servers.

After installing Novell Client software, users can enjoy the full range of Novell services, such as

- ♦ Authentication via NetIQ eDirectory
- ♦ Network browsing and service resolution
- ♦ Secure and reliable file system access
- ♦ Support for industry-standard protocols

The Novell Client supports the traditional Novell protocols (NDAP, NCP, and RSA) and interoperates with open protocols (LDAP, CIFS, and NFS).

Is the Novell Client Right for Your Network?

Although Novell offers services that don't require Novell Client, (such as NetStorage, Novell iFolder 3.9.2, and iPrint), many network administrators prefer that their network users access the network through the client 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 Servers

eDirectory users have access to services on OES servers just like they do on NetWare, with one additional consideration—to access some of the services, users must have Linux user credentials, such as a user ID (UID) and primary group ID (GID).

Because eDirectory users don't have Linux user credentials by default, Novell provides the Linux User Management (LUM) technology. Users and groups who need access to the affected services, 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 217.

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 237
- ♦ [“Planning Print Service Access”](#) on page 238
- ♦ [“Matching Protocols and Services to Check Access Requirements”](#) on page 239

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 237
- ♦ [“Feature Support”](#) on page 238

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 Samba	Yes-Novell CIFS, Novell Samba
NetStorage	Yes	Yes
NetWare Core Protocol (NCP)	Yes	Yes
NFS	Yes	Yes-NFSv3
Novell iFolder 2.1x	No	No
Novell iFolder 3.9.2	Yes	Yes

Details about the file systems supported by each file service are explained in the documentation for the 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 239](#).

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 configured as an NCP volume)	Yes
Novell directory and file attributes	No	Yes
Purge/Salvage	No	Yes
Trustee rights	Yes (if configured 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 for each eDirectory User, Group, or container object 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 11 SP2: iPrint Linux Administration Guide*

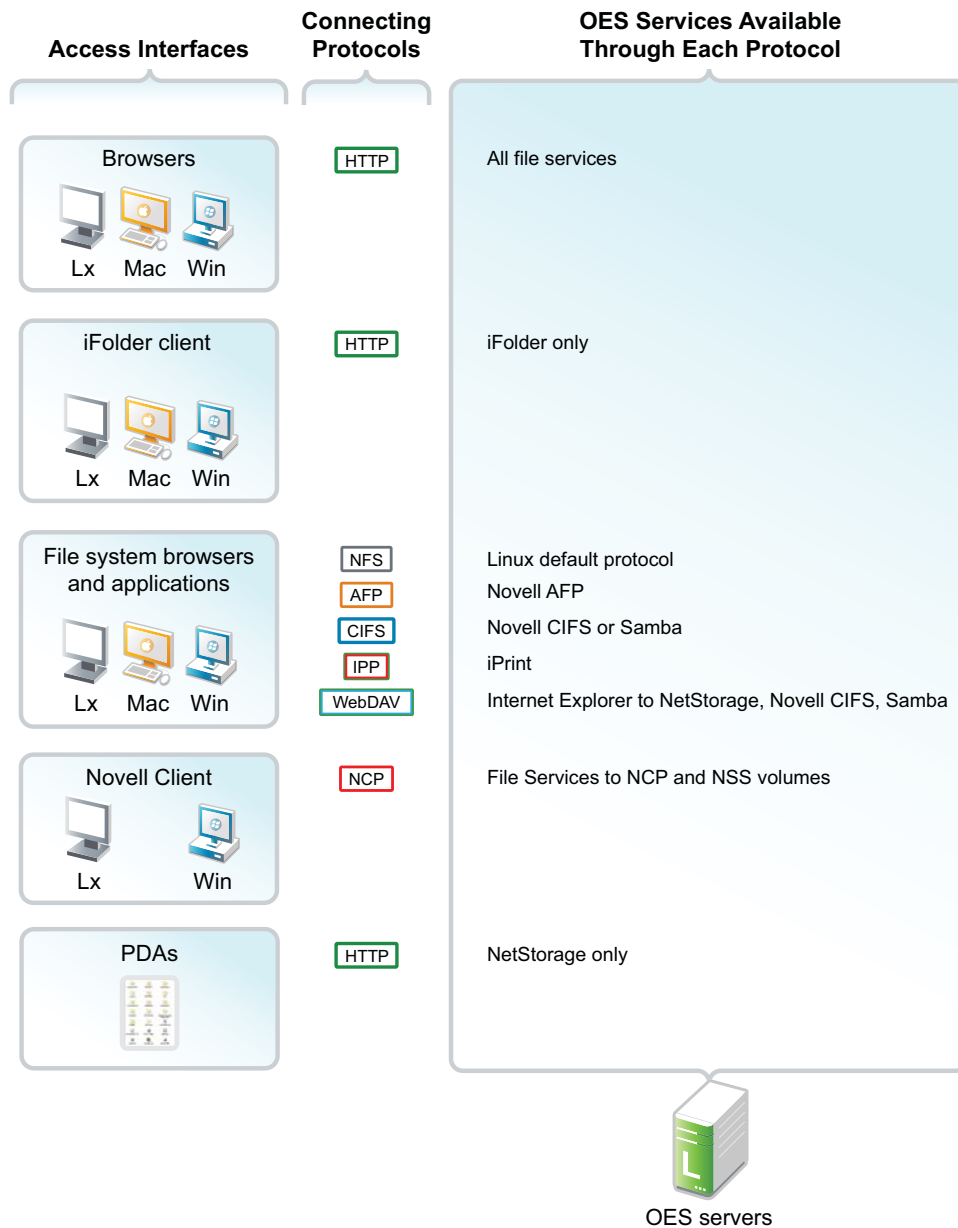
Matching Protocols and Services to Check Access Requirements

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 available in OES, your Novell Client users can attach to OES 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 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. 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 11 SP2: NCP Server for Linux Administration Guide](#).

16.1.4 Access Implementation Suggestions

After you plan and install OES services, be sure to provide clear access instructions to your network users. For a summary of access methods, see [Appendix D, "Quick Reference to OES User Services," on page 325](#).

16.1.5 Configuring and Administering Access to Services

The following sections discuss administering access to services.

- ♦ ["Password Management" on page 240](#)
- ♦ ["Linux \(POSIX\) File System Access Rights" on page 240](#)
- ♦ ["NSS File and Directory Trustee Management" on page 241](#)

Password Management

Many network administrators let users administer their own passwords. For more information on password self management, see ["Password Self-Service"](#) in the [NetIQ Password Management 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 Trustees and File System Attributes](#)” in the *OES 11 SP2: File Systems Management Guide*.

NSS File and Directory Trustee Management

The *OES 11 SP2: File Systems Management Guide* contains a thorough discussion of file and directory trustee management in its “[Configuring Trustees and File System 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 241
- ♦ “[Using the Novell Client to Change File and Directory Attributes and Trustee Rights](#)” on page 241
- ♦ “[Using iManager 2.7 to Change File and Directory Attributes and Trustee Rights](#)” on page 241
- ♦ “[Using the Linux Command Prompt to Change File Attributes](#)” on page 241
- ♦ “[Using the Linux Command Prompt to Change Trustee Rights](#)” on page 242

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 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 “[Using the Attrib Utility to Set NSS File System Attributes](#)” in the *OES 11 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 “Using the Rights Utility to Set Trustee Rights for the NSS File System” in the *OES 11 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 242](#)
- ♦ [Section 16.2.2, “Planning for Authentication,” on page 245](#)
- ♦ [Section 16.2.3, “Authentication Coexistence and Migration,” on page 245](#)
- ♦ [Section 16.2.4, “Configuring and Administering Authentication,” on page 245](#)

16.2.1 Overview of Authentication Services

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

- ♦ [“NetIdentity Agent” on page 242](#)
- ♦ [“NetIQ Modular Authentication Services \(NMAS\)” on page 243](#)
- ♦ [“Password Support in OES” on page 243](#)

For more authentication topics, see [“access, authenticate, log in \(http://www.novell.com/documentation/oes11/index.html#cat_acc-auth-log\)”](http://www.novell.com/documentation/oes11/index.html#cat_acc-auth-log) in the OES online documentation.

NetIdentity Agent

In OES 11, the NetIdentity Agent works with NetIQ 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 11 server included 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](#).

NetIQ Modular Authentication Services (NMAS)

NetIQ Modular Authentication Services (NMAS) lets you protect information on your network by providing various authentication methods to NetIQ 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.
- ♦ **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.

For more information on how to use NMAS, see the [NetIQ Modular Authentication Services Administration Guide](#).

Password Support in OES

In the past, administrators have needed to manage multiple passwords (simple password, NDS passwords, Samba passwords) because of password differences. Administrators have also needed to deal with keeping the passwords synchronized.

In OES you have the choice of retaining your current password maintenance methods or deploying Universal Password to simplify password management. For more information, see the [NetIQ Password Management Administration Guide](#).

All Novell products and services are being developed to work with extended character (UTF-8 encoded) passwords. For a current list of products and services that work with extended characters, see [Novell TID 3065822 \(http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3065822&sliceId=1&docTypeID=DT_TID_1_1&dialogID=77556590&stateId=0%200%2077560425\)](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3065822&sliceId=1&docTypeID=DT_TID_1_1&dialogID=77556590&stateId=0%200%2077560425).

The password types supported in eDirectory are summarized in [Table 16-7](#).

Table 16-7 eDirectory Password Types

Password Type	Description
NDS	The NDS password is stored in a hash form that is nonreversible in eDirectory. Only the NDS system can make use of this password, and it cannot be converted into any other form for use by any other system.
Novell AFP and Novell CIFS	In OES 11 SP2, AFP and CIFS users have Universal Password policies assigned by default. More information about password policy planning is available in Appendix J, “Coordinating Password Policies Among Multiple File Services,” on page 363.
Samba	<p>In OES 11 SP2, Samba users have a Universal Password policy assigned by default.</p> <p>OES 11 SP2 also supports the Samba hash password if desired. However, you must choose to not deploy Universal Password if you want to use the Samba hash password. Choosing the Samba password requires that users always remember to synchronize it when changing their eDirectory password.</p> <p>For more information, see “Samba Passwords” in the <i>OES 11 SP2: Novell 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>
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 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 server. (You can optionally choose to have the Samba hash password stored separately. This requires, however, that users always synchronize the Samba password when changing their eDirectory password.)</p> <p>The Novell Client supports the Universal Password. It also supports the NDS password for older systems in the network. The Novell Client automatically upgrades to use Universal Password when UP is deployed.</p> <p>For more information, see “Deploying Universal Password” in the <i>NetIQ Password Management Administration Guide</i>.</p>

16.2.2 Planning for Authentication

For planning topics, see the “[access, authenticate, log in \(http://www.novell.com/documentation/oes11/index.html#cat_acc-auth-log\)](http://www.novell.com/documentation/oes11/index.html#cat_acc-auth-log)” in the OES online documentation.

16.2.3 Authentication Coexistence and Migration

For authentication and security coexistence and migration information, see “[Chapter 22, “Security,” on page 293](#) and [Chapter 23, “Certificate Management,” on page 307](#)” in this guide.

16.2.4 Configuring and Administering Authentication

For a list of configuration and administration topics, see “[access, authenticate, log in \(http://www.novell.com/documentation/oes11/index.html#cat_acc-auth-log\)](http://www.novell.com/documentation/oes11/index.html#cat_acc-auth-log)” in the OES online documentation.

17 Backup Services

The following sections briefly outline the backup services available in Open Enterprise Server 11 SP2.

- ♦ [Section 17.1, “Services for End Users,” on page 247](#)
- ♦ [Section 17.2, “System-Wide Services,” on page 247](#)

17.1 Services for End Users

OES 11 SP2 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 3.9.2:** By implementing Novell iFolder 3.9.2, you empower your users to have their local files automatically follow them everywhere—online, offline, all the time—across computers. Users can share files in multiple iFolders, and share each iFolder with a different group of users. Users control who can participate in an iFolder and their access rights to the files in it. Users can also participate in iFolders that others share with them.
- ♦ **Salvage and Purge:** By default, all NSS volumes have the Salvage system enabled at the time they are created. With Salvage enabled, deleted files are retained on the volume for a short time, during which users can restore (salvage) them. File are eventually purged from the system, either manually, or by the system when the Purge Delay setting times out or space is needed on the volume.

17.2 System-Wide Services

OES offers both Novell Storage Management Services and services that are available as part of the SUSE Linux Enterprise Server distribution.

- ♦ [Section 17.2.1, “Links to Backup Partners,” on page 247](#)
- ♦ [Section 17.2.2, “Novell Storage Management Services \(SMS\),” on page 247](#)
- ♦ [Section 17.2.3, “SLES 11 Backup Services,” on page 248](#)

17.2.1 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).

17.2.2 Novell Storage Management Services (SMS)

- ♦ [“Understanding SMS” on page 248](#)
- ♦ [“SMS Coexistence and Migration Issues” on page 248](#)

Understanding SMS

Novell Storage Management Services (SMS) is not a backup application. Rather, it provides a standard framework and the necessary interfaces that can be used in developing a complete backup/restore solution. SMS helps back up file systems (such as NSS) on OES 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 11, the SMS API framework is available on SLES 11 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 11 SP2: Storage Management Services Administration Guide for Linux*.

17.2.3 SLES 11 Backup Services

Two SLES 11 services might be of interest.

- ♦ **DRBD:** 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 [Distributed Replicated Block Device \(DRBD\)](http://www.novell.com/documentation/sle_ha/book_sleha/data/cha_ha_drbd.html) (http://www.novell.com/documentation/sle_ha/book_sleha/data/cha_ha_drbd.html) in the *SLES 11 High Availability Guide* (http://www.novell.com/documentation/sle_ha/book_sleha/data/book_sleha.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.suse.com/documentation/sles11/book_sle_admin/data/sec_net_sync_rsync.html)” (http://www.suse.com/documentation/sles11/book_sle_admin/data/sec_net_sync_rsync.html) in the *SLES 11 Installation and Administration Guide* (http://www.suse.com/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html).

18 File Services

The file services in Open Enterprise Server 11 SP2 let you provide Web-based and network-based file services to your network users.

This section contains the following information:

- ♦ [Section 18.1, “Overview of File Services,” on page 249](#)
- ♦ [Section 18.2, “Planning for File Services,” on page 259](#)
- ♦ [Section 18.3, “Coexistence and Migration of File Services,” on page 262](#)
- ♦ [Section 18.4, “Aligning NCP and POSIX File Access Rights,” on page 264](#)
- ♦ [Section 18.5, “Novell FTP \(Pure-FTPd\) and OES 11 SP2,” on page 268](#)
- ♦ [Section 18.6, “NCP Implementation and Maintenance,” on page 276](#)
- ♦ [Section 18.7, “NetStorage Implementation and Maintenance,” on page 277](#)
- ♦ [Section 18.8, “Novell AFP Implementation and Maintenance,” on page 279](#)
- ♦ [Section 18.9, “Novell CIFS Implementation and Maintenance,” on page 280](#)
- ♦ [Section 18.10, “Novell iFolder 3.9.2 Implementation and Maintenance,” on page 281](#)
- ♦ [Section 18.11, “Samba Implementation and Maintenance,” on page 282](#)

18.1 Overview of File Services

The file service components in OES include the following:

- ♦ [FTP Services \(page 250\)](#): Lets users securely transfer files to and from OES servers.
- ♦ [NetWare Core Protocol \(page 250\)](#): Provides NetWare Core Protocol (NCP) access to NCP volumes (including NSS volumes) that you define on OES server partitions.
- ♦ [NetStorage \(page 251\)](#): 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 \(page 254\)](#): Provides native Macintosh access to files stored on an NSS volume on an OES server.
- ♦ [Novell CIFS \(page 255\)](#): Provides native Windows (CIFS and HTTP-WebDAV) access to files stored on an NSS volume on an OES server.
- ♦ [Novell iFolder 3.9.22 \(page 256\)](#): Provides a Web-based and network-based repository (Novell iFolder server) that stores master copies of locally accessible files on the OES server.
- ♦ [Novell Samba \(page 257\)](#): Provides Windows (CIFS and HTTP-WebDAV) access to files stored on an OES server's file system.

The file service components in OES are generally compatible. However you cannot run Novell Samba on the same OES server as Novell AFP, Novell CIFS, or Domain Services for Windows, which is not reviewed as a file service, but includes an alternative Samba file service instead of Novell Samba.

18.1.1 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 18.2, “Planning for File Services,” on page 259](#).

18.1.2 FTP Services

OES 11 SP2 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 11 SP2 installation, 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 11 SP2.

For migration instructions and a brief FAQ, see “[Migrating FTP to OES 11 SP2](#)” in the *OES 11 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).

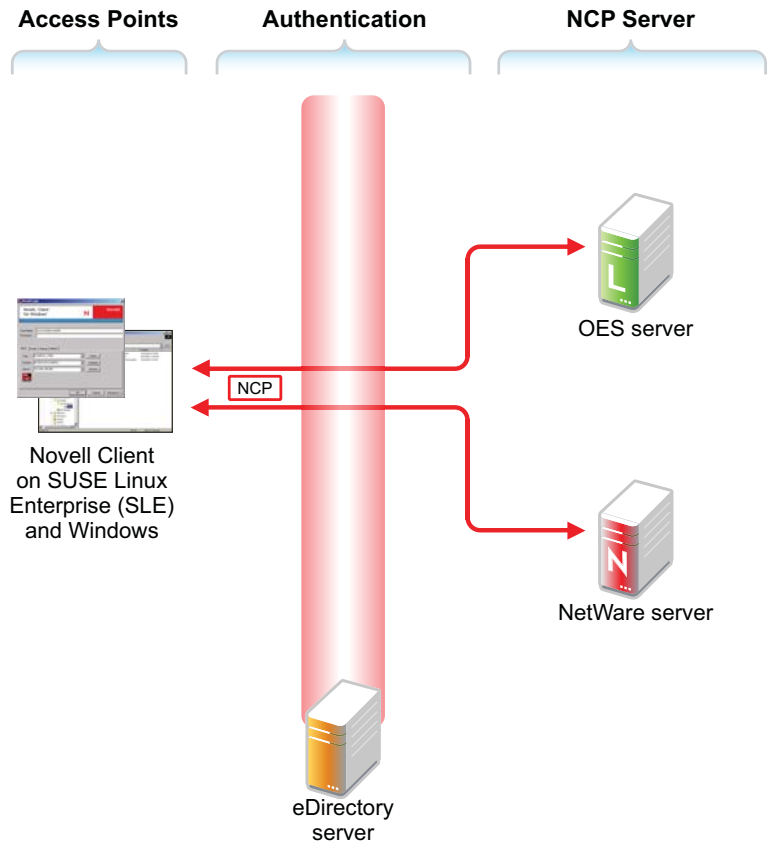
18.1.3 NetWare Core Protocol

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 access data, manage files and folders, map drives, etc., using the same methods as they do on NetWare servers.

[Figure 18-1](#) 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 231.

Figure 18-1 NCP Services for Linux and NetWare



The following table explains the information illustrated in [Figure 18-1](#).

Table 18-1 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. The same core set of NetWare file attributes are available on both Linux and NetWare.

18.1.4 NetStorage

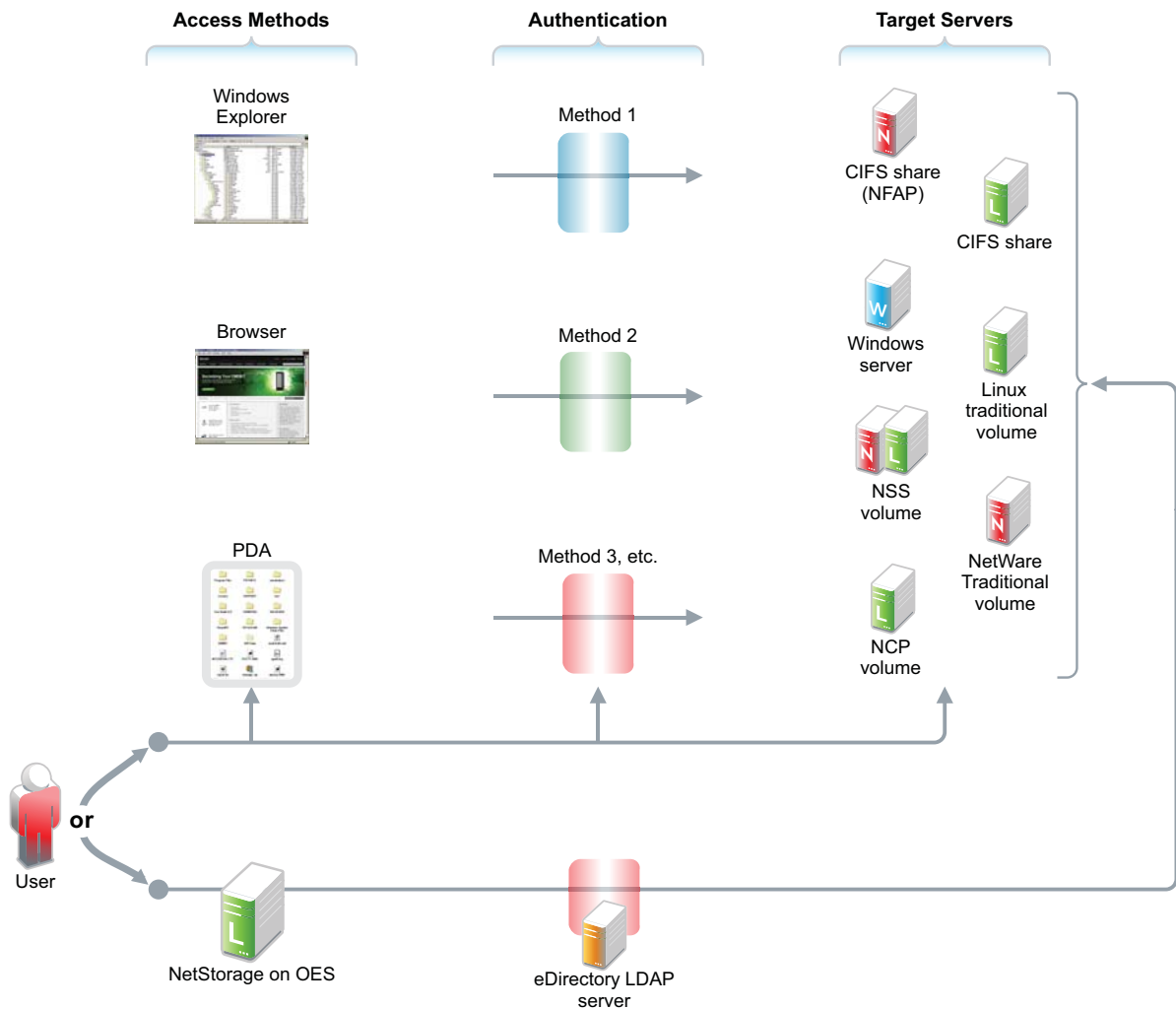
- ♦ [“Common Network File Storage Problems” on page 251](#)
- ♦ [“NetStorage” on page 252](#)

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 18-2](#).

Figure 18-2 Common Network File Storage Problems



The following table explains the information illustrated in [Figure 18-2](#).

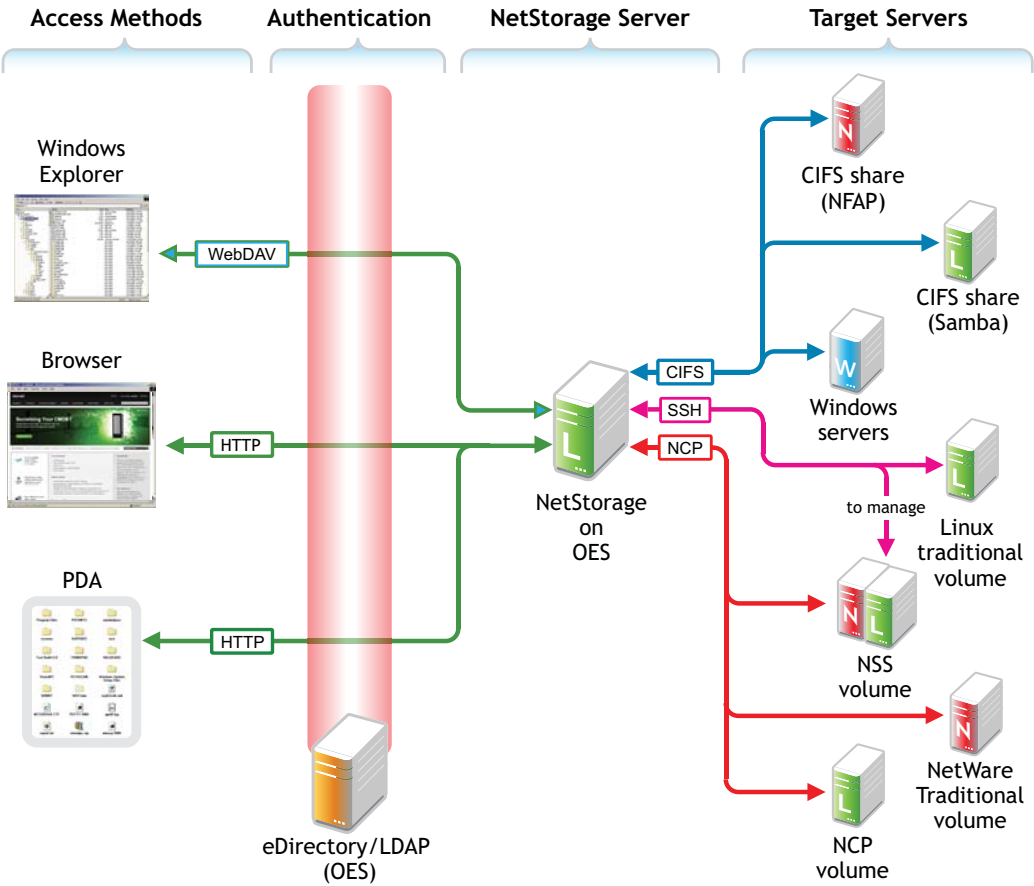
Table 18-2 NetStorage Access Solutions

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.

NetStorage

NetStorage on OES provides local and Web access to files on many systems without requiring the Novell Client (see [Figure 18-3](#)).

Figure 18-3 How NetStorage Works on OES



The following table explains the information illustrated in Figure 18-3.

Table 18-3 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"> ♦ Windows Explorer: Enabled by the HTTP protocol with WebDAV extensions. ♦ Browsers: Users can access files directly by connecting to the NetStorage server. ♦ PDAs: PDA users with network connections can access their files as well. <p>Access is granted through login script drive mapping (NCP server required) or through Storage Location Objects.</p>	<p>File service access is controlled by LDAP-based authentication through the eDirectory LDAP server.</p> <p>Although shown separately, eDirectory could be running on the OES 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"> ♦ Windows workgroup shares (CIFS or Samba shares) ♦ Linux POSIX volumes through an SSH connection. <p>Linux volumes can also be made available as NCP volumes.</p> <p>Management of NSS volumes on OES through NetStorage requires SSH access to the server. See “When Is SSH Access Required?” on page 155.</p>

18.1.5 Novell AFP

The Novell AFP service lets users on Macintosh workstations access and store files on OES servers with NSS volumes (see [Figure 18-4](#)).

Figure 18-4 How Novell AFP Works

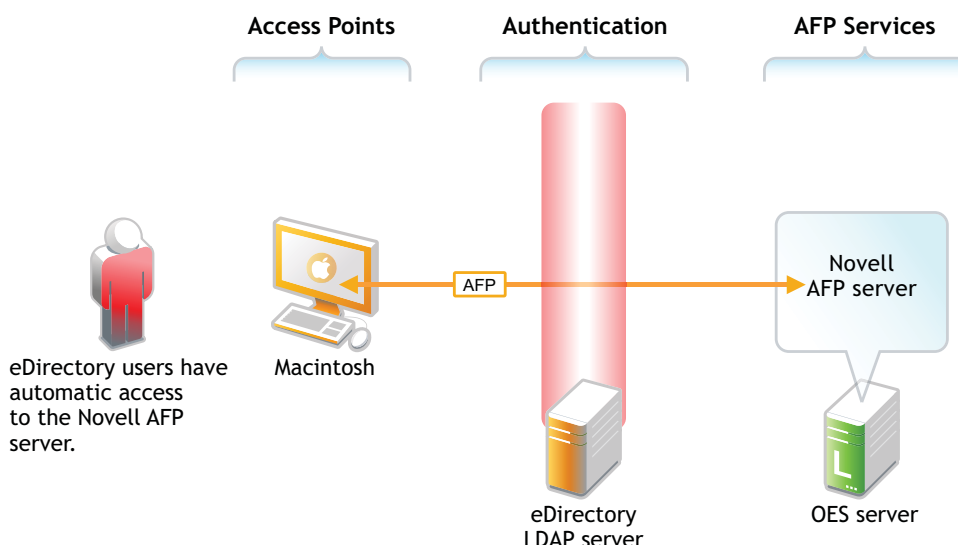


Table 18-4 AFP Access

Access Points	Authentication	AFP File Services
eDirectory users on Macintosh workstations have native access to NSS volumes on the OES server.	All file service access is controlled by LDAP-based authentication through the eDirectory LDAP server. Although shown separately, eDirectory could be installed on the OES server.	Of course, the same files can also be accessed through other OES file services (such as NetStorage) that connect to NSS volumes.

18.1.6 Novell CIFS

The Novell CIFS service lets users on Windows workstations access and store files on OES servers with NSS volumes without installing any additional software, such as the Novell Client (see [Figure 18-4](#)).

Figure 18-5 How Novell CIFS Works

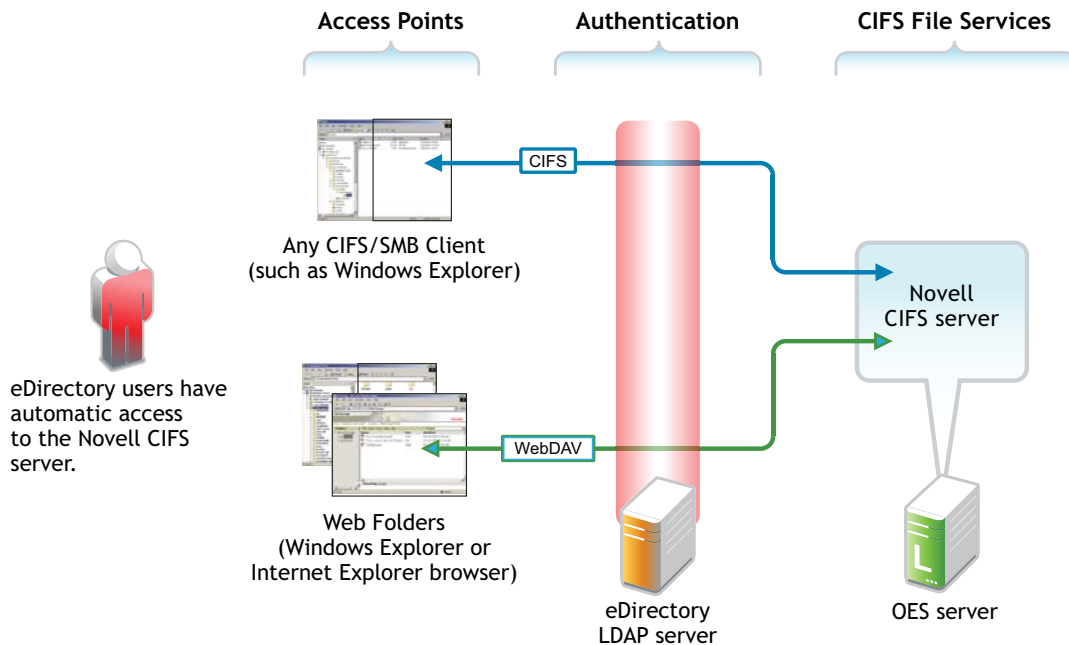


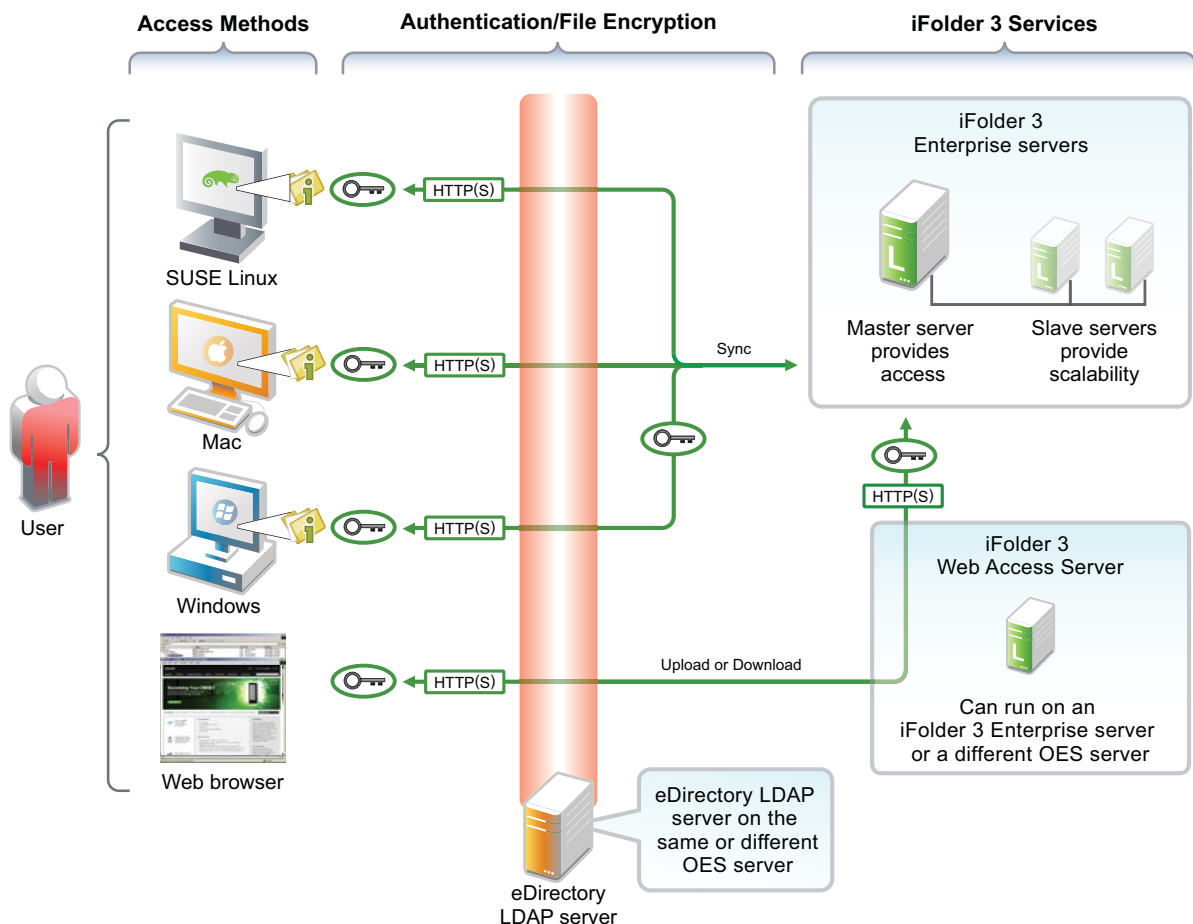
Table 18-5 CIFS Access

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

18.1.7 Novell iFolder 3.9.22

Novell iFolder 3.9.2 supports multiple iFolders per user, user-controlled sharing, and a centralized network server for file storage and secure distribution (see Figure 18-6).

Figure 18-6 How Novell iFolder Works



The following table explains the information illustrated in [Figure 18-6](#).

Table 18-6 *iFolder Access*

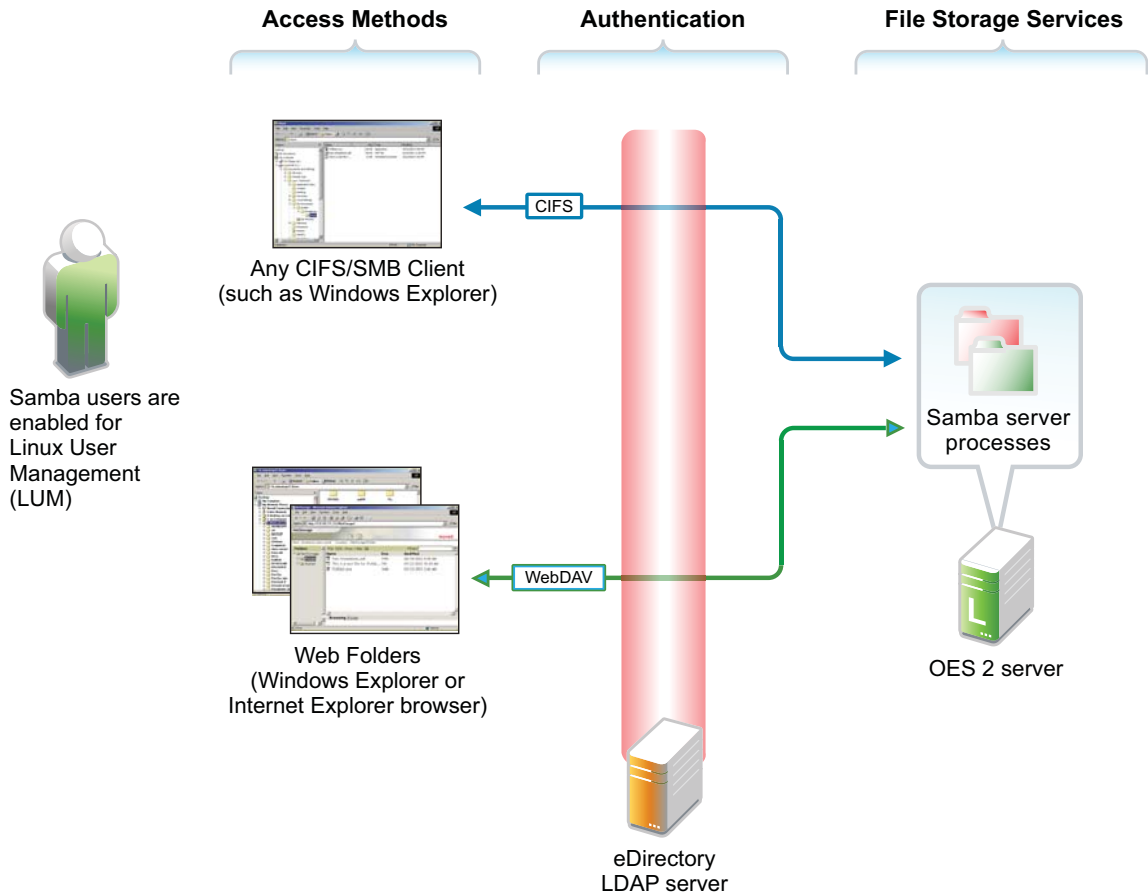
Access Methods	Authentication/File Encryption	Novell iFolder 3.9.2 Services
Linux, Mac, and Windows workstation users who have the Novell iFolder Client installed can access and modify their files in one or more workstation folders. Changes are automatically synchronized with the iFolder 3.9.2 Enterprise servers. A Web interface lets users access their files from any computer with an active network or Internet connection.	All file service access is controlled by LDAP- based authentication through the eDirectory LDAP server. Although shown separately, eDirectory could be installed on the OES server. Files can be encrypted for transport using SSL connections (HTTPS).	Slave servers can be added as needed, providing the ability to dynamically grow iFolder services without disrupting users. Local and network copies of each file are automatically synchronized by the Novell iFolder Client and Server pieces.

Additional overview information is available in the [Novell iFolder 3.9.2 Administration Guide](#).

18.1.8 Novell Samba

Novell Samba on an OES server provides Windows (CIFS and HTTP-WebDAV) access to files stored on the OES server (see [Figure 18-7](#)).

Figure 18-7 How Samba on OES Works



The following table explains the information illustrated in [Figure 18-7](#).

Table 18-7 Samba Access

Access Methods	Authentication	File Storage Services
eDirectory users on Windows workstations have two native Windows file access options (if their eDirectory accounts have been enabled for LUM and Samba): <ul style="list-style-type: none">♦ CIFS Client Access: Windows Explorer users can access and modify files on the Samba server just as they would on any workgroup server share.♦ Web Folder: Users can create Web Folders in Windows Explorer or Internet Explorer. Files on the OES server running Samba are accessed and maintained with the HTTP-WebDAV protocol.	All file service access is controlled by LDAP-based authentication through the eDirectory LDAP server. Although shown separately, eDirectory could be installed on the OES server.	Of course, the same files can also be accessed through other OES file services (such as NetStorage) that connect to Linux volumes.

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>).

18.2 Planning for File Services

Functional overviews of each file service product are included in [Section 18.1, "Overview of File Services,"](#) on page 249.

- ♦ [Section 18.2.1, "Deciding Which Components Match Your Needs,"](#) on page 259
- ♦ [Section 18.2.2, "Comparing Your CIFS File Service Options,"](#) on page 260
- ♦ [Section 18.2.3, "Planning Your File Services,"](#) on page 261

18.2.1 Deciding Which Components Match Your Needs

To decide which file service components to install, you should match service features listed in [Table 18-8](#) to your network's file service requirements.

Table 18-8 OES File Services Feature Breakdown

Service	Access Method Features	Back-End Storage Features	Security Features
NCP Server (NetWare Core Protocol)	Novell Client (NCP client)	♦ Any Linux volumes (including NSS) that are defined as NCP volumes	♦ eDirectory Authentication
NetStorage	<ul style="list-style-type: none"> ♦ Any supported browsers ♦ Personal Digital Assistant (PDA) ♦ Remote access (browser-based) ♦ Web Folders (on either an Internet Explorer browser or in Windows Explorer) ♦ Windows Explorer 	<ul style="list-style-type: none"> ♦ Linux POSIX volumes ♦ NCP volumes ♦ NSS volumes ♦ Samba (CIFS) servers ♦ Windows (CIFS) servers 	♦ Secure LDAP Authentication
Novell AFP	♦ Macintosh Chooser	♦ NSS volumes	♦ Secure LDAP Authentication
Novell CIFS	<ul style="list-style-type: none"> ♦ Any CIFS client ♦ Remote access (Web Folders in the Internet Explorer browser) ♦ Windows Explorer 	♦ NSS volumes	♦ Secure LDAP Authentication

Service	Access Method Features	Back-End Storage Features	Security Features
Novell iFolder 3.9.2	<ul style="list-style-type: none"> ♦ Linux File Managers ♦ Macintosh Chooser ♦ Offline access with file synchronization (between local and network copies) on reconnect ♦ Web browsers ♦ Windows Explorer <p>Except for Web browser access, each method above requires an installed iFolder client.</p>	<ul style="list-style-type: none"> ♦ Novell iFolder 3.9.2 Enterprise server file repository on OES server 	<ul style="list-style-type: none"> ♦ Files can be encrypted for transport through SSL (HTTPS). ♦ Secure LDAP Authentication
Novell Samba	<ul style="list-style-type: none"> ♦ Any CIFS client ♦ Remote access (Web Folders in the Internet Explorer browser) ♦ Windows Explorer 	<ul style="list-style-type: none"> ♦ Linux POSIX file system on OES server ♦ NSS volumes 	<ul style="list-style-type: none"> ♦ Secure LDAP Authentication

18.2.2 Comparing Your CIFS File Service Options

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

Table 18-9 Comparing OES 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>

Item	Novell CIFS	Novell Samba	Samba in DSfW
File system support	NSS is the only file system supported for this release.	It is recommended (but not required) that you create Samba shares on NSS data volumes. 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 server. For instructions on how to set up an NSS volume, see “ Managing NSS Volumes ” in the <i>OES 11 SP2: File Systems Management Guide</i> .	
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.	eDirectory users in the domain (eDirectory partition) are automatically Samba users and are enabled to access Samba shares. See “ Creating Users ” in the <i>OES 11 SP2: Domain Services for Windows Administration Guide</i> . Domain users are set up with the necessary UID and default group (DomainUsers) membership. Every additional eDirectory group created within the domain is automatically Linux-enabled.
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.

18.2.3 Planning Your File Services

- 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 3.9.2:** Suggestions for calculating the additional RAM you need are contained in “[Server Workload Considerations](#)” in the *Novell iFolder 3.9.2 Administration Guide*.
 - ♦ **Samba:** There are no additional RAM requirements.
- 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.
 - ♦ **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 3.9.2:** Suggestions for calculating the additional disk space you need are contained in "Server Workload Considerations" in the [Novell iFolder 3.9.2 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 sections of the OES 11 SP2 installation guide that are indicated in the following table.

Note your planning choices on your planning sheet.

File Service Product	Linux Planning References
NCP	"Novell NCP Server / Dynamic Storage Technology" in the OES 11 SP2: Installation Guide
NetStorage	"Novell NetStorage" in the OES 11 SP2: Installation Guide
Novell AFP	"Novell AFP Services" in the OES 11 SP2: Installation Guide
Novell CIFS	"Novell CIFS for Linux" in the OES 11 SP2: Installation Guide
Novell FTP	"Novell FTP Services" in the OES 11 SP2: Installation Guide
Novell iFolder 3.9.2	"Novell iFolder" in the OES 11 SP2: Installation Guide
Samba	"Novell Samba" in the OES 11 SP2: Installation Guide

18.3 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.

This section discusses migration of the following services:

- ♦ [Section 18.3.1, "Novell Client \(NCP\)," on page 263](#)
- ♦ [Section 18.3.2, "NetStorage," on page 263](#)
- ♦ [Section 18.3.3, "Novell AFP," on page 263](#)
- ♦ [Section 18.3.4, "Novell CIFS," on page 263](#)
- ♦ [Section 18.3.5, "Novell iFolder 3.9.2," on page 264](#)
- ♦ [Section 18.3.6, "Samba," on page 264](#)

18.3.1 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 7, see the [Novell Client 2 SP1 for Windows Administration Guide](#). For older Windows workstations, 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 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 servers, and other services commonly associated with Novell Client access.

For more information on NCP Server for Linux, see the [OES 11 SP2: NCP Server for Linux Administration Guide](#).

18.3.2 NetStorage

NetStorage provides Web access to the files and directories on OES 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 [OES 11 SP2: NetStorage Administration Guide for Linux](#).

18.3.3 Novell AFP

Novell AFP provides native AFP protocol access from Macintosh workstations to data on OES 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 11 SP2, see “[Migrating AFP to OES 11 SP2](#)” in the [OES 11 SP2: Migration Tool Administration Guide](#).

18.3.4 Novell CIFS

Novell CIFS provides native CIFS protocol access from Windows workstations to data on OES 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 11 SP2, see “[Migrating CIFS to OES 11 SP2](#)” in the [OES 11 SP2: Migration Tool Administration Guide](#).

18.3.5 Novell iFolder 3.9.2

iFolder 3.9.2 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 is only available on OES.

For information on migrating from iFolder 2 to iFolder 3.9.2, see “[Migrating iFolder 2.x](#)” in the *OES 11 SP2: Migration Tool Administration Guide*.

18.3.6 Samba

OES 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 11 SP2, see the *OES 11 SP2: Novell Samba Administration Guide*.

18.4 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 owner can see a directory’s contents. However, because of the differences in the NetWare Core Protocol (NCP) and POSIX file security models (see [Section 22.2.1, “Comparing the Linux and the Novell Trustee File Security Models,”](#) on page 295) that is not the case by default on POSIX file systems.

Fortunately, when you install Linux User Management (LUM) in OES, 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 18.4.1, “Managing Access Rights,”](#) on page 265
- ♦ [Section 18.4.2, “Providing a Private Work Directory,”](#) on page 266
- ♦ [Section 18.4.3, “Providing a Group Work Area,”](#) on page 266
- ♦ [Section 18.4.4, “Providing a Public Work Area,”](#) on page 267
- ♦ [Section 18.4.5, “Setting Up Rights Inheritance,”](#) on page 267

18.4.1 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 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 in Linux"](http://www.suse.com/documentation/sles11/book_security/data/cha_acls.html) (http://www.suse.com/documentation/sles11/book_security/data/cha_acls.html) in the *SLES 11 SP3: Security Guide* (<http://www.suse.com/documentation/sles11/index.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 server.

The Linux `chmod` command provides a very simple and fast way of adjusting directory and file access privileges for the three user types: owner, group, and other (all users). In its simplest form, the command uses three numbers, ranging from 0 through 7, to represent the rights for each of the three user types. The first number sets the rights for the owner, the second number sets the rights for the group, and the third number sets the rights for all others. Each number represents a single grouping of rights, as follows:

Number	Setting	Binary Representation
0	- - -	0 0 0
1	- - x	0 0 1
2	- w -	0 1 0
3	- w x	0 1 1
4	r - -	1 0 0
5	r - x	1 0 1
6	r w -	1 1 0
7	r w x	1 1 1

Those familiar with the binary number system find this method an easy way to remember what each number represents.

For example, the command `chmod 777 /home` would grant read, write and execute rights (7) to owner, group, and other for the `/home` directory, while `chmod 700 /home` would grant the three rights to only the directory owner, with group and other having no rights. `chmod 750 /home` would grant `rw` rights to the owner, `r-x` rights to the group, and no rights to other users.

For more information about the `chmod` command, see the `chmod` man page on your OES server.

18.4.2 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.

18.4.3 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 18.4.1, “Managing Access Rights,” on page 265.”](#)

18.4.4 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 (`rxw rxw rxw`) (`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 `rxw --- r-x`.

To provide a public work area on a Linux POSIX volume:

- 1 Use the `chown` command to assign all rights (`rxw`) 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 `rxw` 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 (`. rxw`). (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.

18.4.5 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 11 SP2: NCP Server for Linux Administration Guide*.

18.5 Novell FTP (Pure-FTPd) and OES 11 SP2

FTP file services on OES 11 SP2 servers are provided by Pure-FTPd, a free (BSD), secure, production-quality and standard-conformant FTP server. The OES implementation includes support for FTP gateway functionality as on NetWare and offers a level of integration between eDirectory and Pure-FTP that allows users to authenticate to eDirectory for FTP access to the server.

This section discusses the following topics:

- ♦ [Section 18.5.1, “Planning for Pure-FTPd,” on page 268](#)
- ♦ [Section 18.5.2, “Installing Pure-FTPd,” on page 268](#)
- ♦ [Section 18.5.3, “Home Directory Support in Pure-FTPd,” on page 268](#)
- ♦ [Section 18.5.4, “Configuring Pure-FTPd on an OES 11 SP2 Server,” on page 269](#)
- ♦ [Section 18.5.5, “Administering and Managing Pure-FTPd on an OES 11 SP2 Server,” on page 270](#)
- ♦ [Section 18.5.6, “Cluster Enabling Pure-FTPd in an OES 11 SP2 Environment,” on page 274](#)
- ♦ [Section 18.5.7, “Migrating Pure-FTPd From NetWare to Linux,” on page 275](#)
- ♦ [Section 18.5.8, “Troubleshooting Pure-FTPd from Novell,” on page 276](#)

18.5.1 Planning for Pure-FTPd

Before installing Pure-FTPd, make sure that users requiring FTP access are LUM-enabled and have access rights to the areas on the server they need to use.

18.5.2 Installing Pure-FTPd

To install Pure-FTPd, select the *Novell FTP Server* pattern in the OES 11 SP2 installation.

18.5.3 Home Directory Support in Pure-FTPd

The FTP server supports a home directory for users on local and remote NCP servers. The remote server can be an OES server. When the home directory is set for the user in eDirectory, the user is placed in the home directory on successful login to the Linux server.

Pure-FTPd supports three levels of home directory, default home directory, a user specific home directory on the local system, and a user specific home directory identified by the value set in eDirectory.

POSIX User Home Directory

The POSIX home directory is the directory that is available by default on POSIX file systems. The POSIX home directory is defined at the file system level and cannot be disabled.

DefaultHomeDirectory and eDirectory home directories can be disabled. If one or both of them are enabled, the following is used to establish the precedence:

- ♦ User specific home directory set in eDirectory
- ♦ Default home directory
- ♦ POSIX user home directory

User Specific Home Directory in eDirectory

An administrator can set the home directory for eDirectory users as part of the User object in eDirectory. On successful login to the FTP server, the user is placed in the home directory set in the user object. The User's home directory can exist either on the OES server that is hosting the FTP service or on any other OES server in the same tree.

A new `EnableRemoteHomeDirectory` option is now available to support this home directory. By default, this option is set to `NO` and the home directory set for the user in eDirectory is ignored.

To enable eDirectory based home directory support, you must set both `EnableRemoteHomeDirectory` and `remote_server` to `YES`. FTP will then read the user's home directory from eDirectory and mount it locally.

Default Home Directory

`DefaultHomeDirectory` indicates the path to the common home directory for all FTP users. On successful login to the Pure-FTPd, users are placed in the default home directory. The default home directory can be local or on a locally mounted NSS path or on a remote NCP Server. It can be either an NCP volume or an NSS volume and it can be configured by using the `DefaultHomeDirectory` and `DefaultHomeDirectoryServer` settings. If the home directory is on a remote server, use `DefaultHomeDirectoryServer`, and set it to the IP or DNS name of the remote NCP server. As with any NSS volume, the FTP client should have required rights over the NSS volume whether `DefaultHomeDirectory` is on a local or remote server or not.

The `DefaultHomeDirectoryServer` option is now available to differentiate whether `DefaultHomeDirectory` is on a local or remote server. By default, this option is set to `NO` so `DefaultHomeDirectory` points to a local path.

To set `DefaultHomeDirectory` to point to a remote NCP server with a DNS entry, you must specify the full path to the remote server, including the volume name. For example, `DefaultHomeDirectory /ftphome`. You must also set both `DefaultHomeDirectory` and `remote_server` to `YES`.

NOTE: If `DefaultHomeDirectory` path is a POSIX path (non NCP volume) then it is supported only on local FTP server and not on remote server. In that case `DefaultHomeDirectory` path should be `/home/commonpath` (any POSIX path) and `DefaultHomeDirectoryServer` should be Null or commented.

Backslash in Input Paths

Support for backslashes in input path is provided. Using FTP client on Windows, you can use backslash as separator in the path. `allow_backslash_in_path` option is now available to allow back slash in the path. By default the option is set to `NO`.

18.5.4 Configuring Pure-FTPd on an OES 11 SP2 Server

To configure the Pure-FTPd server on OES 11 SP2, edit the `/etc/pure-ftpd/pure-ftpd.conf` file.

NOTE: It is very strongly recommended that you read through the entire `/etc/pure-ftpd/pure-ftpd.conf` file and be familiar with the available parameters and settings.

For complete details, refer the `pure-ftpd` man page.

The following table lists the recommended configuration parameters for Pure-FTPd.

Table 18-10 Configuration Parameters

Parameter	Description	Default Value
DefaultHomeDirectory	Default home directory of the user.	
MaxClientsNumber	Maximum numbers of clients that can simultaneously access the server.	10
PassivePortRange	Port range for passive connection replies. Range must be a minimum of 2*MaxClientsNumber.	30000 30100
MaxClientsPerIP	Maximum number of sim clients with the same IP address	3
NoRename	Set to yes if you do not want the users to rename the files	yes no
remote_server	Enables remote server navigation for the FTP server ChrootEveryone parameter is required for remote_server to be enabled	yes
disallow_list_oes_server	Disables the <code>site slist</code> from listing the OES servers	yes
edir_ldap_port	LDAP port of the eDirectory server	389:0
AnonymousOnly	Enables authenticated connection to pure-ftp server	no
NoAnonymous	Disables anonymous connection	yes
ChrootEveryone	Allows the user to browse outside the home directory. This configuration is required for remote server navigation	no
DefaultHomeDirectoryServer	Allows to differentiate whether DefaultHomeDirectory is on local or remote server.	no
EnableRemoteHomeDirectory	Supports eDirectory based home directory.	no
allow_backslash_in_path	Allows Windows user to you use backslash as separator in the path.	

18.5.5 Administering and Managing Pure-FTPd on an OES 11 SP2 Server

- ♦ [“Starting Pure-FTPd” on page 271](#)
- ♦ [“Initializing Multiple Instances” on page 271](#)
- ♦ [“Unloading Specific Instances” on page 272](#)
- ♦ [“Pure-FTPd Remote Server Navigation” on page 272](#)

Starting Pure-FTPd

Start the Pure-FTPd server using the `rcpure-ftp` command.

Initializing Multiple Instances

Pure-FTPd is loaded by using a configuration file. Multiple instances of Pure-FTPd can be loaded using different configuration files.

By default, an instance of Pure-FTPd using `/etc/pure-ftp/pure-ftp.conf` file is loaded at the boot time by `init.d` script. For loading multiple instances, new configuration files need to be created.

To load a new instance of Pure-FTPd:

- 1 Create a new configuration file for each instance.

For example: Copy `/etc/pure-ftp/pure-ftp.conf` to a different location. Rename the file to `pure-ftp1.conf` and move it to `/etc/opt/novell/pure-ftp1.conf`.

- 2 Modify the following settings in the configuration file to avoid IP address or port conflicts between the instances:

- ♦ **PIDFile:** Points to the full path of the PID file created by the pure-ftp instance. PID file is used for unloading a particular instance of pure-ftp. Hence, ensure that the PID File path is unique for every instance.

For example: `/var/run/pure-ftp1.pid`, `/var/run/pure-ftp2.pid`.

- ♦ **Bind:** By default, pure-ftp binds to all the IP addresses on the system and listens to requests over port 21. Modify the settings of the bind such that all the pure-ftp instances bind to different IP addresses or port combinations.

also, modify the settings in the `/etc/pure-ftp/pure-ftp.conf` to avoid any IP address or port conflict from the second instance.

For example: If a system has two interfaces with two IP addresses 10.1.1.1 and 10.1.1.2, then the bind setting for two pure-ftp instances can be *Bind 10.1.1.1,21* and *Bind 10.1.1.2,21*.

- 3 Load the new instance using `/usr/sbin/pure-config.pl <Full path of the config file>`

For example: `/usr/sbin/pure-config.pl /etc/opt/novell/pureftpd-confs/pure-ftp1.conf` loads an instance using the config file `/etc/opt/novell/pureftpd-confs/pure-ftp1.conf`.

Verifying the Load of a New Instance

Use the following methods to verify that the new instance of pure-ftp is successfully loaded:

- ♦ The `ps -eaf | grep pure-ftp` command lists all the instances of pure-ftp loaded on the system.
- ♦ The PID file as specified using the `PIDFile` entry in the configuration file has been created.
- ♦ An FTP connection from the client to the server over the IP address being used by the pure-ftp instance can be created.

Unloading Specific Instances

A new script, `pure-ftp-stop.pl`, is added to unload an instance of `pure-ftpd` and all its child processes. The full path of the configuration file used to load the instance of `pure-ftpd` must be passed to the `pure-ftp-stop.pl` script.

For example: `/usr/sbin/pure-ftpd-stop.pl /etc/opt/novell/pureftpd-confs/pure-ftpd1.conf` unloads the instance of `pure-ftpd` that was loaded using `/etc/opt/novell/pureftpd-confs/pure-ftp1.conf`.

The PID file of the `pure-ftpd` instance is also used for unloading the `pure-ftpd` instance.

Verifying the Unload of a New Instance

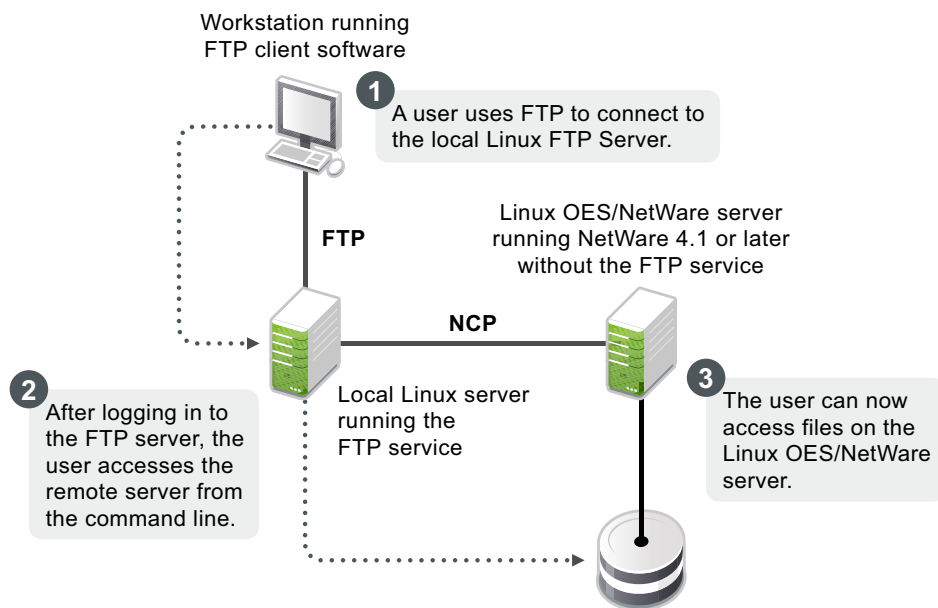
- The PID file specified using the `PIDFile` entry in the configuration file has been deleted.
- The number of instances displayed by `ps -eaf | grep pure-ftpd` is reduced.
- An FTP connection request to the server errors out.

Pure-FTPd Remote Server Navigation

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.

This section describes how to configure and use the Remote Server Navigation feature.

- [“Configuring Novell FTP” on page 273](#)
- [“Path Formats” on page 273](#)
- [“SITE Command” on page 274](#)
- [“Disable-ascii” on page 274](#)



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

Configuring Novell FTP

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

The configuration parameters for remote server navigation are as follows:

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

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

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

Path Formats

Table 18-11 *Linux FTP Server path formats*

Task	Command Format
Specifying the volume and directory path name	<code>//server_name/volume_name/directory_path</code>
Navigating to different volumes	<code>cd //server_name/volume_name</code>
Switching back to the home directory	<code>cd ~</code>
Switching to home directory of any user	<code>cd ~user_name</code>
Switching to the root of the server	<code>/root</code>

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

SITE Command

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

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 18-12](#) provides the `SITE` command along with the description:

Table 18-12 *Linux FTP SITE command*

Command	Description
<code>SLIST</code>	Lists all the OES servers within the eDirectory tree. Site list command accepts an eDirectory context in LDAP format. By default, site slist command lists all the NCP Servers in the entire tree. When context is passed to the command it lists all the NCP Servers within the context.

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

Disable-ascii

This command is to enable or disable ascii based file transfer. If this is set to YES, all the file transfers are done in a binary mode and the client command 'TYPE A' is ignored.

18.5.6 Cluster Enabling Pure-FTPd in an OES 11 SP2 Environment

You can configure Pure-FTPd server in active/active mode of Novell Cluster Services.

- ♦ [“Prerequisites” on page 274](#)
- ♦ [“Active/Active Mode” on page 274](#)

Prerequisites

- ♦ Novell Cluster Services is installed and setup.

For step-by-step information on setting up Novell Cluster Services, refer to [“Installing, Configuring, and Repairing Novell Cluster Services”](#) in the *“OES 11 SP2: Novell Cluster Services for Linux Administration Guide.”*

Active/Active Mode

In active/active cluster mode, multiple instances of FTP server runs on a single node cluster.

Pure-FTPd must be associated with a shared NSS volume and the DefaultHomeDirectory of users must be on the shared NSS volume.

Configuring Active/Active Mode

- 1 Install pure-ftpd on all the cluster nodes by selecting *Novell FTP* in the OES install. Upgrade pure-ftpd on all the nodes with the test RPM.
- 2 Enable hard links on the shared NSS volumes.
- 3 Create a [unique configuration file](#) for every FTP server to be associated with a shared NSS volume. Ensure that:

- ♦ The Bind setting in the configuration file is same as the IP Address of the virtual server created for the NSS pool.
- ♦ The PID file must be unique for each FTP instance running on the cluster.

- 4 Copy the configuration file to the shared volume to `/etc/opt/novell` on the shared volume. Copying the configuration file to the shared volume, the file is automatically moved across the nodes with the volume and is always available to the FTP Server.

For example: If the shared volume is FTPVol1, the path to copy the configuration file is `/media/nss/FTPVol1/etc/opt/novell/pure-ftpd`.

- 5 Configure all the FTP servers for DefaultHomeDirectory support. As NSS volume is shared, the DefaultHomeDirectory in the configuration file must be on the shared volume.

For example: If FTPVol1 is the shared volume attached to an FTP Server, DefaultHomeDirectory in the configuration file is `/media/nss/FTPVol1/FTPShare`.

- 6 Update the load and unload scripts of the cluster resource.

- ♦ **Load script:** Add the following command to load the FTP server with the shared volume:

```
/usr/sbin/pure-config.pl <Full Path to configuration file>
```

For example: If the shared volume is FTPVol1 and the Pure-FTP configuration file is `/etc/opt/novell/pure-ftpd/ftpvol1.conf` on FTPVol1, the pure-ftpd load command in the load script is `exit_on_error /usr/sbin/pure-config.pl /media/nss/FTPVol1/etc/opt/novell/pure-ftpd/ftpvol1.conf`.

- ♦ **Unload script:** Add the following command to unload the FTP server:

```
/usr/sbin/pure-ftpd-stop.pl <Full Path to configuration file>
```

Configuration file path must be same as the one passed to pure-config.pl in the load script.

NOTE: In iManager, load and unload the cluster resources. Pure-ftpd instances must be loaded along with the shared NSS volumes. During the migration process, the pure-ftpd instances alongwith the associated shared volumes are moved across the cluster nodes.

18.5.7 Migrating Pure-FTPd From NetWare to Linux

You can also migrate an existing FTP server configuration from a NetWare server to OES 11 SP2. For migration instructions and a brief FAQ, see “[Migrating FTP to OES 11 SP2](#)” in the [OES 11 SP2: Migration Tool Administration Guide](#).

18.5.8 Troubleshooting Pure-FTPd from Novell

Applying the OES 11 SP1 May 2014 Scheduled Maintenance Update Puts the novfsd daemon into an Unused State

FTP and other services require the novfsd daemon. Applying the May 2014 Scheduled Maintenance Update puts novfsd into an unused state.

To restore novfsd functionality, reboot the server.

If you are using Novell ZENworks for managing maintenance updates, after you apply the update, execute the following command at a terminal prompt:

```
/sbin/chkconfig --add novfsd
```

Then reboot the server.

After the server reboots, the daemon always runs irrespective of its previous state.

This issue does not exist if you upgrade to OES 11 SP2.

18.6 NCP Implementation and Maintenance

If you have installed the NCP server for OES, eDirectory/Novell Client users can access files on the OES 11 SP2 server with no additional configuration.

The implementation information in the following sections can help you get started with NCP on OES 11 SP2 servers.

- [Section 18.6.1, “The Default NCP Volume,” on page 276](#)
- [Section 18.6.2, “Creating NCP Home and Data Volume Pointers,” on page 276](#)
- [Section 18.6.3, “Assigning File Trustee Rights,” on page 277](#)
- [Section 18.6.4, “NCP Caveats,” on page 277](#)
- [Section 18.6.5, “NCP Maintenance,” on page 277](#)

18.6.1 The Default NCP Volume

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

18.6.2 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 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 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.

18.6.3 Assigning File Trustee Rights

You can use the same methods for assigning file trustee rights on NCP volumes on OES 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 11 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.)

18.6.4 NCP Caveats

Cross-protocol file locking (CPL) is enabled by default on all new servers with NCP installed. For more information, see [Section 3.9.6, “Cross-Protocol File Locking Might Need To Be Reconfigured if AFP or CIFS Is Functioning on an NCP Server,”](#) on page 94.

18.6.5 NCP Maintenance

Because NCP provides Novell Client access to files on NetWare and OES servers, the service is covered by maintenance tasks that apply to file systems on these servers. For information on maintaining file services, see “[storage, file systems, & databases](#) (http://www.novell.com/documentation/oes11/index.html#cat_stor-file-systems-databases)” in the online documentation.

18.7 NetStorage Implementation and Maintenance

The following sections are provided only as introductory information. For more information about using NetStorage, see the *OES 11 SP2: NetStorage Administration Guide for Linux*.

- ♦ [Section 18.7.1, “About Automatic Access and Storage Locations,”](#) on page 278
- ♦ [Section 18.7.2, “About SSH Storage Locations,”](#) on page 278
- ♦ [Section 18.7.3, “Assigning User and Group Access Rights,”](#) on page 278
- ♦ [Section 18.7.4, “Authenticating to Access Other Target Systems,”](#) on page 279
- ♦ [Section 18.7.5, “NetStorage Authentication Is Not Persistent by Default,”](#) on page 279
- ♦ [Section 18.7.6, “NetStorage Maintenance,”](#) on page 279

18.7.1 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.

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)

Administrators can create storage locations to storage on any of the target servers illustrated in [Figure 18-3 on page 253](#), including Dynamic Storage Technology (DST) volume pairs and Distributed File Services (DFS). For instructions on creating Storage Locations, see “[Creating a Storage Location Object](#)” in the *OES 11 SP2: NetStorage Administration Guide for Linux*.

18.7.2 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 11.5, “SSH Services on OES 11 SP2,” on page 155](#).

18.7.3 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 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 server, they must be enabled for LUM and Samba access on the OES server. For more information, see “[OES Services That Require LUM-Enabled Access](#)” on page 220.

IMPORTANT: The eDirectory usernames and passwords that are used to authenticate to the NetStorage (OES) server must match the usernames and passwords defined on the target systems.

18.7.4 Authenticating to Access Other Target Systems

The OES installation establishes a primary authentication domain (or context) 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 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. In contrast to the way it searches in the primary authentication domain, 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 11 SP2: NetStorage Administration Guide for Linux*.

18.7.5 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 11 SP2: NetStorage Administration Guide for Linux*.

18.7.6 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 11 SP2: NetStorage Administration Guide for Linux*.

18.8 Novell AFP Implementation and Maintenance

To use the Novell implementation of AFP file services on your OES 11 SP2 server, you must install the service by using the instructions in the *OES 11 SP2: Installation Guide* (for a new installation) or install it after the initial OES installation, as explained in [“Installing AFP after OES 11 SP2 Installation”](#) in the *OES 11 SP2: Novell AFP for Linux Administration Guide*.

- ♦ [Section 18.8.1, “Implementing Novell AFP File Services,” on page 280](#)
- ♦ [Section 18.8.2, “Maintaining Novell AFP File Services,” on page 280](#)

18.8.1 Implementing Novell AFP File Services

NOTE: If you are new to OES, we recommend the [OES 11 SP2: Getting Started with OES 11 and Virtualized NetWare](#) for an introduction to creating and working with eDirectory objects and OES file services, including Novell AFP.

All eDirectory users can access the AFP file services on an OES 11 SP2 server as they would any Macintosh server.

18.8.2 Maintaining Novell AFP File Services

Information on maintaining your AFP installation is found in the [OES 11 SP2: Novell AFP for Linux Administration Guide](#).

18.9 Novell CIFS Implementation and Maintenance

To use the Novell implementation of CIFS file services on your OES server, you must install the service by using the instructions in the [OES 11 SP2: Installation Guide](#) (for a new installation) or install it after the initial OES installation, as explained in “Installing CIFS after the OES 11 SP2 Installation” in the [OES 11 SP2: Novell CIFS for Linux Administration Guide](#).

- ♦ [Section 18.9.1, “Implementing Novell CIFS File Services,” on page 280](#)
- ♦ [Section 18.9.2, “Maintaining Novell CIFS File Services,” on page 280](#)

18.9.1 Implementing Novell CIFS File Services

NOTE: If you are new to OES, we recommend the [OES 11 SP2: Getting Started with OES 11 and Virtualized NetWare](#) for an introduction to creating and working with eDirectory objects and OES file services, including Novell CIFS.

All eDirectory users can access the CIFS file services on an OES 11 SP2 server as they would any Windows workgroup server.

For instructions on implementing Novell CIFS, see “Planning and Implementing CIFS” in the [OES 11 SP2: Novell CIFS for Linux Administration Guide](#).

18.9.2 Maintaining Novell CIFS File Services

Information on maintaining your CIFS installation is found in the [OES 11 SP2: Novell CIFS for Linux Administration Guide](#).

18.10 Novell iFolder 3.9.2 Implementation and Maintenance

The following implementation pointers are provided only as introductory information. To begin using Novell iFolder, see the [Novell iFolder 3.9.2 Administration Guide](#).

- ♦ [Section 18.10.1, “Managing Novell iFolder 3.9.2,” on page 281](#)
- ♦ [Section 18.10.2, “Configuring Novell iFolder 3.9.2 Servers,” on page 281](#)
- ♦ [Section 18.10.3, “Creating and Enabling Novell iFolder 3.9.2 Users,” on page 281](#)
- ♦ [Section 18.10.4, “Novell iFolder 3.9.2 Maintenance,” on page 281](#)

18.10.1 Managing Novell iFolder 3.9.2

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 3.9.2 Administration Guide](#).

18.10.2 Configuring Novell iFolder 3.9.2 Servers

Before you let users log in to the Novell iFolder 3.9.2 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 3.9.2 Administration Guide](#).

18.10.3 Creating and Enabling Novell iFolder 3.9.2 Users

To provide user access to Novell iFolder 3.9.2:

1. Provision eDirectory User objects for iFolder 3.9.2.
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 3.9.2 Administration Guide](#).

18.10.4 Novell iFolder 3.9.2 Maintenance

As the Novell iFolder service load increases, you might need to increase the server capacity or add additional servers. For help, see [“Installing and Configuring iFolder Services”](#) in the [Novell iFolder 3.9.2 Administration Guide](#).

18.11 Samba Implementation and Maintenance

To use the Novell implementation of Samba file services on your OES server, you must install the service by using the instructions in the [OES 11 SP2: Installation Guide](#) (for a new installation) or install it after the initial OES installation, as explained in “Installing Novell Samba for OES” in the [OES 11 SP2: Novell Samba Administration Guide](#).

- ♦ [Section 18.11.1, “Implementing Samba File Services,” on page 282](#)
- ♦ [Section 18.11.2, “Maintaining Samba File Services,” on page 282](#)

18.11.1 Implementing Samba File Services

All users whose accounts have been enabled for Samba access can access the OES server as they would any Windows server.

For instructions on implementing Samba, see “Installing Novell Samba for OES” in the [OES 11 SP2: Novell Samba Administration Guide](#).

18.11.2 Maintaining Samba File Services

Information on maintaining your Samba installation is found in the [OES 11 SP2: Novell Samba Administration Guide](#).

19 Print Services

Open Enterprise Server 11 SP2 includes Novell iPrint, a powerful and easy-to-implement printing solution that provides print-anywhere functionality to network users.

This section contains the following information:

- ♦ [Section 19.1, “Overview of Print Services,” on page 283](#)
- ♦ [Section 19.2, “Planning for Print Services,” on page 285](#)
- ♦ [Section 19.3, “Coexistence and Migration of Print Services,” on page 285](#)
- ♦ [Section 19.4, “Print Services Implementation Suggestions,” on page 286](#)
- ♦ [Section 19.5, “Print Services Maintenance Suggestions,” on page 287](#)

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 283](#)
- ♦ [Section 19.1.2, “iPrint Components,” on page 283](#)
- ♦ [Section 19.1.3, “iPrint Functionality,” on page 284](#)

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 285](#).

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:

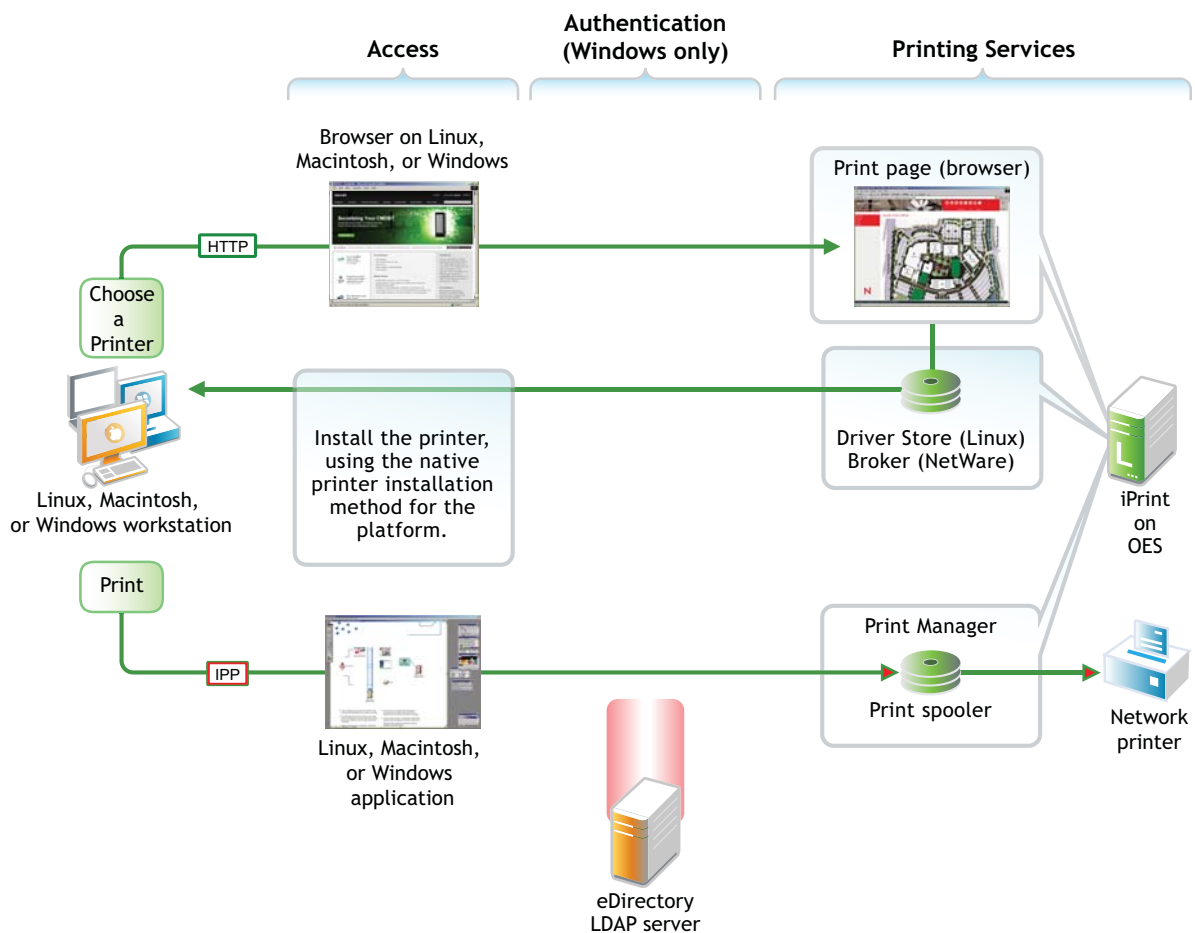
- ♦ **Print Driver Store:** This is a repository that stores the drivers on an OES server for your network printers. It is the first component you configure and is represented by an eDirectory object that you create. It corresponds to the Print Broker on NetWare.

- ♦ **Printer Drivers:** These are the platform-specific printer drivers and PostScript* Printer Description (PPD) files that are stored in the Driver Store 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 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. 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.

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
The iPrint Client must be installed on each workstation accessing iPrint services.	You can require authentication for Windows users if needed. The option to require authentication is not available for Linux and Macintosh users.	Users with the iPrint Client installed and access to the OES server can install printer drivers and print to iPrint printers.
A user needing to use a printer for the first time accesses the organization's print page on the Web.	Although shown separately, eDirectory could be installed on the OES server.	By default, iPrint generates a printer list for the printers hosted on the server.
When the user selects the target printer, its platform-specific driver is automatically installed and configured.		A customized Web page lets users browse to the target printer by using location lists and maps that you have previously created for the site where the printer is located.
After printer installation, users can print to the printer from any application.		

19.2 Planning for Print Services

We recommend that you record your decisions in planning notes for future reference.

Consider the following information as you plan your iPrint installation:

- ♦ 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 servers.
- ♦ To finish planning your iPrint installation, refer to the information in “Novell iPrint” in the [OES 11 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 installed with the SLES 11 packages, 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 11 SP2: iPrint Linux Administration Guide](#).

Migrating iPrint services from a NetWare server to an OES 11 SP2 server is supported by the OES 11 SP2 Migration Tool. For more information, see “Migrating iPrint to OES 11 SP2” in the [OES 11 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 11 SP2: iPrint Linux Administration Guide](#).

- ♦ [Section 19.4.1, “Initial Setup,” on page 286](#)
- ♦ [Section 19.4.2, “Implementation Caveats,” on page 287](#)
- ♦ [Section 19.4.3, “Other Implementation Tasks,” on page 287](#)

19.4.1 Initial Setup

After your OES server is installed, you must do the following to complete your iPrint installation:

- 1 Create a Driver Store to store the print drivers.

This eDirectory object stores the drivers for your network printers. Each Printer object you create for your network needs to reference a printer driver in Driver Store. 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 11 SP2: iPrint Linux Administration Guide](#)

- 2 Add a printer driver to the Driver Store for each printer/platform combination needed.

For example, If you have Windows XP, Windows 7, 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.

You add printer drivers to the store through iManager. For specific instructions, see “[Updating Printer Drivers](#)” in the [OES 11 SP2: iPrint 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 11 SP2: iPrint 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 11 SP2: iPrint 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 in a building with multiple floors or even at multiple sites, 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 11 SP2: iPrint 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 123.

19.4.3 Other Implementation Tasks

In addition to the tasks described in [Section 19.4.1, “Initial Setup,”](#) on page 286, there are additional tasks you might want or need to consider. To see a list of potential tasks, refer to the “[Print Services](#) (http://www.novell.com/documentation/oes11/index.html#cat_iprint)” 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 11 SP2: iPrint Linux Administration Guide*

For more information on iPrint and its functionality within OES, see the “[Print Services](#) (http://www.novell.com/documentation/oes11/index.html#cat_iprint)” links in the online documentation.

20 Search Engine (QuickFinder)

Open Enterprise Server 11 SP2 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.

When indexing a file system, the QuickFinder engine indexes only what the `wwwrun` user and the `www` group have rights to see.

For more information, see the topics in “[Search Engine \(http://www.novell.com/documentation/oes11/index.html#cat_quick-finder\)](http://www.novell.com/documentation/oes11/index.html#cat_quick-finder)” in the OES 11 SP2 online documentation or refer to the *OES 11 SP2: Novell QuickFinder Server 5.0 Administration Guide*.

21 Web Services

The Web and application services in Open Enterprise Server 11 SP2 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 *OES 11 SP2: Web Services and Applications Guide* and the topics in “Web Services (http://www.novell.com/documentation/oes11/oes11_toc/data/index-category.html#cat_web-services)” in the OES online documentation.

Apache

OES 11 includes Apache 2.2, the most popular Web server on the Internet.

For additional information, see the [Apache.org Web site \(http://httpd.apache.org/docs/2.2/\)](http://httpd.apache.org/docs/2.2/).

Tomcat

OES 11 includes Tomcat 6.0, which is used to run basic Java servlet and JavaServer Pages (JSP) applications.

For information, see the [Apache Tomcat 6.0 Web site \(http://tomcat.apache.org/tomcat-6.0-doc/index.html\)](http://tomcat.apache.org/tomcat-6.0-doc/index.html).

22 Security

This section contains the following topics:

- ♦ [Section 22.1, “Overview of OES Security Services,” on page 293](#)
- ♦ [Section 22.2, “Planning for Security,” on page 295](#)
- ♦ [Section 22.3, “Configuring and Administering Security,” on page 299](#)
- ♦ [Section 22.4, “Resolving Nessus Security Scan Issues,” on page 299](#)
- ♦ [Section 22.5, “Links to Product Security Considerations,” on page 305](#)
- ♦ [Section 22.6, “Links to Anti-Virus Partners,” on page 306](#)

22.1 Overview of OES Security Services

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

- ♦ [Section 22.1.1, “Application Security \(AppArmor\),” on page 293](#)
- ♦ [Section 22.1.2, “NSS Auditing Engine,” on page 293](#)
- ♦ [Section 22.1.3, “Encryption \(NICI\),” on page 294](#)
- ♦ [Section 22.1.4, “General Security Issues,” on page 295](#)

22.1.1 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).

22.1.2 NSS Auditing Engine

OES 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 \(http://download.novell.com/Download?buildid=yDnJELwauAo~\)](http://download.novell.com/Download?buildid=yDnJELwauAo~). 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

22.1.3 Encryption (NICI)

The Novell International Cryptography Infrastructure (NICI) is the cryptography service for NetIQ eDirectory, NetIQ Modular Authentication Services (NMAS), NetIQ Certificate Server, NetIQ 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 NCI Configuration Files

In the early days of NCI development, some NCI problems could be solved only by deleting the NCI 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 NCI problem.

No one should ever delete the [NCI configuration files](#) unless they are directly told to do so by a member of the NCI 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 NCI impossible.

More Information

For more information on how to use NCI, see the [Novell International Cryptographic Infrastructure \(NCI\) 2.7.6 Administration Guide](#).

22.1.4 General Security Issues

In addition to the information explained and referenced in this section, the OES online documentation contains links to “security issues” (http://www.novell.com/documentation/oes11/index.html#cat_security).

22.2 Planning for Security

This section discusses the following topics. For additional planning topics, see the [Security section in the OES online documentation](#) (http://www.novell.com/documentation/oes11/index.html#cat_security).

- ♦ [Section 22.2.1, “Comparing the Linux and the Novell Trustee File Security Models,” on page 295](#)
- ♦ [Section 22.2.2, “User Restrictions: Some OES Limitations,” on page 297](#)
- ♦ [Section 22.2.3, “Ports Used by OES 11 SP2,” on page 297](#)

22.2.1 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 22-1](#).

Table 22-1 *POSIX vs. NSS/NCP File Security Models*

Feature	POSIX / Linux	Novell Trustee Model on OES
Administrative principles	<p>Permissions are individually controlled and managed for each file and subdirectory.</p> <p>Because of the nature of the POSIX security model, users usually have read rights to most of the system.</p> <p>To make directories and files private, permissions must be removed.</p> <p>For more information on making existing directories private, see Section 18.4.2, “Providing a Private Work Directory,” on page 266.</p>	<p>Trustee assignments are made to directories and files and flow down from directories to everything below unless specifically reassigned.</p>
Default accessibility	<p>Users have permissions to see most of the file system.</p> <p>The contents of a few directories, such as the <code>/root</code> home directory, can only be viewed by the <code>root</code> user.</p> <p>Some system configuration files can be read by everyone, but the most critical files, such as <code>/etc/fstab</code>, can only be read and modified by <code>root</code>.</p>	<p>Users can see only the directories and files for which they are trustees (or members of a group that is a trustee).</p>
Home directories—an example of default accessibility	<p>By default, all users can see the names of directories and files in home directories.</p> <p>During LUM installation, you can specify that newly created home directories will be private.</p> <p>For more information on making existing home directories private, see Section 18.4.2, “Providing a Private Work Directory,” on page 266.</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>

Feature	POSIX / Linux	Novell Trustee Model on OES
Subdirectory and file visibility	<p>Permissions granted to a file or directory apply to only the file or directory. Users can't see parent directories along the path up to the root unless permissions are granted (by setting the UID, GID, and mode bits) for each parent.</p> <p>After permissions are granted, users can see the entire contents (subdirectories and files) of each directory in the path.</p>	When users are given a trustee assignment to a file or directory, they can automatically see each parent directory along the path up to the root. However, users can't see the contents of those directories, just the path to where they have rights.

When an NCP volume is created on a Linux POSIX or NSS volume, some of the behavior described above is modified. For more information, see the [OES 11 SP2: NCP Server for Linux Administration Guide](#), particularly the “NCP on Linux Security” section.

22.2.2 User Restrictions: Some OES 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 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 11.5, “SSH Services on OES 11 SP2,” on page 155](#).

For more information on Linux User Management, see [“Linux User Management: Access to Linux for eDirectory Users” on page 217](#). For more information on the services that can be PAM-enabled, see [Table 15-2 on page 220](#).

22.2.3 Ports Used by OES 11 SP2

The ports used by OES 11 SP2 services are listed in [Table 22-3](#).

Table 22-2 Open Enterprise Server Services and Ports

Service	Default Ports
Domain Services for Windows	<ul style="list-style-type: none"> ♦ 1636 (LDAPS) ♦ 1389 (LDAP) ♦ 88 (Kerberos TCP and UDP) ♦ 135 (RPC Endpoint Manager TCP and UDP) ♦ 1024 - 65535 (RPC Dynamic Assignments TCP) ♦ 3268 (Global Catalog LDAP TCP) ♦ 3269 (Global Catalog LDAP over SSL TCP) ♦ 123 (Network Time Protocol UDP) ♦ 137 (NetBIOS Name Service TCP and UDP) ♦ 138 (NetBIOS Datagram Service TCP and UDP) ♦ 139 (NetBIOS Session Service TCP and UDP) ♦ 8025 (Domain Service Daemon TCP) ♦ 445 (Microsoft-DS traffic TCP and UDP)
NetIQ eDirectory	<ul style="list-style-type: none"> ♦ 389 (LDAP) ♦ 636 (secure LDAP) <p>IMPORTANT: The scripts that manage the common proxy user require port 636 for secure LDAP communications.</p> <ul style="list-style-type: none"> ♦ 8028 (HTTP for iMonitor) ♦ 8030 (secure HTTP for iMonitor) ♦ 524 (NCP)
iManager	<ul style="list-style-type: none"> ♦ 80 (HTTP) ♦ 443 (secure HTTP)
iPrint	<ul style="list-style-type: none"> ♦ 80 (HTTP) ♦ 443 (secure HTTP) ♦ 631 (IPP)
Novell AFP	<ul style="list-style-type: none"> ♦ 548
Novell Archive and Version Services	<ul style="list-style-type: none"> ♦ 26029
Novell CIFS	<ul style="list-style-type: none"> ♦ 636 (secure LDAP) <p>IMPORTANT: The scripts that manage the common proxy user require port 636 for secure LDAP communications.</p>
Novell DHCP	<ul style="list-style-type: none"> ♦ 67
Novell DNS	<ul style="list-style-type: none"> ♦ 953 (secure HTTP) ♦ 53 (TCP) ♦ 53 (UDP)
Novell FTP	<ul style="list-style-type: none"> ♦ 21

Service	Default Ports
Novell Information Portal	<ul style="list-style-type: none"> ♦ 80 (HTTP) ♦ 443 (secure HTTP)
Novell NetWare Core Protocol (NCP)	♦ 524
Novell Remote Manager	<ul style="list-style-type: none"> ♦ 8008 (HTTP) ♦ 8009 (secure HTTP)
SFCB	<ul style="list-style-type: none"> ♦ 5988 (HTTP) ♦ 5989 (secure HTTP)
QuickFinder	<ul style="list-style-type: none"> ♦ 80 (HTTP) ♦ 443 (secure HTTP)
Samba	<ul style="list-style-type: none"> ♦ 139 (Netbios) ♦ 445 (Microsoft-ds)
Secure Shell	♦ 22
Storage Management Services (Backup)	♦ 40193 (smdr daemon)
Time Synchronization	♦ 123 (Network Time Protocol UDP)

22.3 Configuring and Administering Security

For a list of configuration and administration topics, see the [Security section in the OES online documentation](http://www.novell.com/documentation/oes11/index.html#cat_security) (http://www.novell.com/documentation/oes11/index.html#cat_security).

22.4 Resolving Nessus Security Scan Issues

- ♦ [Section 22.4.1, “Port dns \(53/tcp\): DNS Server Zone Transfer Information Disclosure \(AXFR\),” on page 300](#)
- ♦ [Section 22.4.2, “Port dns \(53/udp\): DNS Server Recursive Query Cache Poisoning Weakness,” on page 300](#)
- ♦ [Section 22.4.3, “Port dns \(53/udp\): DNS Server Cache Snooping Remote Information Disclosure,” on page 301](#)
- ♦ [Section 22.4.4, “Port dns \(53/udp\): Multiple Vendor DNS Query ID Field Prediction Cache Poisoning,” on page 301](#)
- ♦ [Section 22.4.5, “Port ftp \(21/tcp\): Anonymous FTP Enabled,” on page 301](#)
- ♦ [Section 22.4.6, “Port ftp \(21/tcp\): Multiple Vendor Embedded FTP Service Any Username Authentication Bypass,” on page 302](#)
- ♦ [Section 22.4.7, “Port ldap: LDAP NULL BASE Search Access,” on page 302](#)
- ♦ [Section 22.4.8, “Port smb \(139/tcp\) : Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials,” on page 302](#)
- ♦ [Section 22.4.9, “Port ssh \(22/tcp\): SSH Protocol Version 1 Session Key Retrieval,” on page 303](#)
- ♦ [Section 22.4.10, “Port \(524/tcp\): Novell NetWare ncp Service NDS Object Enumeration,” on page 303](#)

- [Section 22.4.11, “Port www \(443/tcp\): SSL Certificate signed with an unknown Certificate Authority,” on page 303](#)
- [Section 22.4.12, “Port www \(443/tcp\): SSL Version 2 \(v2\) Protocol Detection,” on page 304](#)
- [Section 22.4.13, “Port www \(tcp\): SSL Weak Cipher Suites Supported,” on page 304](#)
- [Section 22.4.14, “Port www \(tcp\): SSL Medium Strength Cipher Suites Supported,” on page 304](#)

22.4.1 Port dns (53/tcp): DNS Server Zone Transfer Information Disclosure (AXFR)

Nessus Plug in: 10595

Port: DNS service on port 53

Synopsis: The remote name server permits zone transfers.

Description: A zone transfer lets a remote attacker instantly populate a list of potential targets. In addition, companies often use a naming convention that can give hints as to a server’s primary application, for example, proxy.example.com, payroll.example.com, b2b.example.com, etc.

Information like this is of great use to an attacker, who may use it to gain information about the topology of the network and spot new targets.

Resolution: Limit DNS zone transfers to only the servers that need the information. The Security Chapter for DNS includes the required information to restrict zones, allow-update and queries and the security factors. See “[Security Considerations for DNS](#)” in the *OES 11 SP2: Novell DNS/DHCP Services for Linux Administration Guide*.

22.4.2 Port dns (53/udp): DNS Server Recursive Query Cache Poisoning Weakness

Nessus Plug in: 10539

Port: DNS on port 53

Synopsis: The remote name server allows recursive queries to be performed by the host running nsssd.

Description: It is possible to query the remote name server for third party names.

If this is your internal name server, then the attack vector may be limited to employees or guest access if allowed. If you are probing a remote name server, then it allows anyone to use it to resolve third party names, such as www.novell.com. This allows attackers to perform cache poisoning attacks against this name server.

If the host allows these recursive queries via UDP, then the host can be used to “bounce” denial-of-service attacks against another network or system.

Resolution: Restrict recursive queries to the hosts that should use this name server, such as those of the LAN connected to it.

The Security Chapter for Novell DNS includes the required information to restrict zones, allow-update and queries and the security factors. See “[Security Considerations for DNS](#)” in the *OES 11 SP2: Novell DNS/DHCP Services for Linux Administration Guide*.

22.4.3 Port dns (53/udp): DNS Server Cache Snooping Remote Information Disclosure

Nessus Plug in: 12217

Port: DNS on port 53

Synopsis: The remote DNS server is vulnerable to cache snooping attacks.

Description: The remote DNS server responds to queries for third-party domains that do not have the recursion bit set. This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

NOTE: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants, and potential users on a guest network or WiFi connection if supported.

Resolution: The Security Chapter for Novell DNS includes the required information to restrict zones, allow-update and queries and the security factors. See [“Security Considerations for DNS”](#) in the *OES 11 SP2: Novell DNS/DHCP Services for Linux Administration Guide*.

22.4.4 Port dns (53/udp): Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Nessus Plug in: 33447

Port: DNS on Port 53

Synopsis: The remote name resolver (or the server it uses upstream) may be vulnerable to DNS cache poisoning.

Description: The remote DNS resolver does not use random ports when making queries to third party DNS servers. This problem might be exploited by an attacker to poison the remote DNS server more easily, and therefore divert legitimate traffic to arbitrary sites.

Resolution: Nessus might report this if the OES server is configured to use a non-OES DNS server that has the above vulnerability. Configure DNS with Novell-DNS instead of the third-party server that is vulnerable.

22.4.5 Port ftp (21/tcp): Anonymous FTP Enabled

Nessus Plug in: 10079

Port: FTP service on port 21

Synopsis: Anonymous logins are allowed on the remote FTP server.

Description: This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials. This allows a user to access any files made available on the FTP server.

Resolution: Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure sensitive content is not available.

22.4.6 Port ftp (21/tcp): Multiple Vendor Embedded FTP Service Any Username Authentication Bypass

Nessus Plug in: 10990

Port: FTP service on port 21

Synopsis: A random username and password can be used to authenticate to the remote FTP server.

Description: The FTP server running on the remote host can be accessed using a random username and password. Nessus has enabled some countermeasures to prevent other plug ins from reporting vulnerabilities incorrectly because of this.

Resolution: Contact the FTP server's documentation so that the service handles authentication requests properly.

22.4.7 Port ldap: LDAP NULL BASE Search Access

Nessus Plugin: 10722

Port: LDAP on 389, DSfW LDAPS on 1636, msft-gc on 3268

Synopsis: The remote LDAP server may disclose sensitive information.

Description: The remote LDAP server supports search requests with a null, or empty, base object. This allows information to be retrieved without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous user may be able to query your LDAP server using a tool such as LdapMiner.

NOTE: There are valid reasons to allow queries with a null base. For example, it is required in version 3 of the LDAP protocol to provide access to the root DSA-Specific Entry (DSE), with information about the supported naming context, authentication types, and the like. It also means that legitimate users can find information in the directory without any a prior knowledge of its structure.

For these reasons, this finding may be a false-positive.

Resolution: If the remote LDAP server supports a version of the LDAP protocol before v3, consider whether to disable NULL BASE queries on your LDAP server LDAP NULL BASE search access might be required by many OES services.

For more details see, [TID 7000737 \(http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7000737\)](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7000737).

22.4.8 Port smb (139/tcp) : Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials

Nessus Plug in : 56210

Synopsis: It is possible to obtain the host SID for the remote host, without credentials.

Description: By emulating the call to LsaQueryInformationPolicy(), it is possible to obtain the host SID (Security Identifier), without credentials. The host SID can then be used to get the list of local users.

Resolution: Novell-Cifs sends a dummy response with an SID value of 0. Therefore, this is not a security vulnerability.

22.4.9 Port ssh (22/tcp): SSH Protocol Version 1 Session Key Retrieval

Nessus Plug in: 10882

Port: SSH service on port 22

Synopsis: The remote service offers an insecure cryptographic protocol.

Description: The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol. These protocols are not completely cryptographically safe, so they should not be used.

Resolution: Disable compatibility with SSH 1.x.

22.4.10 Port (524/tcp): Novell NetWare ncp Service NDS Object Enumeration

Nessus Plug in: 10988

Port: NCP server on port 524

Synopsis: Remote directory server leaks information.

Description: This host is a Novell NetWare (eDirectory) server, and has browse rights on the PUBLIC object. It is possible to enumerate all NDS objects, including users, with crafted queries. An attacker can use this to gain information about this host.

Resolution: This feature is required by many OES services for their normal operation.

If this is an external system, block Internet access to port 524.

22.4.11 Port www (443/tcp): SSL Certificate signed with an unknown Certificate Authority

Nessus Plug in: 51192

Port: Apache (443), LDAPS (636), DSfW LDAPS (1636), msft-gc-ssl (3269), wbem (5989), NRM (8009), iMonitor (8030)

Synopsis: The SSL certificate for this service is signed by an unknown certificate authority.

Description: The X.509 certificate of the remote host is not signed by a known public certificate authority. If the remote host is a public host in production, this nullifies the use of SSL because anyone could establish a man-in-the-middle attack against the remote host.

Resolution: Purchase or generate a proper certificate for this service. For more information about generating certificates using the NetIQ Certificate Server, see [“Using eDirectory Certificates with External Applications”](#) in the [NetIQ Certificate Server Administration Guide](#).

22.4.12 Port www (443/tcp): SSL Version 2 (v2) Protocol Detection

Nessus Plug in: 20007

Port: Apache port www (443)

Synopsis: The remote service encrypts traffic using a protocol with known weaknesses.

Description: The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

Resolution: Consult the Apache documentation to disable SSL 2.0 and use SSL3.0 or TLS 1.0 instead.

22.4.13 Port www (tcp): SSL Weak Cipher Suites Supported

Nessus Plug in: 26928

Port: Apache (443), NRM (8009), LDAPS (636), DSfW LDAPS (1636), msft-gc-ssl (3269)

Synopsis: The remote service supports the use of weak SSL ciphers.

Description: The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

NOTE: This is considerably easier to exploit if the attacker is on the same physical network.

Resolution:

- 1 Change the weak SSLCipherSuite setting for Apache in the `/etc/apache2/vhosts.d/vhost-ssl.conf` file from:

```
SSLCipherSuite
```

```
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

```
to
```

```
SSLCipherSuite
```

```
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:!MEDIUM:!LOW:+SSLv2:!EXP:!eNULL
```

- 2 Restart Apache by entering the following at the terminal prompt:

```
rcapache2 restart
```

22.4.14 Port www (tcp): SSL Medium Strength Cipher Suites Supported

Nessus Plug in: 42873

Port: Apache (443), NRM (8009), LDAPS (636), DSfW LDAPS (1636), msft-gc-ssl (3269)

Synopsis: The remote service supports the use of medium strength SSL ciphers.

Description: The remote host supports the use of SSL ciphers that offer medium-strength encryption (key lengths at least 56 bits and less than 112 bits).

NOTE: This is considerably easier to exploit if the attacker is on the same physical network.

Resolution: Open the `/etc/opt/novell/httpstkd.conf` file in a text editor, then do the following:

- 1 Find the following section.

```
;;;;;;;;;;;;;
;   Cipher strength determines the bit strength for the SSL key
;   that is required to access Novell Remote Manager(NRM) .
;   The default will be all
;
;   If you modify the setting it will be necessary to restart NRM.
;
;   Options: all, low, medium, high
;
;   all - allows any negotiated encryption level.
;   low - allows less than 56-bit encryption
;   medium - allows 56-bit up to 112-bit encryption
;   high - allows 112-bit or greater encryption
;
;   Example:
;   cipher high
;
;
;
;;;;;;;;;;;;;
cipher all
```

- 2 Change cipher all to cipher high.
- 3 Save the file.
- 4 Restart httpstkd by entering `rcnovell-httpstkd restart` at a terminal prompt.

22.5 Links to Product Security Considerations

The following product documentation contains additional security information:

Table 22-3 Security Consideration Links

Product/Technology	Security Considerations Section Link
AppArmor	Novell AppArmor Administration Guide (http://www.novell.com/documentation/apparmor/apparmor201_sp10_admin/data/book_apparmor_admin.html)
Archive and Version Services	“Security Considerations for Archive and Version Services” in the OES 11 SP2: Novell Archive and Version Services Administration Guide
Domain Services for Windows	OES 11 SP2: Novell Domain Services for Windows Security Guide
Dynamic Storage Technology	“Security Considerations” in the OES 11 SP2: Dynamic Storage Technology Administration Guide
eDirectory	“Security Considerations” in the NetIQ eDirectory 8.8 SP8 Administration Guide
File Systems	OES 11 SP2: File Systems Management Guide (information throughout the guide)

Product/Technology	Security Considerations Section Link
Identity Manager 4.0.2	"Security Best Practices" in the Identity Manager 4.0.2 Documentation (http://www.netiq.com/documentation/idm402/index.html)
iPrint for OES	"Setting Up a Secure Printing Environment" in the OES 11 SP2: iPrint Linux Administration Guide
Linux User Management	"Security Considerations" in the OES 11 SP2: Novell Linux User Management Administration Guide
Novell AFP	"Security Guidelines for AFP" in the OES 11 SP2: Novell AFP for Linux Administration Guide
Novell CIFS	"Security Guidelines for CIFS" in the OES 11 SP2: Novell CIFS for Linux Administration Guide.
Novell Client for Windows 7	"Security Considerations" in the Novell Client 2 SP1 for Windows Administration Guide
Novell Client for Windows XP/2003	"Managing File Security and Passwords" in the Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide
Novell Client for Linux	"Managing File Security" in the Novell Client 2.0 SP3 for Linux Administration Guide
Novell Remote Manager for OES	"Security Considerations" in the OES 11 SP2: Novell Remote Manager Administration Guide
Novell Storage Services	"Securing Access to NSS Volumes, Directories, and Files" and "Security Considerations" in the OES 11 SP2: NSS File System Administration Guide for Linux
Novell iFolder 3.9.2	Novell iFolder 3.9.2 Security Administration Guide
OES 11 SP2 Installation	"Security Considerations" in the OES 11 SP2: Installation Guide
OES 11 SP2 Migration Tools	"Security Considerations for Data Migration" in the OES 11 SP2: Migration Tool Administration Guide
QuickFinder	"Security Considerations for QuickFinder Server" in the QuickFinder Server 5.0 Administration Guide
SuSEfirewall2	"Masquerading and Firewalls" (http://www.suse.com/documentation/sles11/book_security/data/cha_security_firewall.html) in the SLES 11 SP3 Security Guide (http://www.suse.com/documentation/sles11/book_security/data/book_security.html)

22.6 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).

23 Certificate Management

By default, all SUSE Linux Enterprise Server (SLES) 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

- ♦ 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 11 includes solutions that address each of these issues at no additional expense.

This section discusses the certificate management enhancements available in OES and how simple and straightforward it is to utilize them.

- ♦ [Section 23.1, “Overview,” on page 307](#)
- ♦ [Section 23.2, “Setting Up Certificate Management,” on page 309](#)
- ♦ [Section 23.3, “If You Don’t Want to Use eDirectory Certificates,” on page 312](#)

23.1 Overview

The following sections outline how OES lets you automate certificate management for OES and all HTTPS services:

- ♦ [Section 23.1.1, “SLES Default Certificates,” on page 307](#)
- ♦ [Section 23.1.2, “OES Certificate Management,” on page 308](#)
- ♦ [Section 23.1.3, “Multiple Trees Sharing a Common Root,” on page 309](#)

23.1.1 SLES Default Certificates

By default, HTTPS services on SLES 11 SP3 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 services, such as Apache, OpenWBEM, and Novell Remote Manager, are also configured to use these certificates.

23.1.2 OES Certificate Management

OES enhances certificate management as follows:

- ♦ [“Installation of eDirectory Certificates” on page 308](#)
- ♦ [“What Is Installed Where” on page 308](#)
- ♦ [“NetIQ Certificate Server” on page 309](#)
- ♦ [“Server Self-Provisioning” on page 309](#)
- ♦ [“PKI Health Check” on page 309](#)

Installation of eDirectory Certificates

As you install eDirectory and OES, 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 23-1 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 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 applications, are configured to point to the files in this directory.</p> <p>Only root and some specific groups can read the files in this directory.</p>
<code>/etc/opt/novell/certs</code>	<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>

NetIQ Certificate Server

The component that generates eDirectory keys and certificates is the NetIQ Certificate Server.

This certificate server provides public key cryptography services that are natively integrated into NetIQ eDirectory. You can use the server to 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 NetIQ Certificate Server, see the [NetIQ Certificate Server 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 [NetIQ Certificate Server 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 [NetIQ Certificate Server Administration Guide](#).

23.1.3 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 [NetIQ Certificate Server Administration Guide](#).

23.2 Setting Up Certificate Management

Use the information in the following sections to help you set up certificate management as you install OES.

- ♦ [Section 23.2.1, “Setting Up Automatic Certificate Maintenance,” on page 310](#)
- ♦ [Section 23.2.2, “Eliminating Browser Certificate Errors,” on page 310](#)

23.2.1 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 *NetIQ Certificate Server > 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 309](#).

IMPORTANT: If you enable Server Self-Provisioning in an OES 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.

23.2.2 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 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 310](#)
- ♦ [“Importing the CA Certificate into Mozilla Firefox on Linux” on page 311](#)
- ♦ [“Importing the CA Certificate into Mozilla Firefox on Windows” on page 311](#)
- ♦ [“Importing the CA Certificate into Internet Explorer” on page 311](#)

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 *NetIQ 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 310](#) 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 *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 310](#) 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

- 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 310](#), 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.

23.3 If You Don’t Want to Use eDirectory Certificates

For most organizations, the eDirectory certificate solution in OES 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.

A Adding Services to OES Servers

You can add services to OES servers after they are installed.

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

To add OES services to an OES 11 SP2 server, follow the instructions in “[Installing or Configuring OES 11 SP2 on an Existing Server](#)” in the *OES 11 SP2: Installation Guide*.

B Changing an OES 11 SP2 Server's IP Address

The instructions in this section let you change the IP address assigned to an OES 11 SP2 server and the services it hosts.

- ♦ [Section B.1, "Caveats and Disclaimers," on page 315](#)
- ♦ [Section B.2, "Prerequisites," on page 315](#)
- ♦ [Section B.3, "Changing the Server's Address Configuration," on page 316](#)
- ♦ [Section B.4, "Reconfiguring the OES Services," on page 316](#)
- ♦ [Section B.5, "Repairing the eDirectory Certificates," on page 317](#)
- ♦ [Section B.6, "Completing the Server Reconfiguration," on page 317](#)
- ♦ [Section B.7, "Modifying a Cluster," on page 321](#)
- ♦ [Section B.8, "Reconfiguring Services on Other Servers That Point to This Server," on page 321](#)

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 315](#)
- ♦ [Section B.2.2, "iPrint," on page 316](#)
- ♦ [Section B.2.3, "Clustering," on page 316](#)

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 11 SP2: iPrint 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 “[IP Address Requirements](#)” in the *OES 11 SP2: Novell Cluster Services 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 Copy the `ipchange.sh` script file found in `/opt/novell/migration/sbin/serveridswap/scripts/ipchange/nonplugin/` on any OES 11 SP2 server, to the `root (/)` partition of the OES 11 SP2 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 315](#) 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 315](#), 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 316](#).

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 ipchange.sh  
./ipchange.sh oldip newip oldmasterip newmasterip yes
```

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. In the script these are referred to as Remote edir/ldap addresses.

IMPORTANT: By default, the master eDirectory address (the eDirectory server specified at installation) 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 *NetIQ 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 317](#)
- ♦ [Section B.6.2, "DHCP," on page 318](#)
- ♦ [Section B.6.3, "DSfW," on page 318](#)
- ♦ [Section B.6.4, "iFolder," on page 320](#)
- ♦ [Section B.6.5, "iPrint," on page 321](#)
- ♦ [Section B.6.6, "NetStorage," on page 321](#)

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 11 SP2: Novell QuickFinder Server 5.0 Administration Guide*.

- 2 Regenerate the QuickFinder™ index by completing the instructions in see “[Creating Indexes](#)” in the *OES 11 SP2: Novell QuickFinder Server 5.0 Administration Guide*.

B.6.2 DHCP

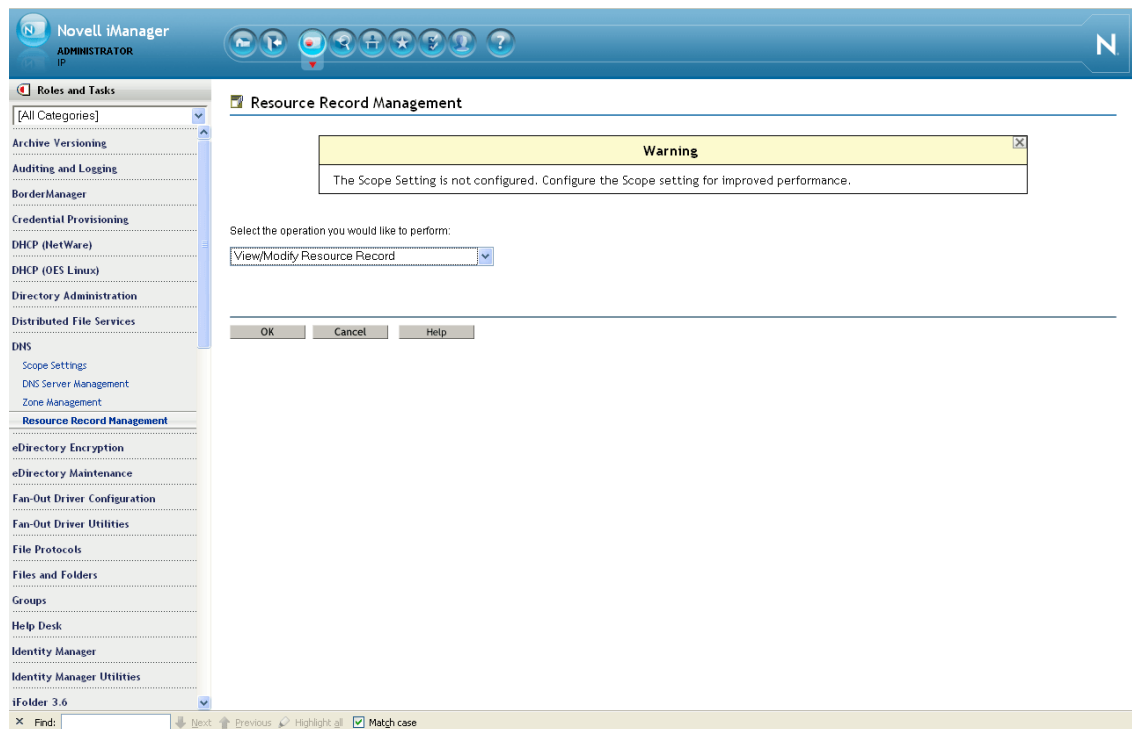
- 1 Make sure the DHCP configuration in eDirectory has a subnet declared for the new IP address.

For instructions, see “[Administering and Managing DHCP](#)” in the *OES 11 SP2: Novell DNS/DHCP Services for Linux Administration Guide*.

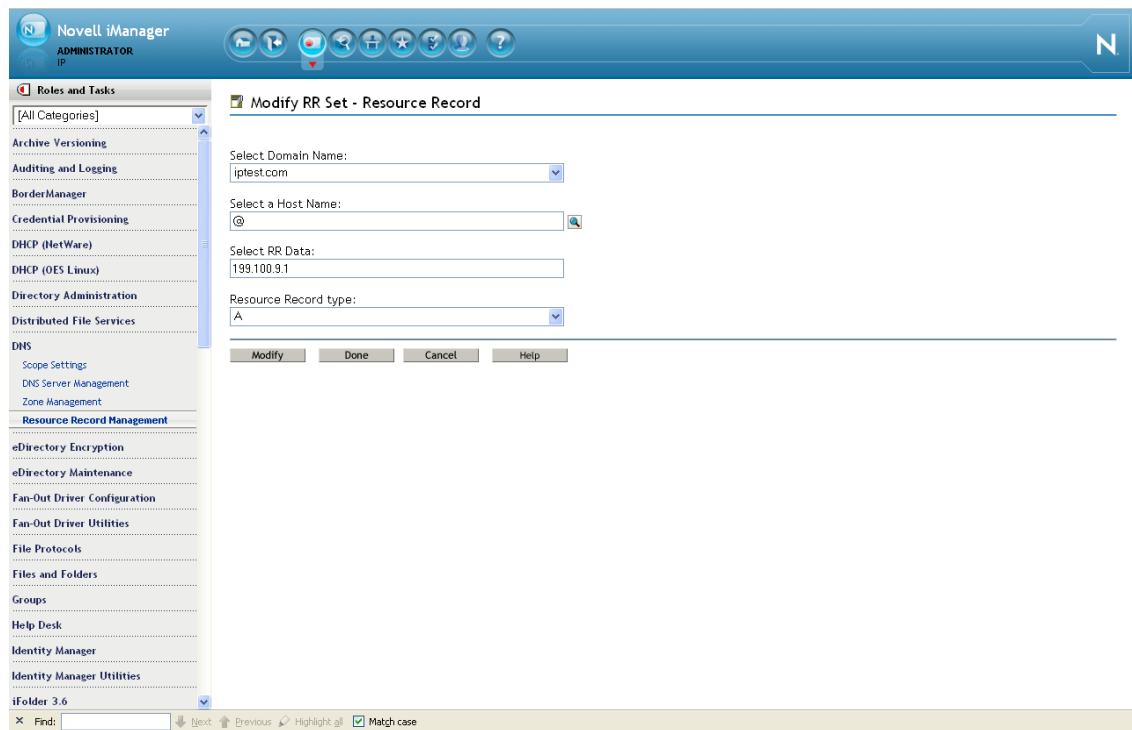
B.6.3 DSfW

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

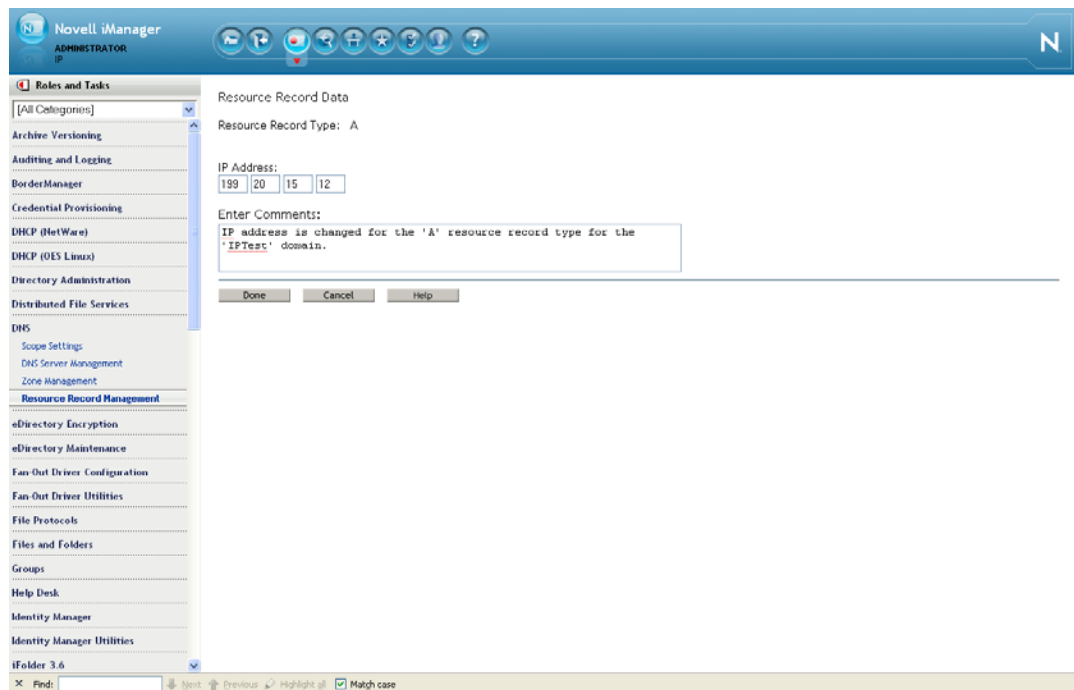
- 1 Open *iManager* > *DNS* > *Resource Record Management*. Select *View and Modify Resource Record* from the drop-down list, then click *OK* to open the Modify Resource Record window.



- 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).



- 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_arpa.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_arpa.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 iFolder

See “[Changing The IP Address For iFolder Services](#)” in the *Novell iFolder 3.9.2 Administration Guide*.

B.6.5 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 11 SP2: iPrint Linux Administration Guide*.

B.6.6 NetStorage

- 1 At a terminal prompt, enter the following commands:
`/opt/novell/xtier/bin/xsrfcfig -D`
`/opt/novell/xtier/bin/xsrfcfig -d newip -c AuthenticationContext`
where *newip* is the new IP address used throughout this section and *AuthenticationContext* is the eDirectory context for NetStorage users. NetStorage searches the eDirectory tree down from this container. If you want NetStorage to search the entire eDirectory tree, specify the root context.
`rcnovell-xregd restart`
`rcnovell-xsrzd restart`
`rcapache2 restart`

B.7 Modifying a Cluster

If the server is running Novell Cluster Services™, complete the instructions in “[Modifying the Cluster Configuration Information](#)” in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide*.

B.8 Reconfiguring Services on Other Servers That Point to This Server

If you have services on other servers that point to the old IP address for this server, be sure to reconfigure those services to point to the new IP address.

C Updating/Patching OES 11 SP2 Servers

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

For instructions on setting up the update channel for each OES 11 SP2 server and running the patch process, see “[Updating \(Patching\) an OES 11 SP2 Server](#)” in the *[OES 11 SP2: Installation Guide](#)*.

D Quick Reference to OES User Services

Use [Table D-1](#) as a quick reference for providing your network users with instructions for accessing each OES service.

Table D-1 OES User Services Quick Reference

services	Access Method or URL	Notes
iPrint	<code>http://server_ip_address_or_dns_name/ipp</code> <code>https://server_ip_address_or_dns_name:443/ipp</code>	
NetStorage	For browser access, use: <code>http: or https://server_ip_or_dns/netstorage</code> For WebDAV access, use: <code>http: or https://server_ip_or_dns/oneNet/NetStorage</code>	The WebDAV URL is case sensitive.
Novell Client	1. Install the Novell Client on a supported Windows workstation. 2. Log in to eDirectory. 3. Access NCP volumes on NetWare or Linux that you have the appropriate file trustee rights to.	
Novell AFP	In the Chooser, click Go and browse to the server.	
Novell CIFS	Map a network drive in Windows Explorer. Create a Web Folder in Internet Explorer.	
Novell iFolder 3.x Web Access server	<code>https://server_ip_address_or_dns_name/ifolder</code>	"ifolder" is the default name, but this can be customized by the administrator.
Novell Remote Manager	<code>http://server_ip_address_or_dns_name:8008</code>	Any LUM-enabled user can see their directories and files on OES servers.
Samba	Map a network drive in Windows Explorer. Create a Web Folder in Internet Explorer.	

E OES 11 SP2 Browser Support

As a general rule, Open Enterprise Server 11 SP2 management tools support the following browsers as they are available on the workstation platforms listed in [“Client/Workstation OS Support” on page 329](#):

- ♦ Mozilla Firefox 64-bit (latest 32- and 64-bit versions) on Windows, Macintosh, and Linux
- ♦ Microsoft Internet Explorer 8 (latest version) on Windows
- ♦ Microsoft Internet Explorer 9 (runs only on Window 7 SP1 or Windows 7 plus patches)
- ♦ Apple Safari (latest version) on Macintosh
- ♦ Google Chrome v14.x (latest version)

[Table E-1](#) provides service-specific links and information about browser support in OES.

Table E-1 *Browser Support in OES*

Management Tool	Supported Browser Information Link
iManager 2.7	<ul style="list-style-type: none">♦ “Using a Supported Web Browser” in the <i>NetIQ® iManager Administration Guide</i> <p>There are rendering differences for some iManager plug-ins between Internet Explorer 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">♦ “System Requirements” in “Using NetIQ iMonitor” in the <i>NetIQ eDirectory 8.8 SP8 Administration Guide</i>
IP Address Manager (NetWare)	Same as Novell Remote Manager
iPrint	<ul style="list-style-type: none">♦ “Supported Browsers for iPrint” in the <i>OES 11 SP2: iPrint Linux Administration Guide</i>
Novell iFolder 3.9.2	<ul style="list-style-type: none">♦ “Web Browser” in the <i>Novell iFolder 3.9.2 Administration Guide</i>
Novell Remote Manager	<ul style="list-style-type: none">♦ “System Requirements” in the <i>OES 11 SP2: Novell Remote Manager Administration Guide</i>♦ “System Requirements” in the <i>NW 6.5 SP8: Novell Remote Manager Administration Guide</i>
OpenSSH Manager (NetWare)	<ul style="list-style-type: none">♦ “Added Functionality” in the <i>NW 6.5 SP8: OpenSSH Administration Guide</i>
QuickFinder Server Manager	<ul style="list-style-type: none">♦ “Managing QuickFinder Server” in the <i>OES 11 SP2: Novell QuickFinder Server 5.0 Administration Guide</i>

Management Tool	Supported Browser Information Link
TCP/IP Configuration (NetWare)	Same as Novell Remote Manager

F Client/Workstation OS Support

As a general rule, Open Enterprise Server 11 SP2 services can be accessed and administered from workstations running the following operating systems:

- ♦ SUSE Linux Enterprise Desktop 10 SP4 (32- and 64-bit)
- ♦ SUSE Linux Enterprise Desktop 11 SP1 (32- and 64-bit)
- ♦ SUSE Linux Enterprise Desktop 11 SP2 (32- and 64-bit)
- ♦ Microsoft Windows XP SP3 (32-bit) (in extended support)
- ♦ Microsoft Windows Vista Business SP2 (32- and 64-bit)
- ♦ Microsoft Windows Vista Home Basic SP1 (32- and 64-bit) (iPrint and iFolder clients; non-administrative only)
- ♦ Microsoft Windows Vista Ultimate SP2 (32- and 64-bit)
- ♦ Microsoft Windows 7 SP1 Home Premium latest release (32- and 64-bit) (iPrint and iFolder clients; non-administrative only)
- ♦ Microsoft Windows 7 SP1 Ultimate latest release (32- and 64-bit)
- ♦ Microsoft Windows 7 SP1 Professional latest release (32- and 64-bit)
- ♦ Macintosh OS X 10.6.7 Snow Leopard (Intel) (32- and 64-bit) (non-administrative only)
- ♦ Macintosh OS X 10.7 Lion (Intel) (32- and 64-bit) (non-administrative, 10.6 feature level only) (DHX2 authentication requires enablement in Novell AFP. See “[Security and Rights](#)” in the *OES 11 SP2: Novell AFP for Linux Administration Guide*)
- ♦ Windows 2008 R2 Server (iPrint, DSfW, Novell Client) (32- and 64-bit) (non-administrative only)

For specific information on a given service, consult the service documentation.

G OES 11 SP2 Service Scripts

Novell Open Enterprise Server 11 SP2 services rely on specific service scripts located in `/etc/init.d`. The scripts used by OES 11 SP2, some of which are standard Linux scripts, are listed in [Table G-1](#).

IMPORTANT: For managing OES 11 SP2 services, we strongly recommend using the browser-based tools outlined in [Section 11.1, “Overview of Management Interfaces and Services,” on page 143](#). 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 G-1 OES Service Scripts in `/etc/init.d`

Services Associated with Scripts	Script Name	Notes
Apache Web server	apache2	The rcapache2 symbolic link, which is by default part of the path, can be used to start, stop, and restart the Apache Web Server, rather than referencing the init script directly.
Archive and Version Services	novell-ark	This lets you to start, stop, restart and display the status of the Archive and Version Service.
CASA	micasad	This is the CASA daemon.
Distributed File Services	novell-dfs	This lets you start and stop the VLDB service.
DNS (NetIQ eDirectory enhanced)	novell-named	This works in connection with <code>named</code> to provide NetIQ eDirectory DNS services.
DNS (SUSE Linux Enterprise Server 11 base)	named	This is the SLES 11 DNS service daemon.
Dynamic Storage Technology	novell-shadowfs	This script starts and stops the shadowfs daemon and the kernel module fuse.
eDirectory	ndsd	This lets you start and stop eDirectory. It executes the <code>/usr/sbin/ndsd</code> binary.
eDirectory SNMP support	ndssnmppsa	This lets you start and stop the NDS subagent.
eDirectory LDAP support	nldap	This lets you load and unload the LDAP library that NetIQ eDirectory uses to provide LDAP support. It is not actually a service.
FTP	pure-ftpd	This is used by the Novell FTP Pattern.

Services Associated with Scripts	Script Name	Notes
iPrint	cups	These scripts are required by iPrint
	novell-idsd	<p>cups lets you to start and stop the cupsd daemon that provides spooling and printing functionality for local and remote printers and is always required, even if printers are broadcasted ("Browsing") into (sub)nets.</p> <p>novell-ipsmd lets you to start and stop the ipsmd daemon that manages printers that are assigned under a Print Manager.</p> <p>novell-idsd lets you to start and stop the idsd daemon that manages drivers that are assigned under a Driver Store.</p>
	novell-ipsmd	
Linux User Management	namcd	<p>These daemons are required by Linux User Management and work together to ensure good performance.</p> <p>The namcd daemon caches user and group names and IDs from eDirectory, speeding subsequent lookups of cached users and groups.</p> <p>The nscd daemon caches host names and addresses.</p>
	nscd	
Logging	syslog	This is used for logging by many OES services.
Novell AFP	novell-afptcpd	This script starts and stops the afptcpd daemon, which is the Novell AFP service daemon
Novell AFP	avahi-daemon	This is used by AFPtcpd to advertise itself.
Novell CIFS	novell-cifs	This script starts and stops the cifsd daemon, which is the Novell CIFS service daemon
NetStorage (actually XTier)	novell-xregd	<p>NetStorage runs inside the novell-xsrvd XTier Web Services daemon, and also utilizes Tomcat services for certain other functions.</p> <p>novell-xregd is the init script for starting and stopping XTier's registry daemon. It is part of the novell-xtier-base RPM and is enabled by default for run levels 2, 3, and 5.</p> <p>novell-xsrvd is the init script for starting and stopping XTier's Web services daemon. It is also part of the novell-xtier-web RPM and is enabled for run levels 2, 3, and 5.</p>
	novell-xsrvd	
Novell Cluster Services (NCS)	adminfs	This is used for NCS through iManager and the command line interface.

Services Associated with Scripts	Script Name	Notes
Novell Cluster Services (NCS)	novell-ncs	<p>NCS uses some shell scripts and utilities that come with the heartbeat package. For example, NCS uses a binary called send_arp to send out ARP packets when a secondary address is bound.</p> <p>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 (chkconfig heartbeat off) when NCS is loaded on the server.</p>
Novell Remote Manager	novell-httpstk	<p>This script runs by default on every OES 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 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.
NSS Auditing	novell-vigil	This is the NSS auditing daemon.
NTP	ntp	This is the SLES 11 Network Time Protocol daemon.
Patching	novell-zmd	This is the GUI patch updater daemon.
QuickFinder	novell-tomcat6-32bit	This script sets up the Tomcat included with SLES 11 specifically to run the QuickFinder service.
Samba	nmb	This is the Samba NetBIOS naming daemon.
Samba CIFS support	smb	This script runs the Samba daemon.
SFCB CIMOM	sfcibd	<p>This is used to start the SFCB CIMOM daemon, which is an integral part of the iManager plug-ins for LUM, Samba, NSS, SMS, and NCS. AFP, CIFS, iPrint, and NRM also use SFCB.</p> <p>Novell Remote Manager on OES gets its server health information from CIMOM.</p>

Services Associated with Scripts	Script Name	Notes
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-tomcat6	This script sets up the Tomcat included with SLES 11 specifically for OES services, such as the Welcome pages.
Zypper	zypper	This is the Zypper command line daemon.

H System User and Group Management in OES 11 SP2

This section discusses the users and groups that are used by Open Enterprise Server. Administrative users are discussed in [Appendix I, “Administrative Users in OES 11 SP2,” on page 361](#).

- ♦ [Section H.1, “About System Users and Groups,” on page 335](#)
- ♦ [Section H.2, “Understanding Proxy Users,” on page 337](#)
- ♦ [Section H.3, “Common Proxy User,” on page 342](#)
- ♦ [Section H.4, “Planning Your Proxy Users,” on page 346](#)
- ♦ [Section H.5, “Implementing Your Proxy User Plan,” on page 355](#)
- ♦ [Section H.6, “Proxy Users and Domain Services for Windows,” on page 357](#)
- ♦ [Section H.7, “System Users,” on page 357](#)
- ♦ [Section H.8, “System Groups,” on page 358](#)
- ♦ [Section H.9, “Auditing System Users,” on page 360](#)

H.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 H.1.1, “Types of OES System Users and Groups,” on page 335](#)
- ♦ [Section H.1.2, “OES System Users and Groups by Name,” on page 336](#)

H.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 H-1](#).

Table H-1 Types of System Users and Groups with Examples

System User or Group Type	Purpose	Examples
Proxy User	Perform very specific service-related functions, such as <ul style="list-style-type: none"> ♦ Retrieving passwords and service attributes ♦ Writing Service information in eDirectory. ♦ Providing a user ID (uid) that the associated service daemon uses to run. 	<ul style="list-style-type: none"> ♦ <i>cifsProxyUser-servername</i> ♦ <i>LUM_Proxy_user</i>
System Group	<ul style="list-style-type: none"> ♦ Facilitate the management of system users ♦ Provide access rights to service data on the server or in the eDirectory tree. 	<ul style="list-style-type: none"> ♦ DHCP ♦ DNSDHCP
System User	The daemons associated with the respective services run as these users.	<ul style="list-style-type: none"> ♦ <i>wwwrun</i> ♦ <i>iprint</i>

H.1.2 OES System Users and Groups by Name

[Table H-2](#) lists the users and groups that OES services depend on and use.

Table H-2 System User and Groups Listing

System User or Group	Object Type	Associated Service
<i>AfpProxyUser-servername</i>	Proxy User	AFP
(Archive Versioning Proxy)	Proxy User	Archive and Versioning Services
The install admin is always assigned.		
<i>arkuser</i>	System User	Archive and Versioning Services
<i>CifsProxyUser-servername</i>	Proxy User	CIFS
<i>cluster_name_MGT_GRP.context</i>	System Group	NCS
<i>DHCP LDAP Proxy</i>	Proxy User	DHCP
<i>dhcpd</i>	System User	DHCP
<i>DHCPGroup</i>	System Group	DHCP
<i>DNS Proxy</i>	Proxy User	DNS
<i>DNSDHCP-GROUP</i>	System Group	DNS
<i>iFolderProxy</i>	Proxy User	iFolder 3
<i>iprint</i>	System User	iPrint

System User or Group	Object Type	Associated Service
lprint (POSIX)	System Group	iPrint
lprintgrp (eDirectory)		
<i>LUM proxy</i> (optional)	Proxy User	Linux User Management
named	System User	DNS
<i>NetStorage Proxy</i>	Proxy User	NetStorage
novell_nobody	System User	CIMOM
novell_nogroup	System Group	CIMOM
novlxregd	System User	XTier
novlxsvd	System User	XTier
novlxtier	System Group	XTier
OESCommonProxy_ <i>hostname</i>	System User	AFP, CIFS, DNS, DHCP, iFolder, NetStorage, Clustering (NCS), Linux User Management (optional)
<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 Tomcat QuickFinder
wwwrun	System User	Apache

H.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 H.2.1, “What Are Proxy Users?,” on page 338](#)
- ♦ [Section H.2.2, “Why Are Proxy Users Needed on OES?,” on page 338](#)
- ♦ [Section H.2.3, “Which Services Require Proxy Users and Why?,” on page 338](#)
- ♦ [Section H.2.4, “What Rights Do Proxy Users Have?,” on page 340](#)

H.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 338](#)). 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 AFP, DNS/DHCP, 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.

H.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.

H.2.3 Which Services Require Proxy Users and Why?

The following services utilize a proxy user.

Table H-3 Proxy Users Functions Listed by Service

Associated Service	Example Proxy User Name	Services That the User Provides
AFP	OESCommonProxy_ <i>hostname</i>	Retrieves AFP user information.
	Or	
	AfpProxyUser- <i>servername</i>	
Archive Versioning	admin	The service runs as this user.
	The install admin is always specified.	

Associated Service	Example Proxy User Name	Services That the User Provides
CIFS	OESCommonProxy_ <i>hostname</i> Or CifsProxyUser- <i>servername</i>	Retrieves CIFS user information.
Clustering (NCS)	OESCommonProxy_ <i>hostname</i> Or installing admin user	The clustering administrator and the proxy user can be two separate users. For more information, see “ OES Common Proxy User ” in the OES 11 SP2: Novell Cluster Services for Linux Administration Guide .
DHCP	OESCommonProxy_ <i>hostname</i> Or DHCP_LDAP_Proxy	Lets the service access DHCP objects in eDirectory.
DNS	OESCommonProxy_ <i>hostname</i> Or DNS_Proxy	Lets the service access DNS objects in eDirectory.
iFolder 3	OESCommonProxy_ <i>hostname</i> Or iFolderProxy IMPORTANT: The Common Proxy user cannot be used if iFolder is running on a cluster node.	Connects to the eDirectory server and retrieves the following information: <ul style="list-style-type: none"> ♦ modifytimestamp ♦ cn ♦ mail ♦ sn ♦ GUID ♦ givenName ♦ member
Linux User Management	OESCommonProxy_ <i>hostname</i> Or <i>LUM_proxy</i>	Searches the tree for LUM users.
NetStorage	OESCommonProxy_ <i>hostname</i> Or <i>NetStorage_Proxy</i>	Performs LDAP searches for users logging into NetStorage.
NSS	<i>server_name</i> admin	Reads user objects and maintains the volume, pool, and other storage system objects. 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.
Samba (Novell)	<i>server_name</i> -SambaProxy	Searches the LDAP tree (eDirectory) for Samba users.

H.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 H-4](#).

Table H-4 Proxy Users Rights

Associated Service	Example Proxy User Name	Default Rights Granted
AFP	AfpProxyUser- <i>servername</i>	♦ This proxy user has Compare and Read rights to the specified AFP user search context.
Archive Versioning	<i>Archive Versioning Proxy</i>	♦ This user has Read and Write rights to the archived volume.
CIFS	CifsProxyUser- <i>servername</i>	♦ This proxy user has Compare and Read rights to the specified CIFS user search context.
Clustering (NCS)	OESCommonProxy_ <i>hostname</i> Or installing admin user	♦ The proxy user has rights (granted through membership in the NCS_Management group) to communicate with eDirectory on behalf of the clustering service.

Associated Service	Example Proxy User Name	Default Rights Granted
DHCP	DHCP_LDAP_Proxy	<ul style="list-style-type: none"> No rights are assigned directly, but membership in the DHCPGroup, which does have assigned rights, provides the rights it needs.
DNS	DNS_Proxy	<ul style="list-style-type: none"> No rights are assigned directly, but membership in the DNS-DHCPGroup, which does have assigned rights, provides the rights it needs.
iFolder 3	iFolderProxy	<ul style="list-style-type: none"> Additional eDirectory rights include: [Entry Rights] Browse LDAP ACL representation: 1#subtree#iFolderProxy# [All Attributes Rights] Read, Compare LDAP ACL representation: 3#subtree#iFolderProxy#
Linux User Management	LUM_proxy	<ul style="list-style-type: none"> If created, this proxy user has Search rights on Unix Config & Unix Workstation Objects.
NetStorage	NetStorage_Proxy	<ul style="list-style-type: none"> Additional eDirectory rights: [Entry Rights] Browse LDAP ACL representation: 1#subtree#NetStorage_Proxy# [All Attributes Rights] Read, Compare LDAP ACL representation: 3#subtree#NetStorage_Proxy#
NSS	server_nameadmin	<ul style="list-style-type: none"> Additional eDirectory rights: Supervisor right to the container it was created in.

Associated Service	Example Proxy User Name	Default Rights Granted
Samba (Novell)	<i>server_name</i> -SambaProxy	<ul style="list-style-type: none"> ♦ The Universal Password policy associated with the Samba users grants this proxy user the right to retrieve user passwords. ♦ Additional eDirectory rights: <ul style="list-style-type: none"> Rights to itself – Supervisor attribute right Rights to the OU where it is located All Attribute rights – Read Write Entry rights – Browse Create samba* – Create Read Write

H.3 Common Proxy User

- ♦ [Section H.3.1, “Common Proxy User FAQ,” on page 342](#)
- ♦ [Section H.3.2, “Managing Common Proxy Users,” on page 345](#)

H.3.1 Common Proxy User FAQ

- ♦ [“Why Would I Want to Specify Common Proxy Users?” on page 342](#)
- ♦ [“Why Was a Proxy User Added to Novell Cluster Services?” on page 343](#)
- ♦ [“Which Services Can and Cannot Leverage the Common Proxy User?” on page 343](#)
- ♦ [“Can a Common Proxy User Service Multiple Servers?” on page 344](#)
- ♦ [“Can I Change the Common Proxy User Name and Context?” on page 344](#)
- ♦ [“Can I Assign the Common Proxy User After Services Are Installed?” on page 344](#)
- ♦ [“What About Upgraded Servers Using a Common Proxy?” on page 344](#)
- ♦ [“Are There Important Limitations to Keep in Mind?” on page 344](#)

Why Would I Want to Specify Common Proxy Users?

The implementation of a common proxy user in OES 11 SP2 addresses the following administrative needs:

- ♦ **Limit the Number of Proxy Users:** By default, the number of proxy users in an eDirectory tree can quickly become quite large. And even though proxy users don't consume user license connections, many administrators are disconcerted by the sheer number of objects to manage and track.

Common proxy users reduce the default number of proxy users from one per service to basically one per OES 11 SP2 server.

- ♦ **Accommodate Password Security Policies:** Many organizations have security policies that require periodic password changes. Some administrators are overwhelmed by having to manually track all proxy users, change their passwords, and restart the affected services after every change.

Common proxy users have their passwords automatically generated by default and changed at whatever interval is required. Services are restarted as needed with no manual intervention required.

- ♦ **Prevent Password Expiration:** When proxy user passwords expire, OES 11 SP2 services are interrupted, leading to network user frustration and administrator headaches.

Automatic password management for common proxy users ensures that services are never disrupted because of an expired password.

Why Was a Proxy User Added to Novell Cluster Services?

In OES 2 SP3 and later, the eDirectory communication functionality that was previously performed by the designated NCS administrator, has been separated out so that it can now be performed by a system user if so desired.

This aligns NCS functionality with other OES services that use proxy (system) users for similar functions. For more information, see [“OES Common Proxy User”](#) in the *OES 11 SP2: Novell Cluster Services for Linux Administration Guide*.

Which Services Can and Cannot Leverage the Common Proxy User?

- ♦ [“Services That Can Leverage the Common Proxy User”](#) on page 343
- ♦ [“Services That Cannot Leverage the Common Proxy User”](#) on page 343

Services That Can Leverage the Common Proxy User

The following OES services are automatically configured at install time by default to use your Common Proxy User (if specified):

- ♦ Novell AFP
- ♦ Novell CIFS
- ♦ Novell Cluster Services
- ♦ Novell DNS
- ♦ Novell DHCP
- ♦ Novell iFolder
- ♦ Novell NetStorage

The following OES service can be configured at install time to use your Common Proxy User (if specified):

- ♦ Linux User Management (having a proxy user is optional)

Services That Cannot Leverage the Common Proxy User

The following services that use proxy users do not leverage the Common Proxy user for the reasons listed:

Service	Reason
Archive and Version Services	This service uses the installing administrator as in the past. The user's credentials are written in the CASA/password files or databases.
Novell Samba	Samba proxy password requirements are not a good fit with the Common Proxy user. The user's credentials are written in the CASA/password files or databases.
Novell Storage Services	This requires full rights to administer NSS and continues to require a system-named user with a system-generated password.

Can a Common Proxy User Service Multiple Servers?

No.

The common proxy user is designed and configured to be the common proxy for the OES services on a single server. Each subsequent new server needs a separate and distinct common proxy created for its services.

Can I Change the Common Proxy User Name and Context?

The Common Proxy User Name cannot be changed at install time and should not be manually changed later. Best practices dictate that each proxy user name reflect the name of the server it is associated with.

The context can be changed at install time. However, eDirectory best practices suggest that object locations within the tree reflect the object purpose and scope of influence or function. For this reason, the OES install proposes the same context that you specify for the server, for its associated common proxy as well.

Can I Assign the Common Proxy User After Services Are Installed?

Yes. See [“Assigning the Common Proxy to Existing Services” on page 345](#).

What About Upgraded Servers Using a Common Proxy?

You can change the services running on an upgraded OES 11 SP2 server to leverage a Common Proxy user. See [“Assigning the Common Proxy to Existing Services” on page 345](#).

Are There Important Limitations to Keep in Mind?

Yes.

iFolder must not be configured to use a Common Proxy on a cluster node.

H.3.2 Managing Common Proxy Users

Common proxy users are eDirectory objects and can therefore be managed via iManager. However, after the initial setup is complete, there should generally be no reason for OES administrators to directly manage Common Proxy users.

Use the information in the following sections to understand and implement common proxy user management.

- ♦ [“Always Use LDAP Port 636 to Communicate with eDirectory” on page 345](#)
- ♦ [“Assigning the Common Proxy to Existing Services” on page 345](#)
- ♦ [“Changing Proxy Passwords Automatically” on page 346](#)

Always Use LDAP Port 636 to Communicate with eDirectory

The Common Proxy user management scripts communicate with eDirectory using port 636 only. See the instructions in [“Installing OES 11 SP2 as a New Installation”](#) in the *OES 11 SP2: Installation Guide*).

Assigning the Common Proxy to Existing Services

You can assign the common proxy user to any of the services listed in [“Services That Can Leverage the Common Proxy User” on page 343](#) using the `move_to_common_proxy.sh` script on your OES 11 SP2 server. In fact, if you have upgraded from SP2 and the server doesn't have a common proxy user associated with it, simply running the script will create and configure the proxy user and assign the services you specify.

- 1 In the `/opt/novell/proxymgmt/bin` folder, run the following command:

```
./move_to_common_proxy.sh service1,service2
```

where the service entries are OES service names: `novell-cifs`, `novell-dns`, `novell-dhcp`, `novell-iFolder`, `novell-netstorage`, `novell-lum`, and/or `novell-nc`.

Example scenario:

- ♦ You have upgraded server `myserver`, which is located in `o=novell` and uses IP address `10.10.10.1`, from OES 2 SP3 to OES 11 SP2.
- ♦ The secure LDAP port for the server is 636.
- ♦ Your eDirectory Admin user FQDN is `cn=admin,o=novell`.
- ♦ Your Admin password is `123abc`.
- ♦ You want to create a common proxy user and assign it as the common proxy for the Novell DNS and DHCP services running on the server.
- ♦ Therefore, you enter the following commands:

```
cd /opt/novell/proxymgmt/bin
```

```
./move_to_common_proxy.sh -d cn=admin,o=novell -w 123abc -i 10.10.10.1 -p 636 -s novell-dhcp,novell-dns
```

User `cn=OESCommonProxy_myserver,o=novell` is created with a system-generated password and assigned the Common Proxy Policy password policy. The DNS and DHCP services are configured to be serviced by the Common Proxy user.

Changing Proxy Passwords Automatically

You can configure your server so that your proxy users are regularly assigned new system-generated passwords by doing the following:

- 1 Open the file `/etc/opt/novell/proxymgmt/proxy_users.conf` in a text editor.
- 2 List the FQDN of each proxy user on the server that you want to automatic password management set up for.

For example you might insert the following entries:

```
cn=OESCommonProxyUser_myserver,o=novell
cn=myproxy,o=novell
```

IMPORTANT: Users listed here must not be listed in the `proxy_users.conf` file on any other servers in the tree.

- 3 Save the file.
- 4 Enter the following commands:

```
cd /opt/novell/proxymgmt/bin
change_proxy_pwd.sh -A Yes
```

By default, the crontab job will run every 30 days.

H.4 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 H.4.1, “About Proxy User Creation,” on page 346](#)
- ♦ [Section H.4.2, “There Are No Proxy User Impacts on User Connection Licenses,” on page 351](#)
- ♦ [Section H.4.3, “Limiting the Number of Proxy Users in Your Tree,” on page 351](#)
- ♦ [Section H.4.4, “Password Management and Proxy Users,” on page 353](#)

H.4.1 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 346](#)
- ♦ [“Do Not Manually Configure Proxy Users” on page 350](#)
- ♦ [“Avoid Assigning an Admin User As a Proxy User” on page 350](#)

Creation Options

[Table H-2](#) presents information about the creation options for each OES proxy user.

Table H-5 Proxy User Creation Options

Associated Service	Service Proxy User Name if Applicable	Creation Information
AFP	OESCommonProxy_ <i>hostname</i> Or AfpProxyUser- <i>servername</i>	<ul style="list-style-type: none"> ♦ Common Proxy User: If a Common Proxy User is specified, AFP will be automatically configured to use it by default, but you have the option to change this. ♦ No Common Proxy User: If a Common Proxy User is not specified, the AFP YaST install automatically does the following: <ul style="list-style-type: none"> ♦ Creates a proxy user named AfpProxyUser-<i>servername</i> in the same context as the server. ♦ Generates a password, and stores it in CASA. <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>
Archive Versioning	admin	The admin account that installs the server is automatically assigned as the Archive and Versioning proxy user. This is not configurable. Therefore, the new Common Proxy User feature doesn't apply.
CIFS	OESCommonProxy_ <i>hostname</i> Or CifsProxyUser- <i>servername</i>	<ul style="list-style-type: none"> ♦ Common Proxy User: If a Common Proxy User is specified, CIFS will be automatically configured to use it by default, but you have the option to change this. ♦ No Common Proxy User: If a Common Proxy User is not specified, the CIFS YaST install automatically does the following: <ul style="list-style-type: none"> ♦ Creates a proxy user named cifsProxyUser-<i>servername</i> in the same context as the server. ♦ Generates a password, and stores it in either CASA or in an encrypted file on the server, depending on which option you select. <p>Alternatively, you can modify any of the defaults, including the password. Or if you have already created a proxy user, you can specify that as well.</p>
Clustering (NCS)	OESCommonProxy_ <i>hostname</i> Or installing admin user	<ul style="list-style-type: none"> ♦ Common Proxy User: If the Common Proxy User is specified, it is granted membership in the NCS_Management group, which enables it to communicate with eDirectory on behalf of the clustering service. ♦ No Common Proxy User: If a Common Proxy User is not specified, the system automatically uses the installing administrator, which is granted membership in the NCS_Management group, which enables it to communicate with eDirectory on behalf of the clustering service.

Associated Service	Service Proxy User Name if Applicable	Creation Information
DHCP	OESCommonProxy_ <i>hostname</i> Or installing administrator	<ul style="list-style-type: none"> ♦ Common Proxy User: If a Common Proxy User is specified, DHCP will be automatically configured to use it by default, but you have the option to change this. ♦ No Common Proxy User: If a Common Proxy User is not specified, the admin account that installs the server is assigned as the DHCP proxy user. 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.
DNS	OESCommonProxy_ <i>hostname</i> Or installing administrator	<ul style="list-style-type: none"> ♦ Common Proxy User: If a Common Proxy User is specified, DNS will be automatically configured to use it by default, but you have the option to change this. ♦ No Common Proxy User: If a Common Proxy User is not specified, the admin account that installs the server is assigned as the DNS proxy user. 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.
Domain Services for Windows (DSfW)	OESCommonProxy_ <i>hostname</i> Or DNS	<ul style="list-style-type: none"> ♦ Common Proxy User: If a Common Proxy User is specified, DSfW will be automatically configured to use it by default, but you have the option to change this. ♦ No Common Proxy User: If a Common Proxy User is not specified, the admin account that installs the server is assigned as the DNS proxy user. 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.
iFolder 3	OESCommonProxy_ <i>hostname</i> Or iFolderProxy IMPORTANT: The Common Proxy user cannot be used if iFolder is running on a cluster node.	<ul style="list-style-type: none"> ♦ Common Proxy User: If a Common Proxy User is specified, iFolder will be automatically configured to use it by default, but you have the option to change this. ♦ No Common Proxy User: If a Common Proxy User is not specified, the system automatically creates a proxy user named iFolderProxy. 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.

Associated Service	Service Proxy User Name if Applicable	Creation Information
Linux User Management	OESCommonProxy_ <i>hostname</i> Or <i>LUM_proxy</i> (optional)	<p>By default, no LUM proxy user is created.</p> <ul style="list-style-type: none"> ♦ Common Proxy User: If a Common Proxy User is specified, you have the option of specifying that it be used as the LUM proxy user. If you do this, LUM is automatically configured to use it. ♦ No Common Proxy User: If you create a proxy user for LUM, it will be assigned rights to search the LDAP tree for LUM objects. <p>If you assign a previously created user as the LUM proxy user, it must have the Read right to the LDAP service.</p>
NetStorage	OESCommonProxy_ <i>hostname</i> Or Installing administrator	<ul style="list-style-type: none"> ♦ Common Proxy User: If the Common Proxy User is specified, NetStorage will be configured to use it by default, but you have the option to change this. <p>You must manually configure the proxy user with the rights specified in NetStorage in Table H-4 on page 340. For more information, see “Changing the NetStorage Default Configuration” in the <i>OES 11 SP2: NetStorage Administration Guide for Linux</i>.</p> <ul style="list-style-type: none"> ♦ No Common Proxy User: If a Common Proxy User is not specified, the system automatically uses the installing administrator. <p>Alternatively, you can modify any of the defaults, including the password, or if you have already created a different proxy user, you can specify that as well. The user must have the Read right to the LDAP service.</p>
NSS	<i>server_name</i> admin	This admin account must have full rights to administer NSS and must be unique to each server. The Common Proxy User does not apply to NSS.

Associated Service	Service Proxy User Name if Applicable	Creation Information
Samba (Novell)	<i>server_name</i> -SambaProxy	<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>A password is automatically generated for the default proxy user, or you specify a different password for this user when you configure Novell Samba.</p> <p>You can specify another eDirectory user as the Samba proxy user. If you do, be aware of the following:</p> <ul style="list-style-type: none"> ♦ If you specify a user that doesn't already exist in eDirectory, the user account is created and granted the necessary rights. You must also specify a password for the new user. ♦ If you specify an existing eDirectory user, it is assumed that you have already created the user account with the necessary rights and no modifications are made to the existing user. ♦ If you specify an existing eDirectory user but enter a new password, you are prompted to change the password for that user. <p>Because of the Samba proxy password requirements, the Common Proxy User cannot be used with Novell Samba.</p>

Do Not Manually Configure Proxy Users

Best practices for most OES installation scenarios dictate that either the Common Proxy user be used or that proxy users be created in eDirectory prior to installing OES. For more information, see [“Common Proxy User” on page 342](#) and [“Limiting the Number of Proxy Users in Your Tree” on page 351](#).

IMPORTANT: The information in the preceding and following sections only answers security questions and provides general information. It is not intended to be used for the manual configuration of proxy users.

Manually created proxy users must be configured for OES-rootservice use only by the YaST based install, not manually.

Avoid Assigning an Admin User As a Proxy User

We recommend that you always use the special-purpose proxy user accounts described in this and the accompanying sections rather than specifying admin users as proxy users. Best practice dictates that proxy users have strictly limited functionality that supports only their specific system-level responsibilities. Proxy users should not be used for any other purposes.

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 if the Common Proxy user option isn't selected), 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 11 SP2 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 11 SP2 on multiple servers, and the credentials were 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.

H.4.2 There Are No Proxy User Impacts on User Connection Licenses

Novell policy dictates that proxy users that function only as proxy users, are simply system users. Therefore, proxy users do not consume user connection licenses.

H.4.3 Limiting the Number of Proxy Users in Your Tree

The main purposes of the common proxy users are to reduce the number of proxy users in a tree and simplify proxy user management. Therefore, the common proxy user is the default in all applicable scenarios.

[Table H-6](#) outlines various alternative options for limiting the number of proxy users in your tree and summarizes the security and manageability considerations of each approach.

Table H-6 Options for Limiting the Number of Proxy Users

Approach	Security Considerations	Manageability Considerations
Per Service per Server	<p>For CIFS, iFolder 3, and Samba this is the most secure option. By default, the 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 "Avoid Assigning an Admin User As a Proxy User" on page 350.</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	Security Considerations	Manageability Considerations
Per Server	This confines any security vulnerabilities to individual servers and is the scenario for which the Common Proxy User was developed.	<p>This requires that a proxy user for the server is created before the server is installed.</p> <p>If the Common Proxy User is not leveraged, then for the first server in the tree, eDirectory and iManager must be installed with the server. After the server installation finishes, a 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 approach is 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>Knowing the proxy user password is not required unless additional services will be installed or password policies require periodic changing, in which cases the install admin must know the proxy user's password.</p>
Per 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 first server in 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	<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 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>
Per Tree	This exposes all OES services and servers in the tree to any security vulnerabilities.	<p>A proxy user for the tree must be created before any OES services are installed in the tree.</p> <p>This is suitable for organizations that have</p> <ul style="list-style-type: none"> ♦ Centralized eDirectory administration ♦ Users that are not confined to the partition or subtree where the OES servers reside, but instead access different OES servers from all over the tree. <p>The install admin must know the proxy user's password.</p>

H.4.4 Password Management and Proxy Users

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. Manually Specified Passwords” on page 353](#)
- ♦ [“Passwords Are Stored on the Server” on page 353](#)
- ♦ [“Avoid Password Expiration Problems” on page 354](#)
- ♦ [“Changing Proxy Passwords Automatically” on page 355](#)
- ♦ [“Changing Proxy Passwords Manually” on page 355](#)

Auto-Generated vs. Manually Specified Passwords

- ♦ **Auto-Generated Passwords:** These offer the highest security because the passwords are known only to the system.

The Common Proxy User, CIFS Proxy User, iFolder Proxy User (YaST calls this the *LDAP proxy user*), and Samba Proxy User all use auto-generated passwords by default.

- ♦ **Manually Specified Passwords:** Although you can change the auto-generated passwords for the various proxy users, this is not recommended because it is less secure and requires that someone keep track of the passwords. Also, manually specified passwords can easily lead to problems, such as service disruption. For a related example of the problems this can cause, see [“Avoid Assigning an Admin User As a Proxy User” on page 350](#).

Passwords Are Stored on the Server

Of course all proxy user passwords are stored in eDirectory. [Table H-7](#) explains where they are stored on the server and how they can be reset if needed.

Table H-7 Password Storage Locations

Associated Service	Where the Password Is Stored Locally	How the Password Can Be Reset
AFP	If the service-specific proxy user is used, the password is stored in either CASA or in an encrypted file, depending on the configuration option specified during service installation.	You can reset the password using iManager or the CASACli tool.
Archive and Versioning	The service-specific password is stored in CASA.	You must use the script provided by Archive and Versioning Services to change the password on the server.
CIFS	If the service-specific proxy user is used, the 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.
Common Proxy User	This password is stored in CASA.	We recommend that you only use the <code>change_proxy_pwd.sh</code> script to manage Common Proxy User passwords.

Associated Service	Where the Password Is Stored Locally	How the Password Can Be Reset
DHCP	The service-specific password is stored in CASA.	You can set the password using the CASACli tool.
DNS	If the service-specific proxy user is used, the service-specific password is stored in CASA if it is available. If CASA is not available, it is stored in an encrypted file.	
iFolder 3	If the service-specific proxy user is used, the service-specific 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	If the service-specific proxy user is used, the service-specific is stored in CASA.	This can be changed in iManager through the Linux User Management plug-in.
NetStorage	If the service-specific proxy user is used, the service-specific 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)	The service-specific password is stored in Samba.	You can change the password by using the smbpasswd 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 350](#).

If password expiration policies cannot be avoided, or a security policy dictates that proxy user passwords must be changed periodically, we strongly urge you to implement an automatic password change routine as explained in [“Changing Proxy Passwords Automatically” on page 355](#).

Otherwise you should probably do the following.

- ♦ Ensure that the responsible administrator knows or has a record of each proxy user’s password and is aware of when each password expires.
- ♦ Before passwords expire, change them in eDirectory and reset them on the server. See the information in [Table H-7](#).

Changing Proxy Passwords Automatically

You can configure your server so that your proxy users are regularly assigned new system-generated passwords by doing the following:

- 1 Open the file `/etc/opt/novell/proxymgmt/proxy_users.conf` in a text editor.
- 2 List the FQDN of each proxy user on the server that you want to automatic password management set up for.

For example you might insert the following entries:

```
cn=OESCommonProxyUser_myserver.o=novell
cn=myproxy.o=novell
```

IMPORTANT: Users listed here must not be listed in the `proxy_users.conf` file on any other servers in the tree.

- 3 Save the file.
- 4 Enter the following commands:

```
cd /opt/novell/proxymgmt/bin
change_proxy_pwd.sh -A Yes
```

By default, the crontab job will run on the fifteenth (15th) day of each month.

Changing Proxy Passwords Manually

The `change_proxy_pwd.sh` command can also be used to enter a proxy user password.

IMPORTANT: If you enter a password by using the `change_proxy_pwd.sh` command, the password cannot contain special shell variables (`$#`, `$_`, or `#?`). These characters are interpreted by the shell while processing service scripts.

The workaround is to enter the password within single quotes. For example, you can enter the password `novell$$` as `'novell$$'`. The shell doesn't interpret content within single quotes.

H.5 Implementing Your Proxy User Plan

The proxy users in OES can be configured at different levels within eDirectory, depending on your needs.

IMPORTANT: If you plan to use the Common Proxy User, you can ignore this note.

The brief instructions that follow assume that you are installing into an existing tree and not leveraging the Common Proxy User.

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 H-5 on page 347](#)). In most cases a default configuration assigns the install admin as the proxy user for the service.

- [Section H.5.1, “Tree-Wide Proxy Users,” on page 356](#)
- [Section H.5.2, “Service-Specific Proxy Users,” on page 356](#)
- [Section H.5.3, “Partition-Wide Proxy Users,” on page 356](#)
- [Section H.5.4, “Server-Wide Proxy User,” on page 356](#)
- [Section H.5.5, “Individual Proxy User Per-Server-Per-Service,” on page 357](#)

H.5.1 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.

H.5.2 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 CIFS proxy user, `cifs_proxy_user`.

2. Use these proxy users and passwords appropriately for each of the OES services on all OES servers.

H.5.3 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.

H.5.4 Server-Wide Proxy User

NOTE: The Common Proxy User is specifically designed as the default for this scenario.

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.

H.5.5 Individual Proxy User Per-Server-Per-Service

This is the installation default if the Common Proxy User is not utilized as explained in [Table H-6, “Options for Limiting the Number of Proxy Users,”](#) on page 351.

H.6 Proxy Users and Domain Services for Windows

Proxy users are not used in DSfW.

The Services part of the Trusted Computed 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.

However, the DNS Proxy User is closely associated with DSfW and can leverage the Common Proxy User.

H.7 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 H-2](#) lists the various system users that are used by OES services.

Table H-8 System User Purposes

System User or Group Name	Associated Service	Purpose
arkuser	Archive and Versioning Services	The service uses PostgreSQL as its metadata store, and PostgreSQL must run as a low-privileged user. arkuser is that low-privileged user.

System User or Group Name	Associated Service	Purpose
dhcpcd	DHCP	<p>DHCP accesses local resources through this or an alternatively specified user.</p> <p>If the DHCP lease and configuration files are stored on NSS, the user must be moved to eDirectory and LUM enabled.</p> <p>dhcpcd is used by default, but any local user can be used.</p>
iprint	iPrint	<p>The iPrint daemons run as this user.</p> <p>If iPrint is moved to NSS, this user is created in eDirectory and the local user is removed.</p>
named	DNS	<p>This system user lets DNS access local resources.</p> <p>In case of clusters, DNS data is on NSS volume, and so the user has to be created in eDirectory as well.</p> <p>named is used by default, but any local user can be used.</p>
novell_nobody	CIMOM	This user is created by CIMOM but is not currently used.
novlxregd	XTier	<p>The XTier Registry Daemon (novell-xregd) runs as this user.</p> <p>When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.</p>
novlxsrvd	XTier	<p>The XTier Server Daemon (novell-xsrvd) runs as this user.</p> <p>When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.</p>
wwwrun	Apache	<p>The Apache daemon runs as this user.</p> <p>When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.</p>

H.8 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 H-2](#) lists the system groups that are used by OES services.

Table H-9 System Group Purposes

System User or Group Name	Associated Service	Purpose
lprint (POSIX) iprintgrp (eDirectory)	iPrint	The iPrint daemons use the group ID (gid) of this group to run. If iPrint is moved to NSS, the iprintgrp 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. Apache (<code>wwwrun</code>) is a group member because it needs XTier socket access. 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 “The Samba connection:” on page 156 .
shadow	QuickFinder	Used by QuickFinder and other Web services.
www	Apache Tomcat QuickFinder	Apache (<code>wwwrun</code>) and tomcat (<code>novlwww</code>) use the group ID (gid) of this group to run. QuickFinder requires that all users who manage the service (including the eDirectory Admin user) belong to this group. User <code>novlxsrvd</code> is in the group because it needs access to an Apache domain socket. When NSS is installed on the Linux server, this group is removed from the local system and created in eDirectory. This is required because members of this group must have access to NSS data, and all NSS access is controlled through eDirectory.

H.9 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](#).” 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 11 SP2

Every OES network requires at least one administrative-level user to manage regular network users and system users.

Table I-1 Administrative Users and Groups

Administrative User or Group	Associated Service	Object Type	Purpose
Admin	eDirectory	Admin User	The eDirectory administrator that has all rights to manage the Tree. The default is Admin.
Container Admin	eDirectory	Admin User	These administrators are usually responsible for administering within a partition or subtree. They might be assigned only enough rights to install servers, or they might be assigned to specific roles in iManager.
admingroup	eDirectory	Admin Group	Provides LUM-enabling for the eDirectory administrator.
iFolderAdmin	iFolder 3	Service Admin	This is the default iFolder service administrator account. By default, the Tree Admin is specified.
QuickFinderAdmin	QuickFinder	Service Admin	This is the QuickFinder administrator. The default is the Tree Admin.

TIP: The iManager Role-based-services (RBS) feature lets you delegate administrative responsibilities based on administrative roles. For more information, see [“Role-Based Services”](#) in the *NetIQ® iManager Administration Guide*.

J Coordinating Password Policies Among Multiple File Services

- ♦ [Section J.1, “Overview,” on page 363](#)
- ♦ [Section J.2, “Concepts and Prerequisites,” on page 363](#)
- ♦ [Section J.3, “Examples,” on page 364](#)
- ♦ [Section J.4, “Deployment Guidelines for Different Servers and Deployment Scenarios,” on page 367](#)

J.1 Overview

OES 11 SP2 includes native file services for Windows and Macintosh workstations:

Macintosh Workstations	Windows Workstations
<ul style="list-style-type: none">♦ Novell AFP♦ Novell CIFS	<ul style="list-style-type: none">♦ Novell CIFS♦ Novell Samba♦ Domain Services for Windows (DSfW) <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.

J.2 Concepts and Prerequisites

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

- ♦ [Section J.2.1, “Prerequisites for File Service Access,” on page 363](#)
- ♦ [Section J.2.2, “eDirectory contexts,” on page 364](#)
- ♦ [Section J.2.3, “Password Policies and Assignments,” on page 364](#)

J.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.

- ♦ There must be at least one writable replica of NMAS version 3.2 or later having the user object trying to access the AFP or CIFS server. NMAS 3.2 is already present on OES 2 servers, and NMAS 3.2 is installed on servers running eDirectory 8.8.2. On NetWare servers with a lone writable replica of a AFP or CIFS user, NMAS 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.

J.2.2 eDirectory contexts

- ♦ **AFP:** 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.

J.2.3 Password Policies and Assignments

- ♦ **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.

J.3 Examples

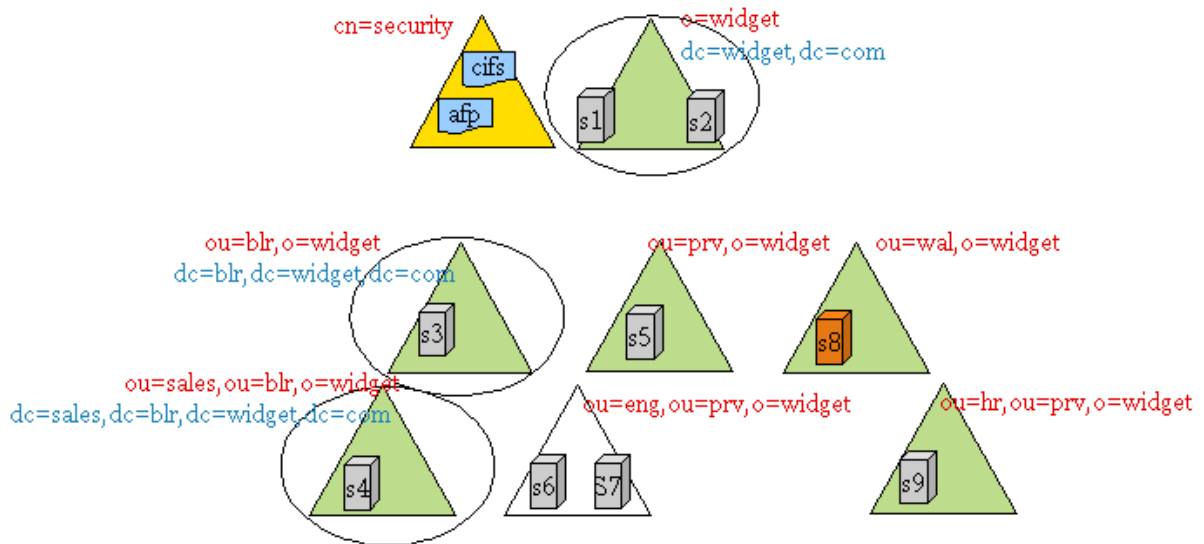
- ♦ [Section J.3.1, "Example 1: Complex Mixed Tree with a Mix of File Access Services and Users from across the Tree," on page 364](#)
- ♦ [Section J.3.2, "Example 2: Mutually Exclusive Users," on page 366](#)

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

- ♦ ["Tree Setup" on page 365](#)
- ♦ ["OES/NetWare Servers" on page 365](#)
- ♦ ["File Services" on page 365](#)

- ♦ “User Access to Services” on page 366
- ♦ “Rights Required for Installation and Administration” on page 366

Figure J-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 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

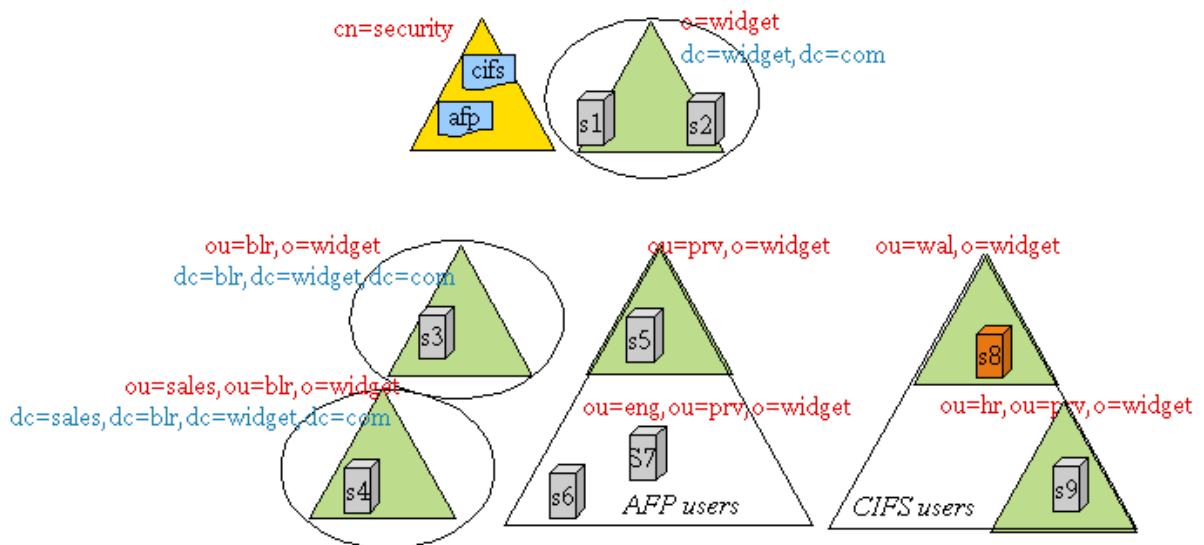
Installation and configuration in iManager must be done by an OES administrator. This is typically a container administrator in eDirectory who has supervisory privileges over the container where the server is being installed. This need not be the tree administrator.

J.3.2 Example 2: Mutually Exclusive Users

- ♦ “File Services” on page 366
- ♦ “Users” on page 367

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 J-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 serves 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.

J.4 Deployment Guidelines for Different Servers and Deployment Scenarios

- ♦ [Section J.4.1, “Deployment Scenario 1: Complex Mixed Scenario with a Mix of File Access Services,” on page 367](#)
- ♦ [Section J.4.2, “Deployment Scenario 2: Mutually /Exclusive Users,” on page 369](#)
- ♦ [Section J.4.3, “Deployment Scenario 3: Simple deployments,” on page 369](#)
- ♦ [Section J.4.4, “Modifying User Password Policies after Samba/DSfW Is Installed,” on page 369](#)
- ♦ [Section J.4.5, “Adding New User eDirectory Contexts to AFP/CIFS after AFP/CIFS/Samba/DSfW Is Installed.,” on page 369](#)
- ♦ [Section J.4.6, “Enabling File Access for DSfW Servers Across Domains,” on page 370](#)

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

- ♦ [“First Server in a New Tree \(Example1\)” on page 367](#)
- ♦ [“Subsequent Servers in a Tree \(Example 1\)” on page 368](#)

First Server in a New Tree (Example1)

- ♦ [“Not recommended—non-name-mapped \(new tree\) S1 \(DSfW\) server” on page 367](#)
- ♦ [“Non-DSFW Server” on page 368](#)

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 auto-created common proxy user in eDirectory configuration for the OES services.
- 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 Use an auto-generated common proxy user for all the services.
 - 4b 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 368
- ♦ “S5” on page 368
- ♦ “S6” on page 368
- ♦ “S7” on page 368
- ♦ “S8” on page 368
- ♦ “S9” on page 369

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 11 SP2: Domain Services for Windows Administration Guide](#) to deploy S3 and S4 in the tree.

S5

- 1 Use an auto-generated common proxy user for all the services.

S6

Use the same procedure as for S5.

S7

Use the same procedure as for S5 and S6.

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 OES11 SP2, AFP and CIFS users should be enabled for Universal Password by having a password policy configured. CIFS users need to log in through NCP (Novell Client) to synchronize their NDS passwords to the Universal Password.

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.

J.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.

J.4.3 Deployment Scenario 3: Simple deployments

Simple deployments require very little planning.

One auto-generated common proxy user per server for all services configured on the server is a good choice.

J.4.4 Modifying User Password Policies after Samba/DSfW Is Installed

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

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

If users from additional or different eDirectory contexts need to be allowed to access CIFS or AFP, rerun the YaST-based configuration and modify or add the required edirectory user contexts.

J.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.

K Configuration and Log Files

- ♦ [Section K.1, “AFP,” on page 371](#)
- ♦ [Section K.2, “Archive and Version Services,” on page 372](#)
- ♦ [Section K.3, “CIFS,” on page 372](#)
- ♦ [Section K.4, “Common Proxy,” on page 373](#)
- ♦ [Section K.5, “DFS,” on page 373](#)
- ♦ [Section K.6, “DHCP,” on page 373](#)
- ♦ [Section K.7, “DNS,” on page 374](#)
- ♦ [Section K.8, “Domain Services for Windows,” on page 374](#)
- ♦ [Section K.9, “Install,” on page 376](#)
- ♦ [Section K.10, “iFolder Server,” on page 377](#)
- ♦ [Section K.11, “iPrint,” on page 378](#)
- ♦ [Section K.12, “Linux User Management,” on page 378](#)
- ♦ [Section K.13, “Migration Tool,” on page 379](#)
- ♦ [Section K.14, “NetStorage,” on page 380](#)
- ♦ [Section K.15, “Novell Cluster Services,” on page 381](#)
- ♦ [Section K.16, “Novell Linux Volume Manager,” on page 381](#)
- ♦ [Section K.17, “Novell Storage Services,” on page 382](#)
- ♦ [Section K.18, “Novell Samba,” on page 382](#)
- ♦ [Section K.19, “NCP,” on page 383](#)
- ♦ [Section K.20, “QuickFinder,” on page 383](#)
- ♦ [Section K.21, “SMS,” on page 384](#)
- ♦ [Section K.22, “Vigil,” on page 384](#)

K.1 AFP

Table K-1 *AFP Configuration Files*

Path	Description
/etc/opt/novell/afptcpd/afpdirxt.conf	List of eDirectory contexts having AFP users
/etc/opt/novell/afptcpd/afptcpd.conf	AFP server
/etc/opt/novell/afptcpd/afpvols.conf	List of NSS volumes to export through AFP server
/opt/novell/afptcpd/lsm/afplinlsmconfig.txt	Used by installation of AFP NMAS method into eDirectory tree.

Table K-2 AFP Log Files

Path	Description
/var/opt/novell/log/afptcp.log	AFP server run-time

K.2 Archive and Version Services

Table K-3 Archive and Version Services Configuration Files

Path	Description
/etc/opt/novell/arkmanager/conf/arkConfig.xml	Server configuration file
/etc/opt/novell/arkmanager/conf/arkdatadir.conf	AV database configuration info.

Table K-4 Archive and Version Services Log Files

Path	Description
/var/opt/novell/arkmanager/logs/ark.log	This file is a link to the latest rotatable logs.

K.3 CIFS

Table K-5 CIFS Configuration Files

Path	Description
/etc/opt/novell/cifs/cifs.conf	CIFS server
/etc/opt/novell/cifs/cifsctxs.conf	List of eDirectory contexts having CIFS users
/etc/opt/novell/cifs/cifslogrotate.conf	Hourly rotation of CIFS log file
/etc/opt/novell/cifs/logrotate.d/novell-cifs-hourly	Customized hourly rotation of CIFS log file
/opt/novell/cifs/share/nmasmthd/ntlm/config.txt	Used by installation of CIFS NMAS method into eDirectory tree.

Table K-6 CIFS Log Files

Path	Description
/var/opt/novell/log/cifs.log	CIFS server run-time

K.4 Common Proxy

Table K-7 Common Proxy Configuration Files

Path	Description
/etc/opt/novell/proxymgmt/proxy_users.conf	List of proxy users on local systems whose password is changed automatically

Table K-8 Common Proxy Log Files

Path	Description
/var/opt/novell/log/proxymgmt/pxylist.txt	List of proxy users used by services on local systems. Created when /opt/novell/proxymgmt/bin/retrieve_proxy_list.sh is run.
/var/opt/novell/log/proxymgmt/pxymgmt.log	

K.5 DFS

Table K-9 DFS Log Files

Path	Description
/var/log/messages	DFS Logs
/var/opt/novell/tomcat6/logs/catalina.out	iManager Logs
/var/opt/novell/log/dfs/vlrpr.log	VLDB Repair Logs

K.6 DHCP

Table K-10 DHCP Configuration Files

Path	Description
/etc/dhcpd.conf	

Table K-11 DHCP Log Files

Path	Description
/var/log/dhcp-ldap-startup.log	
/var/log/dhcpd.log	
/var/log/rc.dhcpd.log	DHCP server failure during startup

K.7 DNS

Table K-12 DNS Configuration Files

Path	Description
/etc/opt/novell/named/named.conf	configuration file loaded from e-directory

Table K-13 DNS Log Files

Path	Description
/var/opt/novell/log/named_zones.info	
/var/opt/novell/log/named.run	

K.8 Domain Services for Windows

Table K-14 DSfW Configuration Files

Path	Description
/etc/krb5.conf	kerberos configuration for DSfW.
/etc/krb5.keytab	Kerberos related link used by samba service.
/etc/nsswitch.conf	Configuration of Name service switch used by DSfW.
/etc/ntp.conf	ntp server Configuration for DSfW.
/etc/opt/novell/eDirectory/conf/nds.conf	The eDirectory configuration file.
/etc/opt/novell/eDirectory/conf/ndsm_modules.conf	This file describes the modules to be loaded at boot-up into ndsd address space. Specific to DSfW it includes samspm.
/etc/opt/novell/named/named.conf	DNS configuration file.
/etc/opt/novell/xad/gss/mech	gssapi configuration information.
/etc/opt/novell/xad/openldap/ldap.conf	Defaults used by LDAP.
/etc/opt/novell/xad/xad.ini	DSfW related information (domain name, Admin details, IP address, DNS context etc).
/etc/opt/novell/xad/xadss.conf	Domain Services for Windows RPC server configuration.
/etc/resolv.conf	Configuration of DNS client for accessing DNS server.
/etc/rsyncd.conf	Configuration file for adding directories to be synchronized during sysvolsync.
/etc/smb.conf	Samba Configuration for DSfW.

Path	Description
/etc/ssh/ssh_config	Used to enable gssapi authentication during installation.
/etc/ssh/sshd_config	Used to enable gssapi authentication during installation.
/etc/sysconfig/novell/xad2_oes11	File containing parameters specified during YaST configuration of DSfW. Used by other components like LU

Table K-15 DSfW Log Files

Path	Description
/var/log/messages	For DSfW the keywords which are of importance are “xadsd”, “smbd”, and “winbind”.
/var/log/samba/log.nmbd	Logs related to nmbd process (“smbcontrol nmbd debug 10” can be used to set the log level to maximum.).
/var/log/samba/log.smbd	Logs related to smbd process (“smbcontrol smbd debug 10” can be used to set the log level to maximum.).
/var/log/samba/log.wb-<DOMAIN>	domain specific winbindd logs. The DOMAIN refers to domain names which winbind is aware of.
/var/log/samba/log.winbindd	Logs related to winbindd process (“smbcontrol winbindd debug 10” can be used to set the log level to maximum.).
/var/log/samba/log.winbindd-idmap	Winbind id mapping related logs, that is SID to UID/GID and vice versa.
/var/log/YaST2/y2log	Logging done during YaST configuration and Installation of DSfW.
/var/opt/novell/log/named.run	DNS logs (Activated using command “rndctrace 10”).
/var/opt/novell/xad/log/domaincntrl.log	Logs related to domaincntrl tool operations.
/var/opt/novell/xad/log/healthCheck.log	Log of server pre-check operations done during Installation and Provisioning.(Replica status, DNS status, remote server connectivity, purger, removing bad address cache etc.).
/var/opt/novell/xad/log/kdc.log	Kerberos (xad-krb5kdc) related logs.
/var/opt/novell/xad/log/kpasswd.log	Kerberos password server (xad-kpasswd) related logs.
/var/opt/novell/xad/log/ndsdcinit.log	More detailed log related to Installation and Provisioning of DSfW.
/var/opt/novell/xad/log/provisioning.log	Logging done during Provisioning phases of DSfW.
/var/opt/novell/xad/log/sysvolsync.log	Log about the sysvol synchronization details.
/var/opt/novell/xad/run/rpcd.log	Logs related to rpcd daemon.

K.9 Install

Table K-16 *Install Framework Configuration Files*

Path	Description
/etc/sysconfig/novell/afp_oes11_sp2	
/etc/sysconfig/novell/arkman_oes11_sp2	
/etc/sysconfig/novell/cmmn_oes11_sp2	
/etc/sysconfig/novell/edir_oes11_sp2	
/etc/sysconfig/novell/ifldr3__oes11_sp2	
/etc/sysconfig/novell/iman_oes11_sp2	
/etc/sysconfig/novell/iprnt_oes11_sp2	
/etc/sysconfig/novell/ldap_servers	
/etc/sysconfig/novell/lum_oes11_sp2	
/etc/sysconfig/novell/ncpsrvr_oes11_sp2	
/etc/sysconfig/novell/ncs_oes11_sp2	
/etc/sysconfig/novell/netstore_oes11_sp2	
/etc/sysconfig/novell/nss_oes11_sp2	
/etc/sysconfig/novell/NvICifs_oes11_sp2	
/etc/sysconfig/novell/NvIDhcp_oes11_sp2	
/etc/sysconfig/novell/NvIDns_oes11_sp2	
/etc/sysconfig/novell/nvlsamba_oes11_sp2	
/etc/sysconfig/novell/oes-ldap	
/etc/sysconfig/novell/quickfndr_oes11_sp2	
/etc/sysconfig/novell/schematool	
/etc/sysconfig/novell/sms_oes11_sp2	
/etc/sysconfig/novell/xad_oes11_sp2	

Table K-17 *Install Framework Log Files*

Path	Description
/var/opt/novell/eDirectory/log/oes_schema.log	

K.10 iFolder Server

Table K-18 iFolder Server Configuration Files

Path	Description
/opt/novell/ifolder3/bin/SimiasServerSetup.exe.config	
/opt/novell/ifolder3/bin/iFolderAdminSetup.exe.config	
/opt/novell/ifolder3/bin/iFolderWebSetup.exe.config	
/opt/novell/ifolder3/etc/novell-ifolder3.conf	
/opt/novell/ifolder3/etc/simias/Simias.config	
/opt/novell/ifolder3/etc/simias/Simias.log4net	
/opt/novell/ifolder3/etc/simias/apache/default/ifolder_admin.conf	
/opt/novell/ifolder3/etc/simias/apache/default/ifolder_webaccess.conf	
/opt/novell/ifolder3/etc/simias/apache/default/simias_server.conf	
/opt/novell/ifolder3/etc/simias/apache/example.com/ifolder_admin.conf	
/opt/novell/ifolder3/etc/simias/apache/example.com/ifolder_webaccess.conf	
/opt/novell/ifolder3/etc/simias/apache/example.com/simias_server.conf	
/opt/novell/ifolder3/etc/simias/apache/ifolder_apache.conf	
/opt/novell/ifolder3/etc/simias/bill/Simias.config	
/opt/novell/ifolder3/etc/simias/bill/modules/Simias.Server.conf	
/opt/novell/ifolder3/etc/simias/defaults.config	
/opt/novell/ifolder3/lib64/simias/web/update/unix/unix-version.config	
/opt/novell/ifolder3/lib64/simias/web/update/windows/version.config	
/opt/novell/ifolder3/lib64/simias/web/update/mac/mac-version.config	
/etc/apache2/conf.d/ifolder_admin.conf	
/etc/apache2/conf.d/ifolder_web.conf	
/etc/apache2/conf.d/simias.conf	
/opt/novell/ifolder3/lib64/simias/admin/Web.config	
/opt/novell/ifolder3/lib64/simias/web/web.config	
/opt/novell/ifolder3/lib64/simias/webaccess/Web.config	

Table K-19 iFolder Server Log Files

Path	Description
/var/opt/novell/log/oes/ifolder/adminweb.log	

K.11 iPrint

Table K-20 iPrint Configuration Files

Path	Description
/etc/ld.so.conf.d/iprint.conf	
/etc/opt/novell/httpd/conf.d/iprint_g.conf	iPrint configuration file for apache server
/etc/opt/novell/httpd/conf.d/iprint_ssl.conf	iPrint configuration file for apache server
/etc/opt/novell/iprint/conf/idsd-template.conf	iPrint Driver Store Daemon template configuration file
/etc/opt/novell/iprint/conf/ipsmd-template.conf	iPrint Print Manager Daemon template configuration file
/var/opt/novell/iprint/htdocs/iprint.ini	Configuration file for iPrint Windows Client

Table K-21 iPrint Log Files

Path	Description
/opt/novell/iprintmgmt/lib/Logger.properties	Logging other configurations file (java.util.logging.config.file).
/var/log/apache2/	Contains log files for Apache activities
/var/opt/novell/iManager/nps/WEB-INF/logs/debug.html	Debug information of iPrint plug-in for iManager
/var/opt/novell/log/iprintmgmt/IPrintManLogger0.log	iprintman log file.
/var/opt/novell/log/oes/iprint/idsd.log	Contains log messages of iPrint driverstore
/var/opt/novell/log/oes/iprint/iprint_nss_relocate.log	Contains logs of iPrint nss relocation script.
/var/opt/novell/log/oes/iprint/iprint_nss_relocate.log	Contains log messages of iPrint relocation script
/var/opt/novell/log/oes/iprint/iprintgw.log	Contains log messages of iPrint gateway process
/var/opt/novell/log/oes/iprint/ipsmd.log	Contains log messages of iPrint manager
/var/opt/novell/tomcat6/logs/catalina.out	Log file for iManager activities

K.12 Linux User Management

Table K-22 LUM Configuration Files

Path	Description
/etc/nam.conf	Configuration parameters for lum.
/etc/nsswitch.conf	LUM puts in 'nam' against 'passwd' and 'group' entries for the nsswitch plugin.

Table K-23 LUM Log Files

Path	Description
/var/lib/novell-lum/nam.log	Logging when LUM is configured.
/var/log/messages	Logging when namcd is running. This is the default location. It can also be configured to a different file by setting log-file-location in nam.conf and can change the level of logging by using log-level in nam.conf.
/var/log/YaST2/y2log*	Logging when LUM is configured.

K.13 Migration Tool

Table K-24 Migration Tool Configuration Files

Path	Description
<project_folder>/config.txt	The source NetWare server configuration file. This is used to verify nlm versions, code page and other details.

Table K-25 Migration Tool Log Files

Path	Description
<project_folder>/data.log	The output and errors encountered during execution of migatedir command.
<project_folder>/mignds.log	The log file created during edirectory dib copy
<project_folder>/migndschek.log	The log file created for nds time sync check
<project_folder>/log/afp.log	This stores the information about the command sequence and errors encountered during AFP migration.
<project_folder>/log/av.log	This stores the information about the command sequence and errors encountered during AV migration.
<project_folder>/log/cifs.log	This stores the information about the command sequence and errors encountered during CIFS migration.
<project_folder>/log/debug.log	This is the developer debug log which stores information on the user inputs, outputs, command sequence, errors and success of the entire migration.
<project_folder>/log/dhcp.log	This stores the information about the command sequence and errors encountered during DHCP migration.

Path	Description
<project_folder>/log/filesystem.log	This stores the information about the command sequence and errors encountered during File System migration.
<project_folder>/log/filesystem.success.log	This stores the list of all successfully migrated files during File System migration.
<project_folder>/log/ftp.log	This stores the information about the command sequence and errors encountered during FTP migration.
<project_folder>/log/ifolder.log	This stores the information about the command sequence and errors encountered during iFolder migration.
<project_folder>/log/iprint.log	This stores the information about the command sequence and errors encountered during iPrint migration.
<project_folder>/log/migration.log	This stores the information about the command sequence and errors encountered during iFolder migration.
<project_folder>/log/ntp.log	This stores the information about the command sequence and errors encountered during NTP migration.
<project_folder>/log/serveridswap.log	This stores the information about the command sequence, errors encountered and success states during identity migration.
/var/opt/novell/log/migration/migfiles.log	migfiles debug log
/var/opt/novell/log/migration/mls.log	mls debug log
/var/opt/novell/log/migration/mismatchup.log	mismatchup debug log
/var/opt/novell/log/migration/maptrustees.log	maptrustees debug log
/var/opt/novell/log/migration/migtrustees.log	migtrustees debug log
/var/opt/novell/log/migration/maprights.log	maprights debug logs
/var/opt/novell/log/migration/migrights.log	migrights debug log
/var/opt/novell/log/migration/volmount.log vol	mount debug log

K.14 NetStorage

Table K-26 NetStorage Configuration Files

Path	Description
/etc/opt/novell/netstorage/netstorage.conf	Apache config file
/opt/novell/netstorage/webapp/WEB-INF/classes/Settings.properties	Config file for ssh enabling, zip encoding, mail configuration changes.

Path	Description
/opt/novell/netstorage/webapp/WEB-INF/classes/Settings_*.properties	Same as Settings.properties but language specific.

Table K-27 NetStorage Log Files

Path	Description
/var/log/messages	Log file for NetStorage/Xtier
/var/opt/novell/netstorage/cifsdav.log	Log file for CIFS access.

K.15 Novell Cluster Services

Table K-28 NCS Configuration Files

Path	Description
/etc/opt/novell/ncs/clstrlib.conf	Cluster configuration file
/etc/opt/novell/ncs/<nodename>	Cluster configuration for a specific cluster node

Table K-29 NCS Log Files

Path	Description
/var/log/messages	Cluster event log. Events are viewable in Novell iManager by going to Clusters > My Clusters, select the cluster, then click Event Log.
/var/log/YaST2/y2log	Cluster Services configuration log
/var/opt/novell/install/ncslog	Cluster Services installation log
/var/opt/novell/log/ncs/<resource_name>.<load unload monitor>.out	Cluster resource runtime messages that are output from the load, unload, or monitor scripts

K.16 Novell Linux Volume Manager

Table K-30 NLVM Configuration Files

Path	Description
/etc/opt/novell/nss/nlvm.conf	Config file for nlvm.
/var/run/novell-nss/nlvm.lock	Local lock file for nlvm.

Table K-31 NLVM Log Files

Path	Description
/opt/novell/nss/nlvm/	Directory for nlvm storage configuration database files.
/var/opt/novell/log/nss.debug/	Directory for debug files when debug is enabled.

K.17 Novell Storage Services

Table K-32 NSS Configuration Files

Path	Description
/etc/opt/novell/nss/nlvm.conf	NLVM configuration file
/etc/opt/novell/nss/nssstart.cfg	NSS configuration file
/etc/opt/novell/nss/trustees.xml	

Table K-33 NSS Log Files

Path	Description
/var/log/messages	All Syslogs from NSS.
/var/opt/novell/log/nss/debug/*	Debug files for NLVM etc.
/var/opt/novell/log/nss/rav/*	Debug file for Rebuild and Verify.

K.18 Novell Samba

Table K-34 Novell Samba Configuration Files

Path	Description
/etc/samba/smb.conf	Service configuration

Table K-35 Novell Samba Log Files

Path	Description
path: /var/log/samba/novell-samba-config.log	Log file generated during execution of novell-samba-config.sh script

K.19 NCP

Table K-36 NCP Configuration Files

Path	Description of Configuration File
/etc/opt/novell/ncp/ncp2nss.audit.conf	Rotation of ncp2nss audit log files (/var/opt/novell/log/oes/ncp/ncp2nss.audit.log)
/etc/opt/novell/ncp/ncp2nss.log.conf	Rotation of NCP2NSS run-time log files (/var/opt/novell/log/oes/ncp/ncp2nss.log)
/etc/opt/novell/ncp/ncpserv.audit.conf	Rotation of NCP server audit log files (/var/opt/novell/log/oes/ncp/ncpserv.audit.log) of NCP Server
/etc/opt/novell/ncp/ncpserv.log.conf	Rotation of NCP server run-time log files (/var/opt/novell/log/oes/ncp/ncpserv.log)
/etc/opt/novell/ncp2nss.conf	NCP2NSS
/etc/opt/novell/ncpserv.conf	NCP server

Table K-37 NCP Log Files

Path	Description of Log File
/var/opt/novell/log/libnrm2ncp.log	Communication between NRM (Novell Remote Manager) and NCP Server
/var/opt/novell/log/ncp2nss.audit.log	NCP2NSS Audit
/var/opt/novell/log/ncp2nss.log	Communication between NCP server and NSS
/var/opt/novell/log/ncpcon.err	
/var/opt/novell/log/ncpcon.log	
/var/opt/novell/log/ncpserv.audit.log	NCP Server Audit
/var/opt/novell/log/ncpserv.log	NCP server

K.20 QuickFinder

Table K-38 QuickFinder Configuration Files

Path	Description of Configuration File
/var/lib/qfsearch/bin/configure-OES.sh	Script to configure quickfinder for OES. Run by YaST
/var/lib/qfsearch/bin/create-admin-user.sh	Script to create admin user in lum
/var/lib/qfsearch/bin/unconfigure-OES2.sh	Script to unconfigure quickfinder
/var/lib/qfsearch/bin/updatetomcat.sh	Script to customize tomcat for quickfinder

Table K-39 QuickFinder Log Files

Path	Description of Log File
/var/opt/novell/log/oes/qfsearch/access.log	access log
/var/opt/novell/log/oes/qfsearch/Cluster.log	cluster synchronization log
/var/opt/novell/log/oes/qfsearch/Error.log	error log

K.21 SMS

Table K-40 SMS Configuration Files

Path	Description of Configuration File
/etc/opt/novell/sms/smdrd.conf	Configuration of SMDRD daemon
/etc/opt/novell/sms/tsafs.conf	Configuration of TSAFS

Table K-41 SMS Log Files

Path	Description of Log File
/var/opt/novell/log/sms/smdrd_debug_MYPID.log	Logs for SMDRD calls (related to PID)
/var/opt/novell/log/sms/tsafs_debug_MYPID.log	Logs of TSAFS calls (related to PID)

K.22 Vigil

Table K-42 Vigil Configuration Files

Path	Description
/etc/ld.so.conf.d/novell-libvigil.conf	Path to libvigil shared object
/usr/share/omc/svcinfo.d/novell-vigil.xml	Description XML for NSS auditing engine

Table K-43 Vigil Log Files

Path	Description of Log File
/var/log/audit/vlog/clientName/	Logs for SMDRD calls (related to PID)

L Small Footprint CIM Broker (SFCB)

- ♦ Section L.1, “Overview,” on page 385
- ♦ Section L.2, “OES CIM Providers,” on page 386
- ♦ Section L.3, “SFCB Is Automatically Installed with OES 11 SP2,” on page 386
- ♦ Section L.4, “Coexistence with NRM and iManager in Earlier Releases,” on page 387
- ♦ Section L.5, “SFCB and Linux User Management (LUM),” on page 387
- ♦ Section L.6, “Links to More Information about WBEM and SFCB,” on page 387

L.1 Overview

OES 11 SP2 services are managed using Web-Based Enterprise Management (WBEM) as proposed by the [Distributed Management Task Force \(DMTF\)](http://www.dmtf.org/home) (<http://www.dmtf.org/home>).

The following information describes a few of the components proposed by the DMTF standards.

- ♦ **Web-Based Enterprise Management (WBEM):** Is a set of management and Internet standard technologies developed to unify the management of enterprise computing environments. WBEM provides the ability for the industry to deliver a well integrated set of standards-based management tools leveraging emerging Web technologies. The DMTF has developed a core set of standards that make up WBEM:
 - ♦ A data model: the Common Information Model (CIM) standard
 - ♦ An encoding specification: CIM-XML Encoding Specification
 - ♦ A transport mechanism: CIM Operations over HTTP
- ♦ **The Common Information Model (CIM):** Is a conceptual information model for describing management that is not bound to a particular implementation. This allows for the interchange of management information between management systems and applications. This can be either agent-to-manager or manager-to-manager communications that provide for distributed system management. There are two parts to CIM: the CIM Specification and the CIM Schema.
 - ♦ The CIM Specification describes the language, naming, and meta schema. The meta schema is a formal definition of the model. It defines the terms used to express the model and their usage and semantics. The elements of the meta schema are Classes, Properties, and Methods. The meta schema also supports Indications and Associations as types of Classes, and References as types of Properties.
 - ♦ The CIM Schema provides the actual model descriptions. The CIM Schema supplies a set of classes with properties and associations that provide a well understood conceptual framework within which it is possible to organize the available information about the managed environment.
- ♦ **The Common Information Model Object Manager (CIMOM)** is a CIM object manager or, more specifically, an application that manages objects according to the CIM standard.
- ♦ **CIMOM Providers:** Are software that performs specific tasks within the CIMOM that are requested by client applications. Each provider instruments one or more aspects of the CIMOM's schema.

The packages contained in the Web-based Enterprise Management pattern in the Primary Functions category include a set of basic Novell providers, including some sample providers, and a base set of accompanying Novell schemas.

SLES 11 provides SFCB as default CIMOM and CIM clients. OES 11 uses these because they are part of the base OS.

L.2 OES CIM Providers

Package (RPM)	Description
novell-afp-providers	Used by the Novell AFP iManager plug-in (novell-plugin-afptcpd) to read and edit configuration parameters in the <code>afptcpd.conf</code> , <code>afpvols.conf</code> and <code>afpdirctx.conf</code> files, and to start or stop the AFP server.
novell-hms-providers	Used by Novell Remote Manager (NRM) HMS (Health Monitoring Services) in conjunction with the sblim-cmpi-base providers to obtain data and status for CPU utilization, process count, physical memory, swap memory, virtual memory, and LAN collisions.
novell-lum-providers	Used by the Linux User Management iManager plug-in (novell-usermanagement-imanager-plugin) to read lum configuration from <code>/etc/nam.conf</code> and lum enabled services information from <code>/etc/pam.d</code>
novell-nss-admin-session-sfcb-provider	A set of Linux Instrumentation for Enterprise (LIFE) providers that the Storage iManager plug-in uses to access OES storage subsystem through the SFCB CIMOM. The Storage plug-in is common to NSS, CIFS, and Archive and Version Services.
novell-sms-cmpi-provider	<p>Reads and modifies the SMS configuration files and is also used for administration of NSS, CIFS, NCS, and DFS.</p> <p>The providers are compiled and located in the <code>/opt/novell/lib64/sfcb/cmpi</code> folder.</p>
Novell-samba-cim	Used by the Samba iManager plug-in (novell-plugin-samba) to read and modify the Samba configuration file (<code>smb.conf</code>) when shares are created, deleted, or modified.

L.3 SFCB Is Automatically Installed with OES 11 SP2

When you install any OES components that depend on WBEM, SFCB and all of its corresponding packages are installed with the components.

L.4 Coexistence with NRM and iManager in Earlier Releases

The SFCB-based CIM providers in OES 11 SP2 provide the same functionality and management capabilities as the WBEM-based CIM providers in earlier NetWare and OES releases.

iManager plugins and NRM running on NetWare and OES (all versions) work seamlessly with services running on NetWare and OES (all versions).

L.5 SFCB and Linux User Management (LUM)

SFCB is automatically PAM-enabled for LUM as part of OES 11 SP2 installation. Users not enabled for LUM cannot use the CIM providers to manage OES.

L.6 Links to More Information about WBEM and SFCB

For more information about WBEM, CIM, and SFCB, see the following:

- ♦ “Web Based Enterprise Management” (http://www.suse.com/documentation/sles11/book_sle_admin/data/cha_wbem.html) in the SLES 11 documentation (<http://www.suse.com/documentation/sles11/index.html>).
- ♦ Web-Based Enterprise Management (WBEM) standard (<http://www.dmtf.org/standards/wbem>) Web site.
- ♦ Common Information Model (CIM) (<http://www.dmtf.org/standards/cim>) Web site.
- ♦ Small Footprint CIM Broker (SFCB) (<http://sblim.wiki.sourceforge.net/Sfcb>) Web site.

M Documentation Updates

This section summarizes the changes made to this guide since the initial release of Novell Open Enterprise Server 11. For links to summaries prior to OES 11 SP2, see the bottom of this page.

- ♦ [Section M.1, “Summary of Changes—OES 11 SP1,” on page 390](#)
- ♦ [Section M.2, “Summary of Changes—OES 11,” on page 390](#)

February 26, 2015

[Section 6.21.5, “NSS Considerations,” on page 132](#)

Removed the restriction that NSS pools and volumes must be created on only SCSI or Fibre Channel devices.

September 3, 2014

[Chapter 6, “Caveats for Implementing OES 11 SP2 Services,” on page 117](#)

Removed section on ConsoleOne being supported for only GroupWise and .Zenworks.

ConsoleOne is no longer supported for use with any Novell products.

June 4, 2014

[Section 18.5.8, “Troubleshooting Pure-FTPd from Novell,” on page 276](#)

New section.

April 15, 2014

[Table 7-1 on page 134](#)

Removed OES 2 SP2 as a supported upgrade source server.

February 13, 2014

[“iManager Differences on OES” on page 155](#)

New Section.

January 29, 2014

[“What’s New or Changed in OES 11 SP1 January 2014 Patches” on page 19](#)

Added information about the OES 11 SP1 January 2014 Patches release.

January 28, 2014

All

Updated for OES 11 the SP2 release.

M.1 Summary of Changes—OES 11 SP1

This section lists only substantive changes. Link fixes and other non-substantive changes are not listed.

June 26, 2013

[“User Specific Home Directory in eDirectory” on page 269](#) and [“Default Home Directory” on page 269](#)

Clarified configuration requirements.

April 29, 2013

Chapter or Section Changed	Summary of Changes
----------------------------	--------------------

[Section 1.3.8, “eDirectory,” on page 50](#)

New section that mentions the inclusion of the Graphical NDS Repair utility in OES 11 SP1.

This item which was inadvertently omitted during the initial documentation release for OES 11 SP1. We apologize for the confusion and frustration this has caused. Utility documentation is being created and will be posted as soon as possible.

March 20, 2013

Chapter or Section Changed	Summary of Changes
----------------------------	--------------------

[Section 15.4, “Using the Identity Manager 4.0.2 Bundle Edition,” on page 226](#)

Revised section.

M.2 Summary of Changes—OES 11

This section lists only substantive changes. Link fixes and other non-substantive changes are not listed.

August 7, 2012

Chapter or Section Changed	Summary of Changes
----------------------------	--------------------

[“Changing Proxy Passwords Automatically” on page 346](#)

Modified explanation of when password is changed to reflect change coming in next patch release.

July 7, 2012

Chapter or Section Changed	Summary of Changes
“Changing Proxy Passwords Automatically” on page 346	Clarified how often password is changed.

April 24, 2012

Chapter or Section Changed	Summary of Changes
Section 1.4.14, “NCP Server,” on page 70	Replaced section content.

April 19, 2012

Chapter or Section Changed	Summary of Changes
Table E-1 on page 327	Removed the reference to Tomcat Manager, which is a NetWare-only tool.

January 9, 2012

Section	Change
Section 4.5.2, “Preparing the Installation Media,” on page 112	Content updated to reflect the addition of the Automated Upgrade CD .iso image file to download.novell.com .

