opentext™

Open Enterprise Server 24.4
Planning and Implementation Guide

July 2025

Legal Notices

Copyright 2022 - 2025 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide 11

1 Welcome to Open Enterprise Server 24.4 13

2 Planning Your OES Implementation 15

2.1 Plan for eDirectory . . . 15
2.1.1 Installing Into a New Tree . . . 15
2.1.2 Installing Into an Existing Tree . . . 16
2.2 Identify a Purpose for Each Server . . . 16
2.3 Understand Server Requirements . . . 16
2.4 Understand User Restrictions and Linux User Management . . . 16
2.5 Understand Your Installation Options . . . 17
2.5.1 OES Installation Overview . . . 17
2.5.2 About Your Installation Options . . . 18
2.5.3 Use Predefined Server Types (Patterns) When Possible . . . 19

3 Getting and Preparing OES Software 21

3.1 64-Bit Only . . . 21
3.2 Do You Want to Purchase OES or Evaluate It? . . . 21
3.3 Evaluating OES Software . . . 22
3.3.1 Understanding OES Software Evaluation Basics . . . 22
3.3.2 Evaluating OES . . . 22
3.3.3 Installing OES for Evaluation Purposes . . . 22
3.4 Downloading and Preparing OES Software . . . 23
3.4.1 Downloading OES Software from the OpenText Web Site . . . 23
3.4.2 Preparing the Installation Media . . . 24
3.4.3 Installing Purchased Activation Codes after the Evaluation Period Expires . . . 24
3.5 Licensing . . . 24
3.5.1 The OES Licensing Model . . . 24
3.5.2 OES Doesn’t Support NLS . . . 24

4 Installing OES 25

4.1 Installing OES on Physical Servers . . . 25
4.1.1 What's Next . . . 25
4.2 Installing OES Servers in a Xen VM . . . 26
4.3 Installing OES Servers in a KVM Virtual Machine . . . 26

5 Upgrading OES 27

5.1 Supported Upgrade Paths . . . 27
5.2 Planning for OES Upgrade . . . 28
5.2.1 Be Sure to Check the Release Notes . . . 28
5.3 Meeting the Upgrade Requirements . . . 28

5.3.1 Securing Current Data . . . 28
5.3.2 Ensuring That There Is Adequate Storage Space on the Root Partition . . . 29
5.3.3 Preparing the Server You Are Upgrading . . . 29
5.3.4 Checking the Server's DNS Name . . . 29
5.3.5 Ensuring That the Server Has a Server Certificate . . . 29
5.3.6 Changing the Mount Options Before an Upgrade . . . 30
5.3.7 Preparing an Installation Source . . . 30
5.3.8 Synchronizing the OES Configuration Information before Starting an Upgrade . . . 30

6 Migrating Existing Servers and Data 33

6.1 Supported OES Migration Paths . . . 33
6.2 Migration Tools and Purposes . . . 33

7 Virtualization in OES 35

7.1 Graphical Overview of Virtualization in OES . . . 35
7.2 Why Install OES Services on Your VM Host? . . . 36
7.3 Services Supported on VM Hosts and Guests . . . 37
7.4 Xen VMs Need Ext2 for the System /Boot Volume . . . 38

8 Clustering and High Availability 39

8.1 Planning for a Cluster . . . 39
8.1.1 Determining Your Design Criteria . . . 39
8.1.2 Using Cluster Best Practices . . . 40
8.1.3 Planning the LAN Connectivity . . . 40
8.1.4 Planning the Shared Storage Connectivity . . . 42
8.1.5 Planning the Shared Storage Solution . . . 42
8.1.6 Planning the eDirectory Deployment . . . 42
8.1.7 Planning for Shared Storage as Cluster Resources . . . 43
8.1.8 Planning for OES Services as Cluster Resources . . . 44
8.2 Planning for OES Cluster Services . . . 44
8.2.1 Cluster Administration Requirements . . . 45
8.2.2 IP Address Requirements . . . 48
8.2.3 Volume ID Requirements . . . 48
8.2.4 Hardware Requirements . . . 49
8.2.5 Virtualization Environments . . . 49
8.2.6 Software Requirements for Cluster Services . . . 50
8.2.7 Software Requirements for Cluster Resources . . . 59
8.2.8 Shared Disk Configuration Requirements . . . 62
8.2.9 SAN Rules for LUN Masking . . . 65
8.2.10 Multipath I/O Configuration Requirements . . . 65

9 Managing OES 69

9.1 Overview of Management Interfaces and Services . . . 69
9.2 OES Welcome Page . . . 71
9.2.1 The Welcome Site Requires JavaScript, Apache, and Tomcat . . . 71
9.2.2 Accessing the Welcome Web Site . . . 71
9.2.3 The Welcome Web Site Is Available to All Users . . . 72
9.2.4 Administrative Access from the Welcome Web Site . . . 72
9.3 Unified Management Console (UMC) . . . 72
9.4 iManager and Self-Signed Certificates . . . 72

9.5 SSH Services on OES . . . 73
9.5.1 Overview . . . 73
9.5.2 Setting Up SSH Access for LUM-enabled eDirectory Users . . . 74

10 Network Services 77

10.1 TCP/IP . . . 77
10.1.1 Coexistence and Migration Issues . . . 77
10.2 DNS and DHCP . . . 78
10.2.1 DNS Differences Between NetWare and OES . . . 78
10.2.2 DHCP Differences Between NetWare and OES . . . 79
10.3 Time Services . . . 80
10.3.1 Overview of Time Synchronization . . . 81
10.3.2 Planning for Time Synchronization . . . 85
10.3.3 Coexistence and Migration of Time Synchronization Services . . . 88
10.3.4 Implementing Time Synchronization . . . 90
10.3.5 Configuring and Administering Time Synchronization . . . 91
10.3.6 Daylight Saving Time . . . 92
10.4 Discovery Services . . . 92
10.4.1 OpenSLP . . . 92
10.5 SLP . . . 93
10.5.1 Overview . . . 93
10.5.2 Comparing Novell SLP and OpenSLP . . . 95
10.5.3 Setting Up OpenSLP on OES Networks . . . 96
10.5.4 Using Novell SLP on OES Networks . . . 101
10.5.5 TIDs and Other Help . . . 106

11 Storage and File Systems 107

11.1 Overview of OES Storage . . . 107
11.1.1 Databases . . . 107
11.1.2 iSCSI . . . 108
11.1.3 File System Support in OES . . . 108
11.1.4 Storage Basics by Platform . . . 110
11.1.5 Storage Options . . . 111
11.2 Planning OES File Storage . . . 112
11.2.1 Directory Structures . . . 113
11.2.2 File Service Support Considerations . . . 113
11.2.3 General Requirements for Data Storage . . . 113
11.2.4 OES Storage Planning Considerations . . . 113
11.2.5 NSS Planning Considerations . . . 119
11.3 Coexistence and Migration of Storage Services . . . 119
11.3.1 Databases . . . 119
11.3.2 OES File System Options . . . 120
11.4 Configuring and Maintaining Storage . . . 121
11.4.1 Managing Directories and Files . . . 121
11.4.2 Managing NSS . . . 122
11.4.3 Optimizing Storage Performance . . . 124

12 eDirectory, LDAP, NSS AD, and Domain Services for Windows 125

12.1 Overview of Directory Services . . . 125
12.2 eDirectory . . . 126

12.2.1 Installing and Managing eDirectory on OES 126
12.2.2 Planning Your eDirectory Tree 127
12.2.3 eDirectory Coexistence and Migration 127
12.3 LDAP (eDirectory) 128
12.3.1 Overview of eDirectory LDAP Services 128
12.3.2 Planning eDirectory LDAP Services 128
12.3.3 Migration of eDirectory LDAP Services 128
12.3.4 eDirectory LDAP Implementation Suggestions 128
12.4 NSS AD Support 128
12.5 Why Both NSS AD and DSfW? 129
12.6 Domain Services for Windows 129
12.6.1 Graphical Overview of DSfW 129
12.6.2 Planning Your DSfW Implementation 131
12.6.3 Implementing DSfW on Your Network 132

13 Users and Groups 135

13.1 Creating Users and Groups 135
13.2 Linux User Management: Access to Linux for eDirectory Users 135
13.2.1 Overview 136
13.2.2 LUM Changes 140
13.2.3 Planning 140
13.2.4 LUM Implementation Suggestions 141
13.3 Identity Management Services 144
13.4 Using the Identity Manager 4.8 Bundle Edition 144
13.4.1 What Am I Entitled to Use? 144
13.4.2 System Requirements 145
13.4.3 Installation Considerations 145
13.4.4 Getting Started 145
13.4.5 Activating the Bundle Edition 146

14 Access Control and Authentication 149

14.1 Controlling Access to Services 149
14.1.1 Overview of Access Control 150
14.1.2 Planning for Service Access 156
14.1.3 Coexistence and Migration of Access Services 159
14.1.4 Access Implementation Suggestions 159
14.1.5 Configuring and Administering Access to Services 159
14.2 Authentication Services 161
14.2.1 Overview of Authentication Services 161
14.2.2 Authentication Coexistence and Migration 163

15 Backup Services 165

15.1 Services for End Users 165
15.2 System-Wide Services 165
15.2.1 List of Backup Software 165
15.2.2 Storage Management Services (SMS) 165
15.2.3 SLES 15 Backup Services 166

16 File Services **167**

16.1 Overview of File Services 167
16.1.1 Using the File Services Overviews 167
16.1.2 FTP Services. 167
16.1.3 NetWare Core Protocol 168
16.1.4 CIFS 169
16.2 Planning for File Services 171
16.2.1 Deciding Which Components Match Your Needs 171
16.2.2 Comparing Your CIFS File Service Options 171
16.2.3 Planning Your File Services. 172
16.3 Coexistence and Migration of File Services 173
16.3.1 Client for Open Enterprise Server (NCP) 173
16.3.2 CIFS 173
16.4 Aligning NCP and POSIX File Access Rights 174
16.4.1 Managing Access Rights 174
16.4.2 Providing a Private Work Directory 175
16.4.3 Providing a Group Work Area 176
16.4.4 Providing a Public Work Area 176
16.4.5 Setting Up Rights Inheritance 177
16.5 FTP (Pure-FTPd) and OES. 177
16.5.1 Planning for Pure-FTPd. 178
16.5.2 Installing Pure-FTPd 178
16.5.3 Home Directory Support in Pure-FTPd 178
16.5.4 Configuring Pure-FTPd on an OES Server 179
16.5.5 Configuring Pure-FTPd for Secure Connections with TLS 179
16.5.6 Administering and Managing Pure-FTPd on an OES Server 181
16.5.7 Cluster Enabling Pure-FTPd in an OES Environment 186
16.5.8 SMB Access for eDirectory Users 187
16.5.9 Migrating Pure-FTPd From NetWare to Linux 187
16.6 NCP Implementation and Maintenance. 187
16.6.1 The Default NCP Volume 188
16.6.2 Creating NCP Home and Data Volume Pointers 188
16.6.3 Assigning File Trustee Rights 188
16.6.4 NCP Caveats 188
16.6.5 NCP Maintenance 189
16.7 OES CIFS Implementation and Maintenance 189
16.7.1 Implementing OES CIFS File Services 189
16.7.2 Maintaining OES CIFS File Services 189

17 Print Services **191**

17.1 Overview of Print Services 191
17.1.1 Using This Overview 191
17.1.2 iPrint Components 192
17.1.3 iPrint Functionality 192
17.2 Planning for Print Services 194
17.3 Coexistence and Migration of Print Services 194
17.4 Print Services Implementation Suggestions 194
17.4.1 Initial Setup 194
17.4.2 Other Implementation Tasks 195
17.5 Print Services Maintenance Suggestions 196

18 Web Services **197**

19 Security **199**

19.1 Overview of OES Security Services 199
19.1.1 Application Security (AppArmor) 199
19.1.2 NSS Auditing Engine 199
19.1.3 Encryption (NICI) 200
19.1.4 General Security Issues 201
19.2 Planning for Security 201
19.2.1 Comparing the Linux and the OES Trustee File Security Models 201
19.2.2 User Restrictions: Some OES Limitations 203
19.2.3 Ports Used by OES 204
19.2.4 Configuring and Administering Security 206
19.3 OES and Security Scanners 206
19.4 Links to Product Security Considerations 206
19.5 List of Antivirus Software 207
19.6 TLS Version Support 207

20 Certificate Management **209**

A Product Improvement **211**

A.1 Overview 211
A.2 Data That is Collected for Product Improvement 212
A.3 How the Server Receives the Data 217

B OES Dashboard **219**

B.1 Overview 219
B.2 Prerequisites 219

C Adding Services to OES Servers **221**

D Changing an OES Server's IP Address **223**

D.1 Caveats and Disclaimers 223
D.2 Prerequisites 223
D.2.1 General 223
D.2.2 iPrint 224
D.2.3 Clustering 224
D.3 Changing the Server's Address Configuration 224
D.4 Reconfiguring the OES Services 224
D.5 Repairing the eDirectory Certificates 225
D.6 Completing the Server Reconfiguration 225
D.6.1 DHCP 226
D.6.2 iPrint 226
D.7 Modifying a Cluster 226
D.8 Reconfiguring Services on Other Servers That Point to This Server 226

E Updating/Patching OES Servers 227

F Quick Reference to OES User Services 229

G OES Browser Support 231

H Client/Workstation OS Support 233

I OES Service Scripts 235

J System User and Group Management in OES 239

J.1 About System Users and Groups 239
J.1.1 Types of OES System Users and Groups 239
J.1.2 OES System Users and Groups by Name 240
J.2 Understanding Proxy Users 241
J.2.1 What Are Proxy Users? 241
J.2.2 Why Are Proxy Users Needed on OES? 242
J.2.3 Which Services Require Proxy Users and Why? 242
J.2.4 What Rights Do Proxy Users Have? 243
J.3 Common Proxy User 244
J.3.1 Common Proxy User FAQ 244
J.3.2 Managing Common Proxy Users 247
J.4 Planning Your Proxy Users 248
J.4.1 About Proxy User Creation 248
J.4.2 There Are No Proxy User Impacts on User Connection Licenses 251
J.4.3 Limiting the Number of Proxy Users in Your Tree 251
J.4.4 Password Management and Proxy Users 253
J.5 Implementing Your Proxy User Plan 255
J.5.1 Tree-Wide Proxy Users 256
J.5.2 Service-Specific Proxy Users 256
J.5.3 Partition-Wide Proxy Users 256
J.5.4 Server-Wide Proxy User 257
J.5.5 Individual Proxy User Per-Server-Per-Service 257
J.6 Proxy Users and Domain Services for Windows 257
J.7 System Users 257
J.8 System Groups 258
J.9 Auditing System Users 259

K Administrative Users and Groups in OES 261

K.1 eDirectory Administrative Users and Groups 261
K.2 Active Directory Administrative Users and Groups 261

L Coordinating Password Policies Among Multiple File Services 263

L.1 Overview 263
L.2 Concepts and Prerequisites 263
L.2.1 Prerequisites for File Service Access 263
L.2.2 eDirectory contexts 264
L.2.3 Password Policies and Assignments 264

L.3 Examples . . . 264
L.3.1 Example 1: Complex Mixed Tree with a Mix of File Access Services and Users from across the Tree . . . 264
L.3.2 Example 2: Mutually Exclusive Users . . . 266
L.4 Deployment Guidelines for Different Servers and Deployment Scenarios . . . 267
L.4.1 Deployment Scenario 1: Complex Mixed Scenario with a Mix of File Access Services . . . 267
L.4.2 Deployment Scenario 2: Mutually /Exclusive Users . . . 269
L.4.3 Deployment Scenario 3: Simple deployments . . . 269
L.4.4 Modifying User Password Policies after Samba/DSfW Is Installed . . . 269
L.4.5 Adding New User eDirectory Contexts to CIFS after CIFS/DSfW Is Installed . . . 269
L.4.6 Enabling File Access for DSfW Servers Across Domains . . . 270

M Configuration and Log Files 271

M.1 CIFS . . . 271
M.2 CIS . . . 272
M.3 Common Proxy . . . 272
M.4 DFS . . . 273
M.5 DHCP . . . 273
M.6 DNS . . . 273
M.7 Domain Services for Windows . . . 274
M.8 Pure-FTPd . . . 276
M.9 Install . . . 276
M.10 iPrint . . . 277
M.11 Linux User Management . . . 278
M.12 Migration Tool . . . 278
M.13 Cluster Services . . . 280
M.14 OES File Access Rights Management (NFARM) . . . 280
M.15 Novell Identity Translator (NIT) . . . 281
M.16 Linux Volume Manager (NLVM) . . . 281
M.17 Storage Services . . . 281
M.18 novell-ad-util . . . 282
M.19 NCP . . . 282
M.20 SMS . . . 283
M.21 Vigil . . . 284

N Small Footprint CIM Broker (SFCB) 285

N.1 Overview . . . 285
N.2 OES CIM Providers . . . 286
N.3 SFCB Is Automatically Installed with OES . . . 286
N.4 Coexistence with NRM and iManager in Earlier Releases . . . 286
N.5 SFCB and Linux User Management (LUM) . . . 287
N.6 Links to More Information about WBEM and SFCB . . . 287

About This Guide

- Chapter 1, “Welcome to Open Enterprise Server 24.4,” on page 13
- Chapter 2, “Planning Your OES Implementation,” on page 15
- Chapter 3, “Getting and Preparing OES Software,” on page 21
- Chapter 4, “Installing OES,” on page 25
- Chapter 5, “Upgrading OES,” on page 27
- Chapter 6, “Migrating Existing Servers and Data,” on page 33
- Chapter 7, “Virtualization in OES,” on page 35
- Chapter 8, “Clustering and High Availability,” on page 39
- Chapter 9, “Managing OES,” on page 69
- Chapter 10, “Network Services,” on page 77
- Chapter 11, “Storage and File Systems,” on page 107
- Chapter 12, “eDirectory, LDAP, NSS AD, and Domain Services for Windows,” on page 125
- Chapter 13, “Users and Groups,” on page 135
- Chapter 14, “Access Control and Authentication,” on page 149
- Chapter 15, “Backup Services,” on page 165
- Chapter 16, “File Services,” on page 167
- Chapter 17, “Print Services,” on page 191
- Chapter 18, “Web Services,” on page 197
- Chapter 19, “Security,” on page 199
- Chapter 20, “Certificate Management,” on page 209
- Appendix A, “Product Improvement,” on page 211
- Appendix B, “OES Dashboard,” on page 219
- Appendix C, “Adding Services to OES Servers,” on page 221
- Appendix D, “Changing an OES Server’s IP Address,” on page 223
- Appendix E, “Updating/Patching OES Servers,” on page 227
- Appendix F, “Quick Reference to OES User Services,” on page 229
- Appendix G, “OES Browser Support,” on page 231
- Appendix H, “Client/Workstation OS Support,” on page 233
- Appendix I, “OES Service Scripts,” on page 235
- Appendix J, “System User and Group Management in OES,” on page 239
- Appendix K, “Administrative Users and Groups in OES,” on page 261
- Appendix L, “Coordinating Password Policies Among Multiple File Services,” on page 263

- Appendix M, “Configuration and Log Files,” on page 271
- Appendix N, “Small Footprint CIM Broker (SFCB),” on page 285

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 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 24.4. Please use the `comment on this topic` feature at the bottom of each page on the online documentation.

Additional Documentation

Additional documentation is found on the OES 24.4 Documentation Web site.

Documentation Conventions

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

1 Welcome to Open Enterprise Server 24.4

OpenText Open Enterprise Server delivers all the enterprise-class networking, file, and print services that enterprises have relied on for years. OES provides valuable benefits including power savings, virtualization, manageability, and interoperability.

OES provides several new features that reduce administrative complexities and provide access to file and storage services regardless of eDirectory as an identity source. For information about the new features, see What's New in the Release Notes.

The support for the add-on install is deprecated and OES is installed only through integrated install media. For more information on OES integrated install procedure, see OES: Installation and Upgrade Guide.

2 Planning Your OES 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 2.1, “Plan for eDirectory,” on page 15
- Section 2.2, “Identify a Purpose for Each Server,” on page 16
- Section 2.3, “Understand Server Requirements,” on page 16
- Section 2.4, “Understand User Restrictions and Linux User Management,” on page 16
- Section 2.5, “Understand Your Installation Options,” on page 17

2.1 Plan for eDirectory

eDirectory is the heart of OES network services and security.

- Section 2.1.1, “Installing Into a New Tree,” on page 15
- Section 2.1.2, “Installing Into an Existing Tree,” on page 16

2.1.1 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 Administration Guide*.
- **Time synchronization:** eDirectory requires that all servers, be time synchronized. For more information, see Chapter 10.3, “Time Services,” on page 80.
- **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 Administration Guide*.

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

2.1.2 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 12.2.3, “eDirectory Coexistence and Migration,” on page 127.

2.2 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 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.

2.3 Understand Server Requirements

OES 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 24.4 Server (Physical):** “Preparing to Install OES” in the *Installation Guide*.
- **OES 24.4 Server (Virtual):** “System Requirements” in the *Installation Guide*.

2.4 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 19.2.2, “User Restrictions: Some OES Limitations,” on page 203.

2.5 Understand Your Installation Options

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

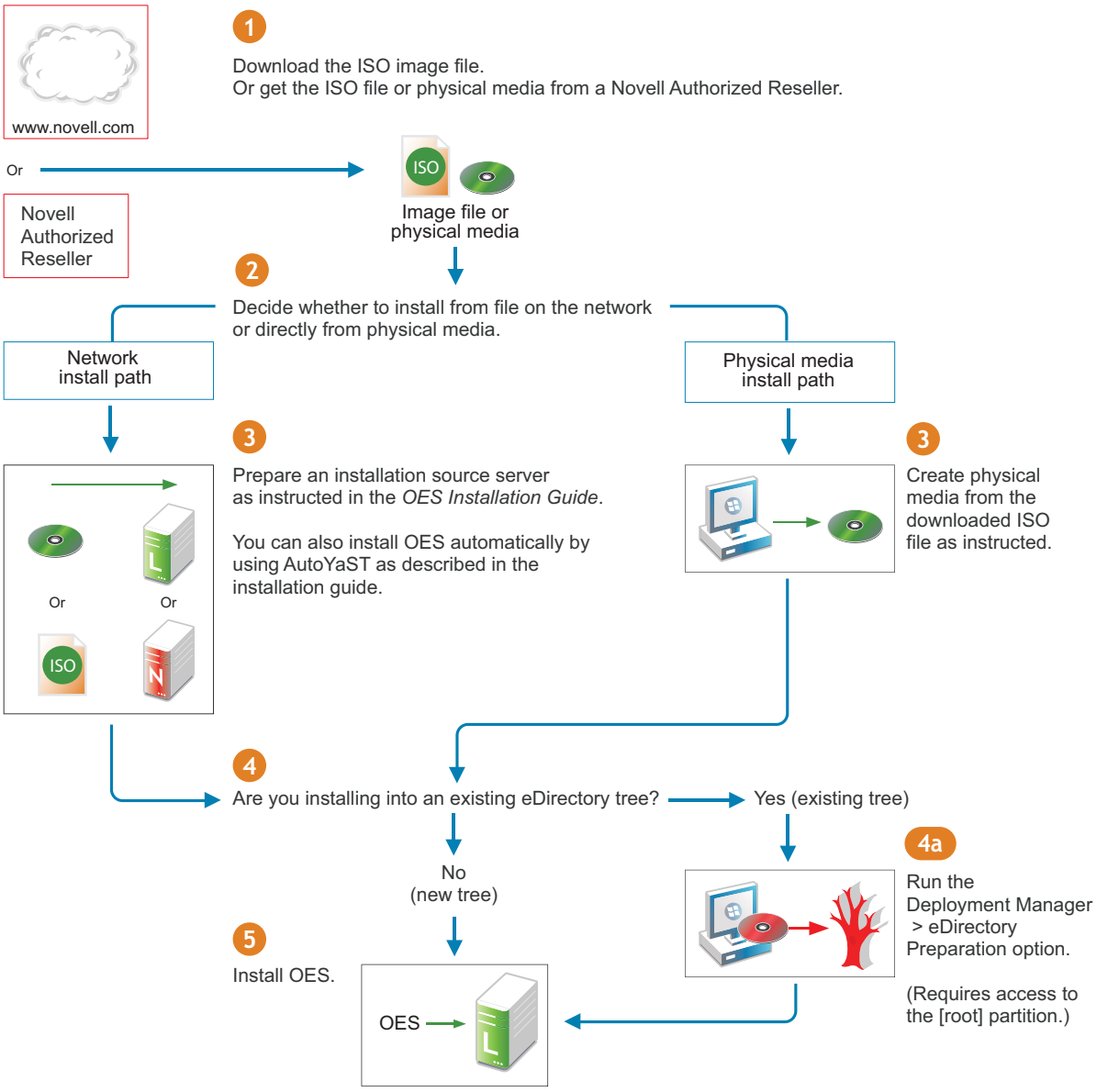
- Section 2.5.1, “OES Installation Overview,” on page 17
- Section 2.5.2, “About Your Installation Options,” on page 18
- Section 2.5.3, “Use Predefined Server Types (Patterns) When Possible,” on page 19

2.5.1 OES Installation Overview

The software and network preparation processes required to install OES are outlined in Figure 2-1.

NOTE: Chapter 3, “Getting and Preparing OES Software,” on page 21 contains instructions for obtaining the ISO image files referred to in the following illustration.

Figure 2-1 *OES Install Preparation*



For detailed instructions, see "Setting Up a Network Installation Source" in the *Installation Guide*.

For information about preparing the tree, see "OES eDirectory Rights Needed for Installing OES" and "Preparing eDirectory for OES" in the *Installation Guide*.

2.5.2 About Your Installation Options

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

- "OES 24.4 Options" on page 19
- "Virtual Machine Installation Options" on page 19

OES 24.4 Options

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

- **OES Install Media:** You can install OES from a single ISO or DVD obtained from a OpenText Authorized Reseller or created from a downloaded ISO image file.

  See "Preparing Physical Media for a New Server Installation" in the *Installation Guide*.

- **DVD Install:** You can install OES by using a DVD obtained from a OpenText Authorized Reseller or created from downloaded ISO image files.

  See "Preparing Physical Media for a New Server Installation" in the *Installation Guide*.

- **Network Install:** You can install from the network by using the NFS, FTP, or HTTP protocol.

  See "Setting Up a Network Installation Source" in the *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 *Installation Guide*.

Virtual Machine Installation Options

Virtual machine installations offer additional options. For more information, see "Installing OES on a VM" in the *Installation Guide*.

2.5.3 Use Predefined Server Types (Patterns) When Possible

OES 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 server that provides enterprise level print services, you should select the **OES iPrint** 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 server with only the service components you need.

More information about server patterns is available in "OES Services Pattern Descriptions" in the *Installation Guide*.

3 Getting and Preparing OES Software

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

- Section 3.1, “64-Bit Only,” on page 21
- Section 3.2, “Do You Want to Purchase OES or Evaluate It?,” on page 21
- Section 3.3, “Evaluating OES Software,” on page 22
- Section 3.4, “Downloading and Preparing OES Software,” on page 23
- Section 3.5, “Licensing,” on page 24

If you have not already done so, we recommend that you review the information in Section 2.5, “Understand Your Installation Options,” on page 17.

3.1 64-Bit Only

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

OES is a set of services available in 64-bit only.

3.2 Do You Want to Purchase OES or Evaluate It?

If you want to evaluate OES prior to purchasing it, skip to the next section, Evaluating OES Software.

If you have decided to purchase OES, visit the OpenText Product Inquiry page (https://www.microfocus.com/en-us/products/open-enterprise-server/contact).

When you purchase OES, you receive an activation code. This code is required for registering an OES system in the 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 licensing model. For a brief description, see Section 3.5, “Licensing,” on page 24.

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 2.5, “Understand Your Installation Options,” on page 17 and then skip to Chapter 4, “Installing OES,” on page 25.

3.3 Evaluating OES Software

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

- Section 3.3.1, “Understanding OES Software Evaluation Basics,” on page 22
- Section 3.3.2, “Evaluating OES,” on page 22
- Section 3.3.3, “Installing OES for Evaluation Purposes,” on page 22

3.3.1 Understanding OES Software Evaluation Basics

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

Briefly, the evaluation period for OES servers is 60 days. To receive software updates during this time, you must have or create an account with the Customer Center, receive evaluation code for OES while downloading the software, and use this code to register your server. No software updates can be downloaded after the 60-day evaluation period expires until you purchase the product.

3.3.2 Evaluating OES

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

If you have decided to purchase OES, visit the OpenText Product Inquiry page (https://www.microfocus.com/en-us/products/open-enterprise-server/contact).

3.3.3 Installing OES for Evaluation Purposes

After completing the instructions in Section 3.4.1, “Downloading OES Software from the OpenText Web Site,” on page 23, you will have an activation/evaluation code for OES. As you install OES, you should register with the Customer Center and use this code to enable your server for online updates from the OES patch channels.

IMPORTANT: Always download the current patches during an installation.

Instructions for using the activation codes during an installation are found in “Specifying Customer Center Configuration Settings” in the *Installation Guide*.

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

3.4 Downloading and Preparing OES Software

- Section 3.4.1, “Downloading OES Software from the OpenText Web Site,” on page 23
- Section 3.4.2, “Preparing the Installation Media,” on page 24
- Section 3.4.3, “Installing Purchased Activation Codes after the Evaluation Period Expires,” on page 24

3.4.1 Downloading OES Software from the OpenText Web Site

If you already have OES ISO image files, skip to Section 3.4.2, “Preparing the Installation Media,” on page 24.

If you have OES product media, skip to Section 3.3.3, “Installing OES for Evaluation Purposes,” on page 22.

To download ISO image files from the Web:

1. Login to Software Licenses and Downloads (SLD) website or if you don’t have a OpenText account, create an account.
2. Click **Search Account** and select your account.
3. Click **Downloads** and select the product as **Open Enterprise Server 24.4**, product name depending on your license type and version as **24.4**.
4. In the **Description** column, mouseover **Reference Material** and click **Readme** to view the `.iso` name and the new features in the release.
5. In the **Action** column, mouseover **More Details** to view the `.iso` name and checksum value.
6. In the **Action** column, click **Download** to download the `.iso` file.
7. If you have purchased OES previously and received your OES activation codes, skip to Step 9.

   Otherwise, in the **Evaluating Open Enterprise Server 24.4** section, click the **Get Activation Codes** link in the **Open Enterprise Server 24.4** paragraph.

   60-day evaluation codes are sent in separate e-mail messages to the e-mail address associated with your OpenText account.
8. Access your e-mail account and print the messages or write down the activation codes.

   OES code is required for product registration and downloading software updates.
9. Verify the integrity of each downloaded file by running an MD5-based checksum utility on it and comparing the values against the value displayed in Step 5.

   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.
10. (Optional) If you plan to install OES from files on your network, see the instructions in “Setting Up a Network Installation Source” in the *Installation Guide*.

3.4.2 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 9 on page 23. 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 *Installation Guide*.

3.4.3 Installing Purchased Activation Codes after the Evaluation Period Expires

After purchasing Open Enterprise Server, use the instructions in "Registering the Server in the Customer Center Using the Command Line" in the *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.

3.5 Licensing

This section explains the following:

- Section 3.5.1, "The OES Licensing Model," on page 24
- Section 3.5.2, "OES Doesn't Support NLS," on page 24

3.5.1 The OES Licensing Model

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

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

For more information on OES licensing, see the following:

- EULA (https://www.microfocus.com/media/documentation/micro_focus_end_user_license_agreement.pdf)
- Additional License Authorizations (https://www.microfocus.com/media/documentation/additional-license-authorization-for-collaboration-solutions-products-documentation.pdf)

3.5.2 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.

4 Installing OES

IMPORTANT: Before you install Open Enterprise Server, ensure to review the information in Chapter 2, “Planning Your OES Implementation,” on page 15.

This section briefly covers the following:

- Section 4.1, “Installing OES on Physical Servers,” on page 25
- Section 4.2, “Installing OES Servers in a Xen VM,” on page 26
- Section 4.3, “Installing OES Servers in a KVM Virtual Machine,” on page 26

4.1 Installing OES on Physical Servers

The OES installation leverages the SUSE Linux YaST graphical user interface.

To ensure a successful installation:

1. Read and follow all instructions in the *Release Notes*.
2. Carefully follow the instructions in the *Installation Guide*, especially those found in
   - “Preparing to Install OES”
   - “Installing OES 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 Services on an Existing OES Server” in the *Installation Guide*.

4.1.1 What's Next

The various service sections in this guide contain information about completing your OES services implementation. See the sections for the services you have installed, beginning with Chapter 9, “Managing OES,” on page 69.

4.2 Installing OES Servers in a Xen VM

Installing OES servers on a Xen virtual machine involves installing an OES or SUSE Linux Enterprise Server (SLES) 15 SP4 VM host server, creating a VM, and then installing an OES server in the VM.

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

- "Introduction to Xen Virtualization" in the *Virtualization Guide*.
- "Installing OES on a VM" in the *Installation Guide*.

4.3 Installing OES Servers in a KVM Virtual Machine

Installing OES servers on a KVM virtual machine involves installing an OES or SUSE Linux Enterprise Server (SLES) 15 SP4 VM host server, creating a VM, and then installing an OES server in the VM.

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

- "Introduction to KVM Virtualization" in the *Virtualization Guide*.
- "Installing OES on a VM" in the *Installation Guide*.

5 Upgrading OES

Open Enterprise Server (OES) provides the option of updating an existing system to the new version without completely reinstalling it. No new installation is needed. Existing data such as home directories and system configuration is kept intact. During the life cycle of the product, you can apply Service Packs to increase system security and correct software defects.

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

- Section 5.1, “Supported Upgrade Paths,” on page 27
- Section 5.2, “Planning for OES Upgrade,” on page 28
- Section 5.3, “Meeting the Upgrade Requirements,” on page 28

5.1 Supported Upgrade Paths

The following table lists the supported upgrade paths for OES 25.3:

Table 5-1 *Supported Paths for Upgrading OES*

Source Version	Supported Methods	Additional Information
OES 24.4, OES 24.4.1, OES 25.1, or OES 25.2	Patch update NCC Subscription Management Tool (SMT) SUSE Manager ZENworks	Before update, you must register to NCC, SMT, SUSE Manage, or ZENworks.
OES 23.4, OES 24.1, OES 24.2, OES 24.3, OES 24.3.1, OES 24.3.2, or OES 24.3.3	Physical Media (OES 24.4) AutoYaST SUSE Manager ZENworks	Before upgrade, you must register to NCC, SMT, SUSE Manager, or ZENworks.
OES 24.3.3	Channel Upgrade	Before upgrade, you must register to NCC or SMT.
OES 2023 with the latest patch	Physical Media (OES 24.4) AutoYaST	Before upgrade, you must register to NCC or SMT.
OES 2018 SP3 (64-bit) with the latest patch	Physical Media (OES 24.4) AutoYaST	Before upgrade, you must register to NCC or SMT.

IMPORTANT: Source servers must have all patches applied from the appropriate SUSE Linux Enterprise Server (SLES) and OES patch update repositories prior to an upgrade.

Other OES releases can be upgraded by installing the interim OES version. For example, to upgrade from OES 2015 SP1 to OES 2023 or OES 23.4, you need to upgrade to OES 2018 SP3 first, and then upgrade from OES 2018 SP3 to OES 2023 or OES 23.4.

5.2 Planning for OES Upgrade

- Section 5.2.1, “Be Sure to Check the Release Notes,” on page 28

5.2.1 Be Sure to Check the Release Notes

The Release Notes documents issues that OpenText plans to address in a future release.

5.3 Meeting the Upgrade Requirements

Meet the following requirements before you upgrade and install any OES components:

- Section 5.3.1, “Securing Current Data,” on page 28
- Section 5.3.2, “Ensuring That There Is Adequate Storage Space on the Root Partition,” on page 29
- Section 5.3.3, “Preparing the Server You Are Upgrading,” on page 29
- Section 5.3.4, “Checking the Server’s DNS Name,” on page 29
- Section 5.3.5, “Ensuring That the Server Has a Server Certificate,” on page 29
- Section 5.3.6, “Changing the Mount Options Before an Upgrade,” on page 30
- Section 5.3.7, “Preparing an Installation Source,” on page 30
- Section 5.3.8, “Synchronizing the OES Configuration Information before Starting an Upgrade,” on page 30

5.3.1 Securing Current Data

Before upgrading, secure the current data on the server. For example, make a backup copy of the data so that you can restore the data volumes later if needed.

Save your configuration files. Copy all configuration files to a separate medium, such as a removable hard disk or USB stick, to secure the data. This primarily applies to files stored in `/etc` as well as some of the directories and files in `/var` and `/opt`. You might also want to write the user data in `/home` (the Home directories) to a backup medium. Back up this data as `root`. Only `root` has read permission for all local files.

5.3.2 Ensuring That There Is Adequate Storage Space on the Root Partition

Before starting your upgrade, make note of the root partition and space available.

If you suspect you are running short of disk space, secure your data before updating and repartition your system. There is no general rule regarding how much space each partition should have. Space requirements depend on your particular partitioning profile and the software selected.

The `df -h` command lists the device name of the root partition. In the following example, the root partition to write down is `/dev/sda2` (mounted as `/`) with 5.8 GB available.

```
blr8:/media # df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda2       9.9G  3.7G  5.8G  39% /
devtmpfs        940M  124K  940M   1% /dev
tmpfs           940M  244K  940M   1% /dev/shm
admin           4.0M     0  4.0M   0% /_admin
```

5.3.3 Preparing the Server You Are Upgrading

Ensure that the server meets the hardware requirements for OES. See Server Hardware in the Installation Guide.

Itanium is not a supported platform for OES.

If the server is running supported source version mentioned in Section 5.1, “Supported Upgrade Paths,” on page 27, complete the following steps before upgrading the server:

1. Run **YaST** > **Software** > **Online Update** to patch the OES source server to the latest patch level.
2. Ensure that the server and services are still running as desired.
3. Upgrade to OES 24.4 using the instructions in Upgrading OES section, then apply all patches and verify services.

5.3.4 Checking the Server’s DNS Name

Ensure that DNS returns the correct static IP address when you ping the server's full DNS name. For example,

```
ping myserver.example.com
```

5.3.5 Ensuring That the Server Has a Server Certificate

IMPORTANT: Most OES servers have either an eDirectory certificate or a third-party certificate installed.

These instructions only apply when that is not the case.

Ensure that the server has a server certificate that has been generated and exported as a Common Server certificate.

To check for or add a certificate:

1. Launch YaST.
2. Click **Security and Users** > **CA Management**.
3. If no certificate authorities (CAs) are listed, create one by clicking **Create Root CA**.

   If a CA is listed, you can use it by selecting the CA and clicking **Enter CA**.
4. If you are using a listed CA, you must provide the CA password (generally the root password).
5. Click **Certificates** > **Add**.
6. Fill out the forms required for a server certificate. After the last form is complete, a server certificate is created and listed in the certificate list.
7. Select the certificate you just created.
8. Click the **Export** button, then select **Export as Common Server Certificate**.

5.3.6 Changing the Mount Options Before an Upgrade

Before starting the upgrade, ensure that the mount options for all the partitions are set to **UUID**.

If the mount options are incorrect, use the following procedure to select the applicable one:

1. Log on to the OES server with root privileges.
2. In the terminal, type `yast2 disk`.
3. In the **Warning** dialog box, click **Yes**
4. In the **Expert Partitioner** window, select a partition, such as **root(/)**, then click **Edit > Fstab Options**.
5. Under **Fstab options:**, click **UUID > OK > Finish**.

   IMPORTANT: If you plan to clone your hard disks in the future, do not select **Device ID** `root` as mount option. The cloning process will fail. For more information, see "New default in SLES/SLED 10 SP1: mount "by Device ID".
6. Repeat Step 4 and Step 5 on page 30 or all the Linux partitions (not for NSS partitions).
7. After you have changed the mount options, click **Next**.
8. In the **Expert Petitioner: Summary** dialog box, click **Finish**.

The mount options are successfully changed.

5.3.7 Preparing an Installation Source

Review and complete the instructions for Setting Up a Network Installation Source in the Installation Guide. We recommend using the network installation option, especially if you are upgrading multiple servers.

5.3.8 Synchronizing the OES Configuration Information before Starting an Upgrade

- Ensure that the LDAP servers configured for OES are up and running.

Each of these servers is represented through a file (named after its IP address) in `/etc/sysconfig/novell/ldap_servers`. There can also be a second file named after the DNS name of the server.

When a server that has been used as an LDAP server for OES is retired these files are left behind and must be removed.

- The modifications that you make to an OES server using YaST are stored in the configuration files at `/etc/syconfig/novell`. These crucial configuration information is used to upgrade an OES server.
- You can also modify an OES server outside of YaST, and those changes are stored as part of the respective service configuration files. In this scenario, if you upgrade the OES server, your latest changes will not be part of the upgrade or the upgrade might fail. This happens because your latest changes are not captured as part of the configuration information at `/etc/syconfig/novell`.

  To synchronize the latest changes that you have done outside of YaST, use the upgrade check script (`/opt/novell/oes-install/util/oes_upgrade_check.pl`) that is available with the OES server. This script assumes that the respective OES service configuration file information is the latest and updates this configuration information to the `/etc/sysconfig/novell/`*`service_release`*.

  For example, if you have modified LUM outside of YaST, LUM configuration information is stored in the LUM configuration file at `/etc/nam.conf`. When you run the `oes_upgrade_check.pl` script, the upgrade script compares the LUM configuration information at `/etc/sysconfig/novell/lum_oes2018` against `/etc/nam.conf`. If there is a mismatch, the LUM configuration information from `/etc/nam.conf` is synchronized with `/etc/sysconfig/novell/lum_oes2018`.

  Syntax: `./oes_upgrade_check.pl <`*`all | OES service name`*`>`

  OES service names include `lum, edir, cifs, iprint, dhcp, ncs, nss,` and `dsfw`.

  Examples:

  - To synchronize all the individual OES service configuration information with `/etc/syconfig/novell`, execute the `./oes_upgrade_check.pl` all command.
  - To synchronize any particular OES service configuration information, for example LUM, with `/etc/syconfig/novell`, execute the `./oes_upgrade_check.pl lum` command.

6 Migrating Existing Servers and Data

This section briefly outlines the following migration topics:

- Section 6.1, “Supported OES Migration Paths,” on page 33
- Section 6.2, “Migration Tools and Purposes,” on page 33

6.1 Supported OES Migration Paths

For a complete list of Open Enterprise Server migration scenarios and paths, see “Migration Scenarios” in the *Migration Tool Administration Guide*.

6.2 Migration Tools and Purposes

The OES Migration Tool lets you migrate and/or consolidate data and services from one or more OES source servers to an OES target server. See “Source Platform Support for OES Services ” in the *Migration Tool Administration Guide*.

You can also transfer a complete server identity, including its IP address, host name, eDirectory identity, NICI keys, and certificates. For more information, see “Transfer ID ” in the *Migration Tool Administration Guide*.

7 Virtualization in OES

Open Enterprise Server runs as a VM guest on any virtual machine host server that is certified for running SUSE Linux Enterprise Server 15 SP4 (SLES 15 SP4) as a paravirtualized guest. Because Xen and KVM are distributed with SLES, they are mentioned more particularly in the OES documentation.

For a list of the VM host platforms that are certified for SLES, see "Supported VM Host Servers for SLES VM Guests" in the *SLES Virtualization Guide*.

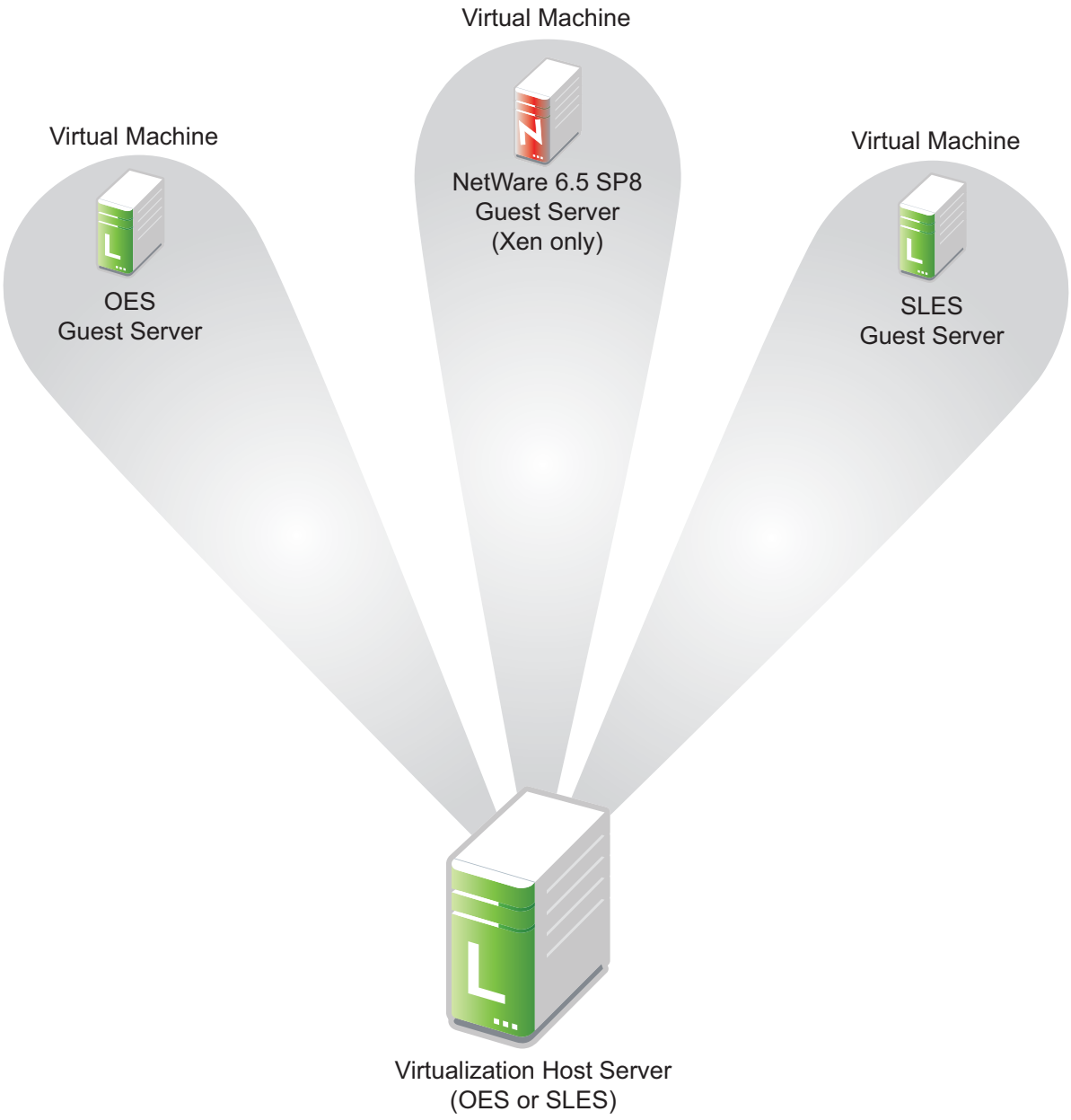
For information about installing and running OES services on virtual machines, see Installation Guide.

- Section 7.1, "Graphical Overview of Virtualization in OES," on page 35
- Section 7.2, "Why Install OES Services on Your VM Host?," on page 36
- Section 7.3, "Services Supported on VM Hosts and Guests," on page 37
- Section 7.4, "Xen VMs Need Ext2 for the System /Boot Volume," on page 38

7.1 Graphical Overview of Virtualization in OES

Figure 7-1 illustrates how a single VM host server can support multiple VM guest servers that in turn provide OES services.

Figure 7-1 *Virtualization in OES*



7.2 Why Install OES Services on Your VM Host?

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

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 9.5.2, "Setting Up SSH Access for LUM-enabled eDirectory Users," on page 74."

- **Storage Management Services (SMS):** Lets you back up VM host server file system data.
- **Cluster Services (NCS):** Lets you cluster the VM host.
- **OpenText iPrint:** Lets you print from the host.

7.3 Services Supported on VM Hosts and Guests

As you plan your virtualization configurations, you will want to consider which services are supported where Table 7-1 and which combinations of services are supported.

Table 7-1 *Services Supported on VM Hosts and Guests*

OES Service	Linux VM Host	OES VM Guest
Backup/SMS	✓	✓
CIFS (OES CIFS)		✓
Cluster Services	✓ (non-NSS and Xen templates only)	✓
DHCP		✓
DNS		✓
Domain Services for Windows (DSfW)		✓
eDirectory		✓
FTP		✓
iManager		✓
iPrint	✓	✓
Linux User Management	✓	✓
NCP Server/Dynamic Storage Technology		✓
OES Remote Manager (NRM)		✓
Storage Services (NSS)		✓

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 *Installation Guide*.

7.4 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.

8 Clustering and High Availability

Open Enterprise Server includes support for a two-node OES Cluster Services cluster.

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

- Can include up to 32 servers.
- 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 *OES Cluster Services for Linux Administration Guide*.

8.1 Planning for a Cluster

The success of your high-availability cluster solution depends on its stability and robustness. Use the guidelines in this section to design your OES Cluster Services cluster and cluster environment.

IMPORTANT: For information about the system requirements for installing and using OES Cluster Services, see Chapter 8, “Clustering and High Availability,” on page 39.

- Section 8.1.1, “Determining Your Design Criteria,” on page 39
- Section 8.1.2, “Using Cluster Best Practices,” on page 40
- Section 8.1.3, “Planning the LAN Connectivity,” on page 40
- Section 8.1.4, “Planning the Shared Storage Connectivity,” on page 42
- Section 8.1.5, “Planning the Shared Storage Solution,” on page 42
- Section 8.1.6, “Planning the eDirectory Deployment,” on page 42
- Section 8.1.7, “Planning for Shared Storage as Cluster Resources,” on page 43
- Section 8.1.8, “Planning for OES Services as Cluster Resources,” on page 44

8.1.1 Determining Your Design Criteria

The purpose of designing a resilient cluster is to ensure that your essential data and services are highly available. Setting up data and services as cluster resources allows them to be moved between nodes in the same cluster. This helps eliminate or minimize the downtime caused by a server failure or maintenance.

You can determine what data and services to set up as cluster resources by asking and answering the following questions:

❒ What are the key services that drive your business?

- ❒ What services are essential for business continuance?
- ❒ What is the cost of downtime for the essential services?
- ❒ Based on their mission-critical nature and cost of downtime, what services are the highest priority for business continuance?
- ❒ What data is necessary to support the highest-priority services?
- ❒ How much data is involved, and how important is it?

8.1.2 Using Cluster Best Practices

Using the following cluster best practices can help you avoid potential problems with your cluster:

- Ensure that eDirectory is stable before implementing a cluster.
- Ensure that you have full Read/Write replicas of the entire eDirectory tree co-located in the data center where you are setting up the cluster.
- Ensure that IP addresses are unique.
- Consistently apply IP address assignments for each cluster and its cluster resources.
- Make IP address changes for the cluster and cluster resources only by using the procedure described in Moving a Cluster or Changing IP Addresses of Cluster Nodes and Resources in the OES Cluster Services for Linux Administration Guide

  IP address changes for cluster resources should always be made on the Protocols page of the iManager Clusters plug-in, not directly in load, unload, and monitor scripts. This is the only way to change the IP address on the virtual NCS:NCP Server object in eDirectory.
- Ensure that Volume IDs used for a cluster resources are unique across all nodes.

  Each cluster node automatically assigns volume ID 0 to volume SYS and volume ID 1 to volume _ADMIN. Cluster-enabled volumes use high volume IDs, starting from 254 in descending order. Volume IDs can be assigned in the cluster load script. You can view the volume IDs assigned on a node by using the `ncpcon volumes` command.

  The Client for Open Enterprise Server uses the volume ID to access a volume.
- Consider each node's configuration requirements for each of the services it is intended to host.
- Create failover matrixes for each cluster resource so that you know what service is supported and which nodes are the preferred nodes for failover.

8.1.3 Planning the LAN Connectivity

The primary objective of LAN connectivity in a cluster is to provide uninterrupted heartbeat communications. Use the guidelines in this section to design the LAN connectivity for the cluster:

- "VLAN" on page 41
- "Channel Bonding" on page 41
- "Spanning Tree Protocol" on page 41
- "IP Addresses" on page 41
- "Name Resolution" on page 41

VLAN

Use a dedicated VLAN (virtual local area network) for each cluster.

The cluster protocol is non-routable, so you cannot direct communications to specific IP addresses. Using a VLAN for the cluster nodes provides a protected environment for the heartbeat process and ensures that heartbeat packets are exchanged only between the nodes of a given cluster.

When you use a VLAN, no foreign host can interfere with the heartbeat. For example, using a VLAN avoids broadcast storms that slow traffic and can result in false split-brain situations.

Channel Bonding

Servers should be redundantly cabled to the network in order to provide LAN fault tolerance, preferably at both the adapter level and the link level. Consider connecting cluster nodes to redundant access switches for fault tolerance.

Use channel bonding for the server adapters. Channel bonding combines Ethernet interfaces on a host computer for redundancy or increased throughput. Higher-level software uses a single virtual-network interface, and the channel bonding driver handles the complex choice of which physical-network interface to use. Channel bonding helps increase the availability of an individual cluster node, which helps avoid or reduce the occurrences of failover caused by slow LAN traffic. See the `/usr/src/linux/Documentation/bonding.txt` document.

Spanning Tree Protocol

Use the Spanning Tree Protocol (STP) to eliminate network topology loops. When you configure STP, ensure that the Portfast Bridge Protocol Data Unit (BPDU) guard feature is enabled, or consider using Rapid Spanning Tree Protocol (RSTP, IEEE 802.11w).

The default settings for STP inhibit the heartbeat for over 30 seconds whenever there is a change in link status. Test your STP configuration with Cluster Services running to ensure that a node is not cast out of the cluster when a broken link is restored.

IP Addresses

Plan your IP address assignment so that it is consistently applied across each cluster. For each cluster, provide a dedicated IP address range with sufficient addresses for the cluster. The addresses do not need to be contiguous.

You need a unique static IP address for each of the following components of a cluster:

- Cluster (master IP address)
- Cluster nodes
- Cluster resources (file system resources and service resources such as DHCP, DNS, SLP, FTP, and so on)

Name Resolution

Ensure that SLP is properly configured for name resolution. See Section 10.5, “SLP,” on page 93.

8.1.4 Planning the Shared Storage Connectivity

The primary objective of the shared storage connectivity in a cluster is to provide solid and stable connectivity between cluster nodes and the storage system. Before installing OES Cluster Services and setting up a cluster, ensure that the storage configuration is established and verified.

Use the guidelines in this section to design the storage connectivity for a cluster:

- Use host-based multipath I/O management. See the following resources:
  - Section 8.2.10, "Multipath I/O Configuration Requirements," on page 65
  - "Managing Multipath I/O for Devices" in the *SLES Storage Administration Guide*
- Connect each node via two fabrics to the storage area network (SAN).
- Use redundant SAN connections to provide fault-tolerant connectivity between the cluster nodes and the shared storage devices.
- Use LUN masking to exclusively assign each LUN to one or more host connections. See Section 8.2.9, "SAN Rules for LUN Masking," on page 65.

8.1.5 Planning the Shared Storage Solution

Use the guidelines in this section to design the shared storage solution for a cluster:

- For maximum flexibility, you should create only one cluster resource per LUN.

  A LUN cannot be concurrently accessed by servers belonging to different clusters. This means that all resources on a given LUN can be active only in a given cluster at any given time.
- You should use only one LUN per pool, and only one volume per pool. If you use multiple LUNs for a given shared NSS pool, all LUNs must fail over together.

  It is possible to create multiple pools per LUN or to use multiple LUNs per pool, but these alternatives are not recommended.

8.1.6 Planning the eDirectory Deployment

Your NetIQ eDirectory solution for each cluster must consider the following configuration elements. Your approach should be consistent across all clusters.

- "Object Location" on page 42
- "Cluster OU Context" on page 43
- "Cluster OU Partitioning and Replication" on page 43

Object Location

Cluster nodes and Cluster objects can exist in any container in the eDirectory tree. The Virtual Server object for the cluster and the objects for cluster resources are automatically created in the eDirectory context of the server where the cluster resource is created and cluster-enabled.

IMPORTANT: You should create cluster resources on the master node of the cluster.

Cluster OU Context

Before you create a new cluster, use iManager to create an OU container for the cluster, and use the OU container for the Cluster objects and Server objects.

Figure 8-1 *Example: Cluster1 Container and Its Objects*

Cluster OU Partitioning and Replication

Partition the Cluster OU, replicate it to dedicated eDirectory servers that are holding a replica of the parent partition, and replicate it to all cluster nodes. This helps prevent resources from being stuck in an NDS Sync state when a cluster resource's configuration is modified.

If you do not want to put a replica of eDirectory on the node, you must configure one or multiple LDAP servers for the node to use. The LDAP servers must have a master replica or a Read/Write replica of eDirectory. For information about how to modify the LDAP server list that is used by a cluster, see Changing the Administrator Credentials or LDAP Server IP Addresses for a Cluster in the OES Cluster Services for Linux Administration Guide

8.1.7 Planning for Shared Storage as Cluster Resources

OES Cluster Services supports using cluster resources for the following file systems and storage solutions:

File System or Storage Solution	See
Storage Services (NSS) pools	Configuring and Managing Cluster Resources for Shared NSS Pools and Volumes
Linux LVM volume groups and logical volumes	Configuring and Managing Cluster Resources for Shared LVM Volume Groups
Linux POSIX volumes	CSMPORT Utility (Cluster Segment Manager Import/Export)
NCP (NetWare Control Protocol) volumes (NCP shares on cluster-enabled Linux POSIX volumes)	"Configuring NCP Volumes with OES Cluster Services" in the *NCP Server for Linux Administration Guide*
Dynamic Storage Technology (DST) volumes (NSS volumes configured in a shadow volume pair)	"Configuring DST Shadow Volume Pairs with OES Cluster Services" in the *Dynamic Storage Technology Administration Guide*

8.1.8 Planning for OES Services as Cluster Resources

OES Cluster Services supports using cluster resources for the following OES services:

Service	See
Apache Web Server	"Apache HTTP Server" in the *OES 2015 SP1: Novell Cluster Services NetWare to Linux Conversion Guide*
Certificate Server (NetIQ eDirectory Server Certificates)	"eDirectory Server Certificates" in the *OES 2015 SP1: Novell Cluster Services NetWare to Linux Conversion Guide*
CIFS (OES CIFS)	"Configuring CIFS with Cluster Services for an NSS File System" in the *OES CIFS for Linux Administration Guide*
DFS VLDB (Distributed File Services Volume Location Database)	"Clustering Distributed File Services" in the *Distributed File Services Administration Guide for Linux*
DHCP Server on a Linux POSIX volume	"Configuring DHCP with OES Cluster Services for the Linux File System" in the *DNS/DHCP Services for Linux Administration Guide*
DHCP Server on an NSS volume	"Configuring DHCP with OES Cluster Services for the NSS File System" in the *DNS/DHCP Services for Linux Administration Guide*
DNS Server	"Configuring DNS with OES Cluster Services" in the *DNS/DHCP Services for Linux Administration Guide*
iPrint	"Configuring iPrint with OES Cluster Services" in the *OES 23.4: OES iPrint Administration Guide*
MySQL	"High Availability and Scalability" in the *MySQL 5.x Reference Manual* "MySQL" in the *OES 2015 SP1: Novell Cluster Services NetWare to Linux Conversion Guide*
PureFTPd (OES FTP)	"Cluster Enabling Pure-FTPd in an OES Environment" in the *Planning and Implementation Guide*

8.2 Planning for OES Cluster Services

This section describes the requirements for installing and using Cluster Services on Open Enterprise Server (OES) servers.

IMPORTANT: For information about designing your cluster and cluster environment, see Chapter 8, "Clustering and High Availability," on page 39.

- Section 8.2.1, "Cluster Administration Requirements," on page 45
- Section 8.2.2, "IP Address Requirements," on page 48
- Section 8.2.3, "Volume ID Requirements," on page 48
- Section 8.2.4, "Hardware Requirements," on page 49
- Section 8.2.5, "Virtualization Environments," on page 49
- Section 8.2.6, "Software Requirements for Cluster Services," on page 50
- Section 8.2.7, "Software Requirements for Cluster Resources," on page 59
- Section 8.2.8, "Shared Disk Configuration Requirements," on page 62
- Section 8.2.9, "SAN Rules for LUN Masking," on page 65
- Section 8.2.10, "Multipath I/O Configuration Requirements," on page 65

8.2.1 Cluster Administration Requirements

You use different credentials to install and set up the cluster and to manage the cluster. This section describes the tasks performed and rights needed for those roles.

- "Cluster Installation Administrator" on page 45
- "NCS Proxy User" on page 46
- "Cluster Administrator or Administrator-Equivalent User" on page 48

Cluster Installation Administrator

Typically, a tree administrator user installs and sets up the first cluster in a tree, which allows the schema to be extended. However, the tree administrator can extend the schema separately, and then set up the necessary permissions for a container administrator to install and configure the cluster.

NOTE: If the eDirectory administrator user name or password contains special characters (such as $, #, and so on), some interfaces in iManager and YaST might not handle the special characters. If you encounter problems, try escaping each special character by preceding it with a backslash (\) when you enter credentials.

- "eDirectory Schema Administrator" on page 45
- "Container Administrator" on page 46

eDirectory Schema Administrator

A tree administrator user with credentials to do so can extend the eDirectory schema before a cluster is installed anywhere in a tree. Extending the schema separately allows a container administrator to install a cluster in a container in that same tree without needing full administrator rights for the tree.

IMPORTANT: It is not necessary to extend the schema separately if the installer of the first cluster server in the tree has the eDirectory rights necessary to extend the schema.

Container Administrator

After the schema has been extended, the container administrator (or non-administrator user) needs the following eDirectory rights to install OES Cluster Services:

- Attribute Modify rights on the NCP Server object of each node in the cluster.
- Object Create rights on the container where the NCP Server objects are.
- Object Create rights where the cluster container will be.

For instructions, see Assigning Install Rights for Container Administrators or Non-Administrator Users.

NCS Proxy User

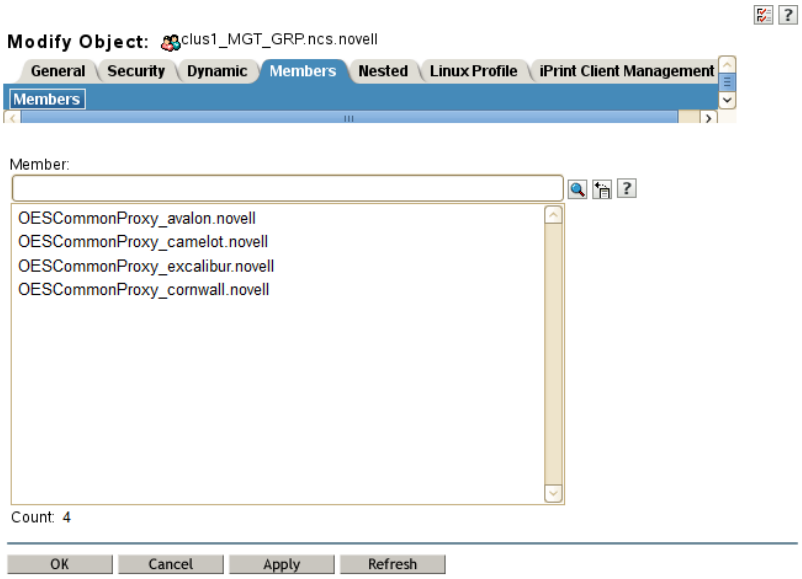
During the cluster configuration, you must specify an NCS Proxy User. This is the user name and password that Cluster Services uses when the cluster management tools exchange information with eDirectory.

Cluster Services supports the OES Common Proxy User enablement feature of eDirectory. The proxy user is represented in eDirectory as a User object named `OESCommonProxy_<server_name>.<context>`. If the OES Common Proxy user is enabled in eDirectory when you configure a node for the cluster, the default NCS Proxy User is set to use the server's OES Common Proxy User. You can alternatively specify the LDAP Admin user or another administrator user.

The specified NCS Proxy User for the node is automatically assigned as a member in the `<cluster_name>_MGT_GRP.<context>` group that resides in the Cluster object container, such as `clus1_MGT_GRP.ncs.novell`. The group accommodates the server-specific NCS Proxy Users that you assign when you configure each node for the cluster. Members are added to the group as you configure each node for a cluster. Each member of the group has the necessary rights for configuring the cluster and cluster resources and for exchanging information with eDirectory.

For example, Figure 8-2 shows that an OES Common Proxy User has been assigned as the NCS Proxy User for each node in a four-node cluster. The nodes are named `avalon`, `camelot`, `excalibur`, and `cornwall`. The context is `novell`.

Figure 8-2 *Members of the NCS Management Group for a Cluster*



IMPORTANT: You can modify this default administrator user name or password for the user name assigned as the NCS Proxy User after the install by following the procedure in Moving a Cluster, or Changing the Node IP Addresses, LDAP Servers, or Administrator Credentials for a Cluster.

Consider the following caveats for the three proxy user options:

- "OES Common Proxy User" on page 47
- "LDAP Admin User" on page 48
- "Another Administrator User" on page 48

OES Common Proxy User

If you specify the OES Common Proxy user for a cluster and later disable the Common Proxy user feature in eDirectory, the LDAP Admin user is automatically assigned to the *<cluster_name>*_MGT_GRP.*<context>* group, and the OES Common Proxy user is automatically removed from the group.

If an OES Common Proxy User is renamed, moved, or deleted in eDirectory, eDirectory takes care of the changes needed to modify the user information in the *<cluster_name>*_MGT_GRP.*<context>* group.

If a cluster node is removed from the tree, the OES Common Proxy User for that server is one of the cluster objects that needs to be deleted from eDirectory.

For information about enabling or disabling the OES Common Proxy User, see the *Installation Guide*. For caveats and troubleshooting information for the OES Common Proxy user, see the *Planning and Implementation Guide*.

LDAP Admin User

If you specify the LDAP Admin user as the NCS Proxy User, you typically continue using this identity while you set up the cluster and cluster resources. After the cluster configuration is completed, you create another user identity to use for NCS Proxy User, and grant that user sufficient administrator rights as specified in "Cluster Administrator or Administrator-Equivalent User" on page 48.

Another Administrator User

You can specify an existing user name and password to use for the NCS Proxy User. Cluster Services adds this user name to the <*cluster_name*>_MGT_GRP.<*context*> group.

Cluster Administrator or Administrator-Equivalent User

After the install, you can add other users (such as the tree administrator) as administrator equivalent accounts for the cluster by configuring the following for the user account:

- Give the user the Supervisor right to the Server object of each of the servers in the cluster.
- Linux-enable the user account with Linux User Management (LUM).
- Make the user a member of a LUM-enabled administrator group that is associated with the servers in the cluster.

8.2.2 IP Address Requirements

- ❒ Each server in the cluster must be configured with a unique static IP address.
- ❒ You need additional unique static IP addresses for the cluster and for each cluster resource and cluster-enabled pool.
- ❒ All IP addresses used by the master cluster IP address, its cluster servers, and its cluster resources must be on the same IP subnet. They do not need to be contiguous addresses.

8.2.3 Volume ID Requirements

A volume ID is a value assigned to represent the volume when it is mounted by NCP Server on an OES server. The Client for Open Enterprise Server accesses a volume by using its volume ID. Volume ID values range from 0 to 254. On a single server, volume IDs must be unique for each volume. In a cluster, volume IDs must be unique across all nodes in the cluster.

Unshared volumes are typically assigned low numbers, starting from 2 in ascending order. Volume IDs 0 and 1 are reserved. Volume ID 0 is assigned by default to volume SYS. Volume ID 1 is assigned by default to volume _ADMIN.

Cluster-enabled volumes use high volume IDs, starting from 254 in descending order. When you cluster-enable a volume, Cluster Services assigns a volume ID in the resource's load script that is unique across all nodes in a cluster. You can modify the resource's load script to change the assigned volume ID, but you must manually ensure that the new value is unique.

In a Business Continuity Clustering (BCC) cluster, the volume IDs of BCC-enabled clustered volumes must be unique across all nodes in every peer cluster. However, clustered volumes in different clusters might have the same volume IDs. Duplicate volume IDs can prevent resources from going online if the resource is BCC-migrated to a different cluster. When you BCC-enable a volume, you

must manually edit its load script to ensure that its volume ID is unique across all nodes in every peer cluster. You can use the `ncpcon volumes` command on each node in every peer cluster to identify the volume IDs in use by all mounted volumes. Compare the results for each server to identify the clustered volumes that have duplicate volume IDs assigned. Modify the load scripts to manually assign unique volume IDs.

8.2.4 Hardware Requirements

The following hardware requirements for installing Cluster Services represent the minimum hardware configuration. Additional hardware might be necessary depending on how you intend to use Cluster Services.

- ❒ A minimum of two Linux servers, and not more than 32 servers in a cluster
- ❒ At least 512 MB of additional memory on each server in the cluster
- ❒ One non-shared device on each server to be used for the operating system
- ❒ At least one network card per server in the same IP subnet.

  In addition to Ethernet NICs, Cluster Services supports VLAN on NIC bonding in OES 11 SP1 (with the latest patches applied) or later. No modifications to scripts are required. You can use eth*x* or vlan*x* interfaces in any combination for nodes in a cluster.

In addition, each server must meet the requirements for Open Enterprise Server 24.4. See "Meeting All Server Software and Hardware Requirements" in the *Installation Guide*.

NOTE: Although identical hardware for each cluster server is not required, having servers with the same or similar processors and memory can reduce differences in performance between cluster nodes and make it easier to manage your cluster. There are fewer variables to consider when designing your cluster and failover rules if each cluster node has the same processor and amount of memory.

If you have a Fibre Channel SAN, the host bus adapters (HBAs) for each cluster node should be identical and be configured the same way on each node.

8.2.5 Virtualization Environments

Xen and KVM virtualization software is included with SUSE Linux Enterprise Server. Cluster Services supports using Xen or KVN virtual machine (VM) guest servers as nodes in a cluster. You can install Cluster Services on the guest server just as you would a physical server. All templates except the Xen and XenLive templates can be used on a VM guest server. For examples, see Configuring OES Cluster Services in a Virtualization Environment.

Cluster Services is supported to run on a host server where it can be used to cluster the virtual machine configuration files on Linux POSIX file systems. Only the Xen and XenLive templates are supported for use in the XEN host environment. These virtualization templates are general, and can be adapted to work for other virtualization environments, such as KVM and VMware. For information about setting up Xen and XenLive cluster resources for a virtualization host server, see Virtual Machines as Cluster Resources.

8.2.6 Software Requirements for Cluster Services

Ensure that your system meets the following software requirements for installing and managing Cluster Services:

- "Open Enterprise Server 24.4" on page 50
- "Cluster Services" on page 50
- "NetIQ eDirectory" on page 50
- "SLP" on page 54
- "iManager 3.2.6" on page 56
- "Clusters Plug-in for iManager" on page 56
- "Storage-Related Plug-Ins for iManager" on page 57
- "SFCB and CIMOM" on page 57
- "OES Credential Store (OCS)" on page 58
- "Web Browser" on page 59

Open Enterprise Server 24.4

Cluster Services for Linux supports OES 24.4. OES Cluster Services is one of the OES Services patterns.

We recommend having uniform nodes in the cluster. The same release version of OES must be installed and running on each node in the cluster.

Mixed-mode clusters with different operating system platforms are supported during rolling cluster upgrades or conversions for the following scenarios:

Upgrading from	See:
OES 2015 SP1 or later	Upgrading OES Clusters
NetWare 6.5 SP8	*OES 2015 SP1: Novell Cluster Services NetWare to Linux Conversion Guide*

Cluster Services

Cluster Services is required for creating and managing clusters and shared resources on your OES servers. OES Cluster Services is one of the OES Services patterns on OES 24.4.

NetIQ eDirectory

NetIQ eDirectory is required for managing the Cluster object and Cluster Node objects for Cluster Services. eDirectory must be installed and running in the same tree where you create the cluster. eDirectory can be installed on any node in the cluster, on a separate server, or in a separate cluster. You can install an eDirectory master replica or replica in the cluster, but it is not required to do so for Cluster Services.

OES Version	eDirectory Version
OES 23.4, OES 24.1	9.2.8
OES 24.2, OES 24.3	9.2.9

For information about using eDirectory, see *NetIQ eDirectory Administration Guide*.

IMPORTANT: Because the cluster objects and their settings are stored in eDirectory, eDirectory must be running and working properly whenever you modify the settings for the cluster or the cluster resources.

In addition, ensure that your eDirectory configuration meets the following requirements:

- "eDirectory Tree" on page 51
- "eDirectory Context" on page 51
- "Cluster Object Container" on page 52
- "Cluster Objects Stored in eDirectory" on page 53
- "LDAP Server List" on page 54

eDirectory Tree

All servers in the cluster must be in the same eDirectory tree.

eDirectory Context

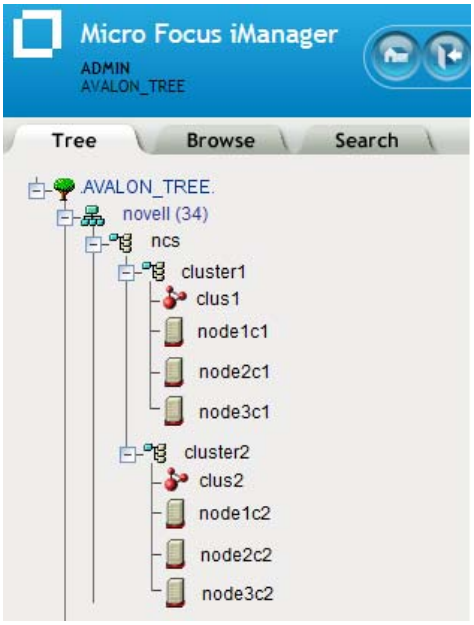
If you are creating a new cluster, the eDirectory context where the new Cluster object will reside must be an existing context. Specifying a new context during the Cluster Services configuration does not create a new context.

Cluster Object Container

We recommend that the Cluster object and all of its member Server objects and Storage objects be located in the same OU context. Multiple Cluster objects can co-exist in the same eDirectory container. In iManager, use **Directory Administration > Create Object** to create a container for the cluster before you configure the cluster.

For example, Figure 8-3 shows an example where all clusters are configured in the ncs organizational unit. Within the container, each cluster is in its own organizational unit, and the Server objects for the nodes are in the same container as the Cluster object:

Figure 8-3 *Same Container for Cluster Object and Server Objects*



If the servers in the cluster are in separate eDirectory containers, the user that administers the cluster must have rights to the cluster server containers and to the containers where any cluster-enabled pool objects are stored. You can do this by adding trustee assignments for the cluster administrator to a parent container of the containers where the cluster server objects reside. For more information, see "eDirectory Rights" in the *NetIQ eDirectory Administration Guide*.

Renaming a pool involves changing information in the Pool object in eDirectory. If Server objects for the cluster nodes are in different containers, you must ensure that the shared pool is active on a cluster node that has its NCP server object in the same context as the Pool object of the pool you are going to rename. For information about renaming a shared pool, see Renaming a Clustered NSS Pool .

Cluster Objects Stored in eDirectory

Table 8-1 shows the cluster objects that are automatically created and stored in eDirectory under the Cluster object ( ) after you create a cluster:

Table 8-1 *Cluster Objects*

Icon	eDirectory Object
	Master_IP_Address_Resource
	Cluster Node object (*servername*)
	Resource Template objects. There are 11 default templates: AV_Template DHCP_Template DNS_Template Generic_FS_Template Generic_IP_Service iPrint_Template MySQL_Template Samba_Template Xen_Template XenLive_Template

For example, Figure 8-4 shows the 13 default eDirectory objects that are created in the Cluster container as viewed from the Tree view in iManager:

Figure 8-4 *Tree View of the Default eDirectory Objects in the Cluster*

Table 8-2 shows the cluster objects that are added to eDirectory when you add nodes or create cluster resources:

Table 8-2 *Cluster Resource Objects*

Icon	eDirectory Object
	Cluster Node object (*servername*)
	NSS Pool Resource object (*poolname_SERVER*)
	Resource object

Table 8-3 shows the cluster objects that are added to eDirectory when you add nodes or create cluster resources in a Business Continuity Cluster, which is made up of OES Cluster Services clusters:

Table 8-3 *BCC Cluster Resource Objects*

Icon	eDirectory Object
	BCC NSS Pool Resource object
	BCC Resource Template object
	BCC Resource object

LDAP Server List

If eDirectory is not installed on a node, it looks to the LDAP server list for information about which LDAP server to use. As a best practice, you should list the LDAP servers in the following order:

- Local to the cluster
- Closest physical read/write replica

For information about configuring a list of LDAP servers for the cluster, see Changing the Administrator Credentials or LDAP Server IP Addresses for a Cluster.

SLP

SLP (Service Location Protocol) is a required component for Cluster Services on Linux when you are using NCP to access file systems on cluster resources. NCP requires SLP for the `ncpcon bind` and `ncpcon unbind` commands in the cluster load and unload scripts. For example, NCP is needed for NSS volumes and for NCP volumes on Linux POSIX file systems.

SLP is not automatically installed when you select Cluster Services. SLP is installed as part of the eDirectory configuration during the OES installation. You can enable and configure SLP on the eDirectory Configuration - NTP & SLP page. For information, see "Specifying SLP Configuration Options" in the *Installation Guide*.

When the SLP daemon (`slpd`) is not installed and running on a cluster node, any cluster resource that contains the `ncpcon bind` command goes comatose when it is migrated or failed over to the node because the bind cannot be executed without SLP.

The SLP daemon (`slpd`) must also be installed and running on all nodes in the cluster when you manage the cluster or cluster resources.

NCP Server re-registers cluster resource virtual NCP servers with SLP based on the setting for the eDirectory advertise-life-time (`n4u.nds.advertise-life-time`) parameter. The parameter is set by default to 3600 seconds (1 hour) and has a valid range of 1 to 65535 seconds.

You can use the `ndsconfig set` command to set the `n4u.nds.advertise-life-time` parameter. To reset the parameter in a cluster, perform the following tasks on each node of the cluster:

1. Log in to the node as the `root` user, then open a terminal console.
2. Take offline all of the cluster resources on the node, or cluster migrate them to a different server. At a command prompt, enter

   ```
   cluster offline <resource_name>
   ```

   or

   ```
   cluster migrate <resource_name> <target_node_name>
   ```

3. Modify the eDirectory SLP advertising timer parameter (`n4u.nds.advertise-life-time`), then restart ndsd and slpd. At a command prompt, enter

   ```
   ndsconfig set n4u.nds.advertise-life-time=<value_in_seconds>
   ```

   ```
   rcndsd restart
   ```

   ```
   rcslpd restart
   ```

4. Bring online all of the cluster resources on the node, or cluster migrate the previously migrated resources back to this node.

   ```
   cluster online <resource_name>
   ```

   or

   ```
   cluster migrate <resource_name> <node_name>
   ```

5. Repeat the previous steps on the other nodes in the cluster.

OpenSLP stores the registration information in cache. You can configure the SLP Directory Agents to preserve a copy of the database when the SLP daemon (`slpd`) is stopped or restarted. This allows SLP to know about registrations immediately when it starts.

For more information about configuring and managing SLP, see "Configuring OpenSLP for eDirectory" in the NetIQ eDirectory Administration Guide.

iManager 3.2.6

iManager is required for configuring and managing clusters on OES.

iManager must be installed on at least one computer in the same tree as the cluster. It can be installed in the cluster or not in the cluster. For information about using iManager, see the iManager documentation website.

For SFCB (Small Footprint CIM Broker) and CIMOM requirements, see "SFCB and CIMOM" on page 57.

For browser configuration requirements, see "Web Browser" on page 59.

Clusters Plug-in for iManager

The Clusters plug-in for iManager provides the Clusters role where you can manage clusters and cluster resources with OES Cluster Services. The plug-in can be used on all operating systems supported by iManager and iManager Workstation.

The following components must be installed in iManager:

- Clusters (`ncsmgmt.rpm`)
- Common code for storage-related plug-ins (`storagemgmt.rpm`)

  See "Storage-Related Plug-Ins for iManager" on page 57.

If iManager is also installed on the server, these files are automatically installed in iManager when you install OES Cluster Services.

The Clusters plug-in also provides an integrated management interface for OES Business Continuity Clustering (BCC). The additional interface is present only if BCC is installed on the server. See the following table for information about the versions of BCC that are supported. BCC is sold separately from OES. For purchasing information, see the BCC product page.

BCC Release	OES Support	iManager and Clusters Plug-In
BCC 2.6	OES 2018 SP1 and later	NetIQ iManager 3.1 or later Requires the Clusters plug-in for OES 24.4 with the latest patches applied. See the *BCC 2.6 Administration Guide*.

Storage-Related Plug-Ins for iManager

In OES 11 and later, the following storage-related plug-ins for iManager share code in common in the `storagemgmt.rpm` file:

Product	Plug-In	NPM File
Novell CIFS	File Protocols > CIFS	`cifsmgmt.rpm`
Novell Cluster Services	Clusters	`ncsmgmt.rpm`
Novell Distributed File Services	Distributed File Services	`dfsmgmt.rpm`
Novell Storage Services	Storage	`nssmgmt.rpm`

These additional plug-ins are needed when working with the NSS file system. Ensure that you include the common `storagemgmt.rpm` plug-in module when installing any of these storage-related plug-ins.

IMPORTANT: If you use more than one of these plug-ins, you should install, update, or remove them all at the same time to ensure that the common code works for all plug-ins.

Ensure that you uninstall the old version of the plug-ins before you attempt to install the new versions of the plug-in files.

The plug-in files are included on the installation disk. The latest storage-related plug-ins can be downloaded as a single zipped download file from the OpenText Downloads website. For information about installing plug-ins in iManager, see "Downloading and Installing Plug-in Modules" in the *NetIQ iManager Administration Guide*.

For information about working with storage-related plug-ins for iManager, see "Understanding Storage-Related Plug-Ins" in the *Storage Services File System (NSS) Administration Guide for Linux*.

SFCB and CIMOM

The Small Footprint CIM Broker (SFCB) replaces OpenWBEM for CIMOM activities in OES 11 and later. SFCB provides the default CIMOM and CIM clients. When you install any OES components that depend on WBEM, SFCB and all of its corresponding packages are installed with the components. For more information, see "Appendix N, "Small Footprint CIM Broker (SFCB)," on page 285".

IMPORTANT: SFCB must be running and working properly whenever you modify the settings for the cluster or the cluster resources.

Port 5989 is the default setting for Secure HTTP (HTTPS) communications. If you are using a firewall, the port must be opened for CIMOM communications. Ensure that the CIMOM broker daemon is listening on port 5989. Log in as the `root` user on the cluster master node, open a terminal console, then enter the following at the command prompt:

```
netstat -an |grep -i5989
```

The Clusters plug-in (and all other storage-related plug-ins) for iManager require CIMOM connections for tasks that transmit sensitive information (such as a user name and password) between iManager and the `_admin` volume on the OES server that you are managing. Typically, CIMOM is running, so this should be the normal condition when using the server. CIMOM connections use Secure HTTP (HTTPS) for transferring data, and this ensures that sensitive data is not exposed.

IMPORTANT: SFCB is automatically PAM-enabled for Linux User Management (LUM) as part of the OES installation. Users not enabled for LUM cannot use the CIM providers to manage OES. The user name that you use to log in to iManager when you manage a cluster and the BCC cluster must be an eDirectory user name that has been LUM-enabled.

For more information about the permissions and rights needed by the administrator user, see Section 8.2.1, “Cluster Administration Requirements,” on page 45.

IMPORTANT: If you receive file protocol errors, it might be because SFCB is not running.

You can use the following commands to start, stop, or restart SFCB:

To perform this task	At a command prompt, enter as the `root` user
To start SFCB	`rcsfcb start` or `systemctl start sblim-sfcb.service`
To stop SFCB	`rcsfcb stop` or `systemctl stop sblim-sfcb.service`
To check SFCB status	`rcsfcb status` or `systemctl status sblim-sfcb.service`
To restart SFCB	`rcsfcb restart` or `systemctl restart sblim-sfcb.service`

For more information, see “Web Based Enterprise Management using SFCB” in the *SUSE Linux Enterprise Server 12 Administration Guide*.

OES Credential Store (OCS)

Cluster Services requires OES Credential Store to be installed and running on each node in the cluster.

To check whether the OCS is running properly, do the following:

1. At the command prompt, enter as the `root` user.
2. Run the following command:

   ```
   oescredstore -l
   ```

Web Browser

For information about supported web browsers for iManager, see "System Requirements for iManager Server" in the *NetIQ iManager Installation Guide*.

The Clusters plug-in for iManager might not operate properly if the highest priority Language setting for your web browser is set to a language other than one of the supported languages in iManager. To view a list of supported languages and codes in iManager, select the **Preferences** tab, click **Language**. The language codes are Unicode (UTF-8) compliant.

To avoid display problems, in your web browser, select **Tools > Options > Languages**, and then set the first language preference in the list to a supported language. You must also ensure the Character Encoding setting for the browser is set to Unicode (UTF-8) or ISO 8859-1 (Western, Western European, West European).

- In a Mozilla browser, select **View > Character Encoding**, then select the supported character encoding setting.
- In an Internet Explorer browser, select **View > Encoding**, then select the supported character encoding setting.

8.2.7 Software Requirements for Cluster Resources

Ensure that your system meets the following software requirements for creating and managing storage cluster resources:

- "NCP Server for Linux" on page 59
- "Storage Services File System for Linux" on page 60
- "LVM Volume Groups and Linux POSIX File Systems" on page 61
- "NCP Volumes on Linux POSIX File Systems" on page 61
- "Dynamic Storage Technology Shadow Volume Pairs" on page 61
- "NCP File Access" on page 61
- "CIFS" on page 61
- "Domain Services for Windows" on page 62

NCP Server for Linux

NCP Server for Linux is required in order to create virtual server names (`NCS:NCP Server` objects) for cluster resources. This includes storage and service cluster resources. To install NCP Server, select the **NCP Server and Dynamic Storage Technology** option during the install.

NCP Server for Linux also allows you to provide authenticated access to data by using the OES Trustee model. The NCP Server component must be installed and running before you can cluster-enable the following storage resources:

- NSS pools and volumes
- NCP volumes on Linux POSIX file systems

- Dynamic Storage Technology shadow volume composed of a pair of NSS volumes
- Linux Logical Volume Manager volume groups that use an NCS:NCP `Server` object, such as those created by using the Logical Volume Manger (NLVM) commands or the NSS Management Utility (NSSMU)

WARNING: Cross-protocol file locking is required when using multiple protocols for data access on the same volume. This helps prevent possible data corruption that might occur from cross-protocol access to files. The NCP Cross-Protocol File Lock parameter is enabled by default when you install NCP Server. If you modify the Cross-Protocol File Lock parameter, you must modify the setting on all nodes in the cluster.

NCP Server does not support cross-protocol locks across a cluster migration or failover of the resource. If a file is opened with multiple protocols when the migration or failover begins, the file should be closed and reopened after the migration or failover to acquire cross-protocol locks on the new node.

See "Configuring Cross-Protocol File Locks for NCP Server" in the *NCP Server for Linux Administration Guide*.

NCP Server for Linux is not required when running Cluster Services on a Xen-based virtual machine (VM) host server (Dom0) for the purpose of cluster-enabling an LVM volume group that holds the configuration files for Xen-based VMs. Users do not directly access these VM files.

For information about configuring and managing NCP Server for Linux, see the *NCP Server for Linux Administration Guide*.

For information about creating and cluster-enabling NCP volumes on Linux POSIX file systems, see "Configuring NCP Volumes with OES Cluster Services" in the *NCP Server for Linux Administration Guide*.

Storage Services File System for Linux

Storage Services (NSS) file system on Linux provides the following capabilities used by OES Cluster Services:

- Initializing and sharing devices used for the SBD (split-brain detector) and for shared pools. See "SBD Partitions" on page 63.
- Creating and cluster-enabling a shared pool. See Configuring and Managing Cluster Resources for Shared NSS Pools and Volumes.
- Creating and cluster-enabling a shared Linux Logical Volume Manager (LVM) volume group. See Configuring and Managing Cluster Resources for Shared LVM Volume Groups.

The NSS pool configuration and NCS pool cluster resource configuration provide integrated configuration options for the following advertising protocols:

- NetWare Core Protocol (NCP), which is selected by default and is mandatory for NSS. See "NCP Server for Linux" on page 59.
- OES CIFS. See "CIFS" on page 61.

LVM Volume Groups and Linux POSIX File Systems

Cluster Services supports creating shared cluster resources on Linux Logical Volume Manager (LVM) volume groups. You can configure Linux POSIX file systems on the LVM volume group, such as Ext3, XFS, and Ext4. LVM and Linux POSIX file systems are automatically installed as part of the OES installation.

After the cluster is configured, you can create LVM volume group cluster resources as described in Configuring and Managing Cluster Resources for Shared LVM Volume Groups.

NCP Server is required if you want to create a virtual server name (NCS:NCP Server object) for the cluster resource. You can add an NCP volume (an NCP share) on the Linux POSIX file system to give users NCP access to the data. See "NCP Server for Linux" on page 59.

NCP Volumes on Linux POSIX File Systems

After you cluster-enable an LVM volume group, Cluster Services supports creating NCP volumes on the volume group's Linux POSIX file systems. NCP Server is required. See "NCP Server for Linux" on page 59.

For information about creating and cluster-enabling NCP volumes, see "Configuring NCP Volumes with OES Cluster Services" in the *NCP Server for Linux Administration Guide*.

Dynamic Storage Technology Shadow Volume Pairs

Cluster Services supports clustering for Dynamic Storage Technology (DST) shadow volume pairs on OES 11 and later. DST is installed automatically when you install NCP Server for Linux. To use cluster-enabled DST volume pairs, select the **NCP Server and Dynamic Storage Technology** option during the install.

For information about creating and cluster-enabling Dynamic Storage Technology volumes on Linux, see "Configuring DST Shadow Volume Pairs with OES Cluster Services" in the *Dynamic Storage Technology Administration Guide*.

NCP File Access

Cluster Services requires NCP file access to be enabled for cluster-enabled NSS volumes, NCP volumes, and DST volumes, even if users do not access files via NCP. This is required to support access control via the OES Trustee model. See "NCP Server for Linux" on page 59.

CIFS

Cluster Services supports using CIFS as an advertising protocol for cluster-enabled NSS pools and volumes.

CIFS is not required to be installed when you install OES Cluster Services, but it must be installed and running in order for the **CIFS Virtual Server Name** field and the **CIFS** check box to be available. Select the check box to enable CIFS as an advertising protocol for the NSS pool cluster resource. A default **CIFS Virtual Server Name** is suggested, but you can modify it. The CIFS daemon should also be running before you bring resources online that have CIFS enabled.

To install CIFS, select the **OES CIFS** option from the OES Services list during the install. For information about configuring and managing the CIFS service, see the *OES CIFS for Linux Administration Guide*.

Domain Services for Windows

Cluster Services supports using clusters in Domain Services for Windows (DSfW) contexts. If Domain Services for Windows is installed in the eDirectory tree, the nodes in a given cluster can be in the same or different DSfW subdomains. Port 1636 is used for DSfW communications. This port must be opened in the firewall.

For information using Domain Services for Windows, see the *Domain Services for Windows Administration Guide*.

8.2.8 Shared Disk Configuration Requirements

A shared disk subsystem is required for a cluster in order to make data highly available. The Cluster Services software must be installed in order to be able to mark devices as shareable, such as the devices you use for clustered pools and the device you use for the SBD (split-brain detector) during the cluster configuration.

Ensure that your shared storage devices meet the following requirements:

- "Shared Devices" on page 62
- "SBD Partitions" on page 63
- "Shared iSCSI Devices" on page 64
- "Shared RAID Devices" on page 64

Shared Devices

Cluster Services supports the following shared disks:

- Fibre Channel LUN (logical unit number) devices in a storage array
- iSCSI LUN devices
- SCSI disks (shared external drive arrays)

Before configuring Cluster Services, the shared disk system must be properly set up and functional according to the manufacturer's instructions.

Prior to installation, verify that all the drives in your shared disk system are recognized by Linux by viewing a list of the devices on each server that you intend to add to your cluster. If any of the drives in the shared disk system do not show up in the list, consult the OES documentation or the shared disk system documentation for troubleshooting information.

Prepare the device for use in a cluster resource:

- **NSS Pool:** For new devices, you must initialize and share the device before creating the pool. For an existing pool that you want to cluster-enable, use NSSMU or iManager to share the device.

All devices that contribute space to a clustered pool must be able to fail over with the pool cluster resource. You must use the device exclusively for the clustered pool; do not use space on it for other pools or for Linux volumes. A device must be marked as Shareable for Clustering before you can use it to create or expand a clustered pool.

- **Linux LVM volume group:** For new devices, use an unpartitioned device that has been initialized. Do not mark the device as shared because doing so creates a small partition on it. LVM uses the entire device for the volume group. For an existing volume group, no not mark the device as shared.

If this is a new cluster, connect the shared disk system to the first server so that the SBD cluster partition can be created during the Cluster Services install. See "SBD Partitions" on page 63.

SBD Partitions

If your cluster uses physically shared storage resources, you must create an SBD (split-brain detector) partition for the cluster. You can create an SBD partition in YaST as part of the first node setup, or by using the SBD Utility (sbdutil) before you add a second node to the cluster. Both the YaST new cluster setup and the SBD Utility (`sbdutil`) support mirroring the SBD partition.

An SBD must be created before you attempt to create storage objects like pools or volumes for file system cluster resources, and before you configure a second node in the cluster. NLVM and other NSS management tools need the SBD to detect if a node is a member of the cluster and to get exclusive locks on physically shared storage.

For information about how SBD partitions work and how to create an SBD partition for an existing cluster, see Creating or Deleting Cluster SBD Partitions.

- "Preparing the SAN Devices for the SBD" on page 63
- "Initializing and Sharing a Device for the SBD" on page 63
- "Determining the SBD Partition Size" on page 64

Preparing the SAN Devices for the SBD

Use the SAN storage array software to carve a LUN to use exclusively for the SBD partition. The device should have at least 20 MB of free available space. The minimum size is 8 MB. Connect the LUN device to all nodes in the cluster.

For device fault tolerance, you can mirror the SBD partition by specifying two devices when you create the SBD. Use the SAN storage array software to carve a second LUN of the same size to use as the mirror. Connect the LUN device to all nodes in the cluster.

The device you use to create the SBD partition must not be a software RAID device. You can use a hardware RAID configured in a SAN array since it is seen as a regular device by the server.

Initializing and Sharing a Device for the SBD

Before you use YaST to set up the a cluster, you must initialize each SAN device that you created for the SBD, and mark each as Shareable for Clustering.

IMPORTANT: The Cluster Services software must already be installed in order to be able to mark the devices as shareable.

After you install Cluster Services, but before you configure the cluster, you can initialize a device and set it to a shared state by using NSSMU, the Storage plug-in for iManager, Linux Volume Manager (NLVM) commands, or an NSS utility called `ncsinit`.

If you configure a cluster before you create an SBD, NSS tools cannot detect if the node is a member of the cluster and cannot get exclusive locks to the physically shared storage. In this state, you must use the `-s` NLVM option with the `nlvm init` command to override the shared locking requirement and force NLVM to execute the command. To minimize the risk of possible corruption, you are responsible for ensuring that you have exclusive access to the shared storage at this time.

When you mark the device as Shareable for Clustering, share information is added to the disk in a free-space partition that is about 4 MB in size. This space becomes part of the SBD partition.

Determining the SBD Partition Size

When you configure a new cluster, you can specify how much free space to use for the SBD, or you can specify the **Use Maximum Size** option to use the entire device. If you specify a second device to use as a mirror for the SBD, the same amount of space is used. If you specify to use the maximum size and the mirror device is bigger than the SBD device, you will not be able to use the excess free space on the mirror for other purposes.

Because an SBD partition ends on a cylinder boundary, the partition size might be slightly smaller than the size you specify. When you use an entire device for the SBD partition, you can use the **Use Maximum Size** option, and let the software determine the size of the partition.

Shared iSCSI Devices

If you are using iSCSI for shared disk system access, ensure that you have installed and configured the iSCSI initiators and targets (LUNs) and that they are working properly. The iSCSI target devices must be mounted on the server before the cluster resources are brought online.

Shared RAID Devices

We recommend that you use hardware RAID in the shared disk subsystem to add fault tolerance to the shared disk system.

Consider the following when using software RAIDs:

- NSS software RAID is supported for shared disks for NSS pools. Any RAID0/5 device that is used for a clustered pool must contribute space exclusively to that pool; it cannot be used for other pools. This allows the device to fail over between nodes with the pool cluster resource. Ensure that its component devices are marked as Shareable for Clustering before you use a RAID0/5 device to create or expand a clustered pool
- Linux software RAID can be used in shared disk configurations that do not require the RAID to be concurrently active on multiple nodes. Linux software RAID cannot be used underneath clustered file systems (such as OCFS2, GFS, and CXFS) because Cluster Services does not support concurrent activation.

  WARNING: Activating Linux software RAID devices concurrently on multiple nodes can result in data corruption or inconsistencies.

8.2.9 SAN Rules for LUN Masking

When you create a Cluster Services system that uses shared storage space, it is important to remember that all of the servers that you grant access to the shared device, whether in the cluster or not, have access to all of the volumes on the shared storage space unless you specifically prevent such access. Cluster Services arbitrates access to shared volumes for all cluster nodes, but cannot protect shared volumes from being corrupted by non-cluster servers.

LUN masking is the ability to exclusively assign each LUN to one or more host connections. With it you can assign appropriately sized pieces of storage from a common storage pool to various servers. See your storage system vendor documentation for more information on configuring LUN masking.

Software included with your storage system can be used to mask LUNs or to provide zoning configuration of the SAN fabric to prevent shared volumes from being corrupted by non-cluster servers.

IMPORTANT: We recommend that you implement LUN masking in your cluster for data protection. LUN masking is provided by your storage system vendor.

8.2.10 Multipath I/O Configuration Requirements

If you use shared devices with multipath I/O capability, ensure that your setup meets the requirements in this section.

- “Path Failover Settings for Device Mapper Multipath” on page 65
- “Modifying the Port Down Retry Setting in the modprobe.conf.local File” on page 66
- “Modifying the Polling Interval, No Path Retry, and Failback Settings in the multipath.conf File” on page 66
- “Modifying the Port Down Retry and Link Down Retry Settings for an HBA BIOS” on page 68

Path Failover Settings for Device Mapper Multipath

When you use Device Mapper Multipath (DM-MP) with Cluster Services, ensure that you set the path failover settings so that the paths fail when path I/O errors occur.

The default setting in DM-MP is to queue I/O if one or more HBA paths is lost. Cluster Services does not migrate resources from a node set to the Queue mode because of data corruption issues that can be caused by double mounts if the HBA path is recovered before a reboot.

IMPORTANT: The HBAs must be set to Failed mode so that Cluster Services can automatically fail over storage resources if a disk paths go down.

Change the Retry setting in the `/etc/modprobe.d/99-local.conf` and `/etc/multipath.conf` files so that DM-MP works correctly with Cluster Services. See “Modifying the Port Down Retry Setting in the modprobe.conf.local File” on page 66 and “Modifying the Polling Interval, No Path Retry, and Failback Settings in the multipath.conf File” on page 66.

Also consider changes as needed for the retry settings in the HBA BIOS. See “Modifying the Port Down Retry and Link Down Retry Settings for an HBA BIOS” on page 68.

Modifying the Port Down Retry Setting in the modprobe.conf.local File

The port_down_retry setting specifies the number of times to attempt to reconnect to a port if it is down when using multipath I/O in a cluster. Ensure that you have installed the latest HBA drivers from your HBA vendor. Refer to the HBA vendor's documentation to understand the preferred settings for the device, then make any changes in the `/etc/modprobe.conf.local` file.

For example, for QLogic HBAs, ensure that you have installed the latest `qla-driver`. Ensure that you verify the vendor's preferred settings before making the changes.

Modifying the Polling Interval, No Path Retry, and Failback Settings in the multipath.conf File

The goal of multipath I/O is to provide connectivity fault tolerance between the storage system and the server. When you configure multipath I/O for a stand-alone server, the retry setting protects the server operating system from receiving I/O errors as long as possible. It queues messages until a multipath failover occurs and provides a healthy connection. However, when connectivity errors occur for a cluster node, you want to report the I/O failure in order to trigger the resource failover instead of waiting for a multipath failover to be resolved. In cluster environments, you must modify the retry setting so that the cluster node receives an I/O error in relation to the cluster SBD verification process (recommended to be 50% of the heartbeat tolerance) if the connection is lost to the storage system. In addition, you want the multipath I/O fail back to be set to manual in order to avoid a ping-pong of resources because of path failures.

Use the guidance in the following sections to configure the polling interval, no path retry and failback settings in the `/etc/multipath.conf` file:

- "Polling Interval" on page 66
- "No Path Retry" on page 66
- "Failback" on page 67
- "Example of Multipath I/O Settings" on page 67

Polling Interval

The polling interval for multipath I/O defines the interval of time in seconds between the end of one path checking cycle and the beginning of the next path checking cycle. The default interval is 5 seconds. An SBD partition has I/O every 4 seconds by default. A multipath check for the SBD partition is more useful if the multipath polling interval value is 4 seconds or less.

IMPORTANT: Ensure that you verify the `polling_interval` setting with your storage system vendor. Different storage systems can require different settings.

No Path Retry

We recommend a retry setting of "fail" or "0" in the `/etc/multipath.conf` file when working in a cluster. This causes the resources to fail over when the connection is lost to storage. Otherwise, the messages queue and the resource failover cannot occur.

IMPORTANT: Ensure that you verify the retry settings with your storage system vendor. Different storage systems can require different settings.

```
features "0"
no_path_retry fail
```

The value `fail` is the same as a setting value of 0.

Failback

We recommend a `failback` setting of "`manual`" for multipath I/O in cluster environments in order to prevent multipath failover ping-pong.

```
failback "manual"
```

IMPORTANT: Ensure that you verify the failback setting with your storage system vendor. Different storage systems can require different settings.

Example of Multipath I/O Settings

For example, the following code shows the default `polling_interval`, `no_path_retry`, and `failback` commands as they appear in the `/etc/multipath.conf` file for EMC storage:

```
defaults
{
    polling_interval    5
#    no_path_retry        0
    user_friendly_names     yes
    features 0
}

devices {
  device {
        vendor "DGC"
        product ".*"
        product_blacklist "LUNZ"
        path_grouping_policy "group_by_prio"
        path_checker "emc_clariion"
        features "0"
        hardware_handler "1 emc"
        prio "emc"
        failback "manual"
        no_path_retry fail    #Set MP for failed I/O mode, any other non-zero values sets
the HBAs for Blocked I/O mode
  }
}
```

For information about configuring the `multipath.conf` file, see "Managing Multipath I/O for Devices" in the *SLES 15 Storage Administration Guide*.

Modifying the Port Down Retry and Link Down Retry Settings for an HBA BIOS

In the HBA BIOS, the default settings for the **Port Down Retry** and **Link Down Retry** values are typically set too high for a cluster environment. For example, there might be a delay of more than 30 seconds after a fault occurs before I/O resumes on the remaining HBAs. Reduce the delay time for the HBA retry so that its timing is compatible with the other timeout settings in your cluster.

For example, you can change the **Port Down Retry** and **Link Down Retry** settings to 5 seconds in the QLogic HBA BIOS:

```
Port Down Retry=5
Link Down Retry=5
```

9 Managing OES

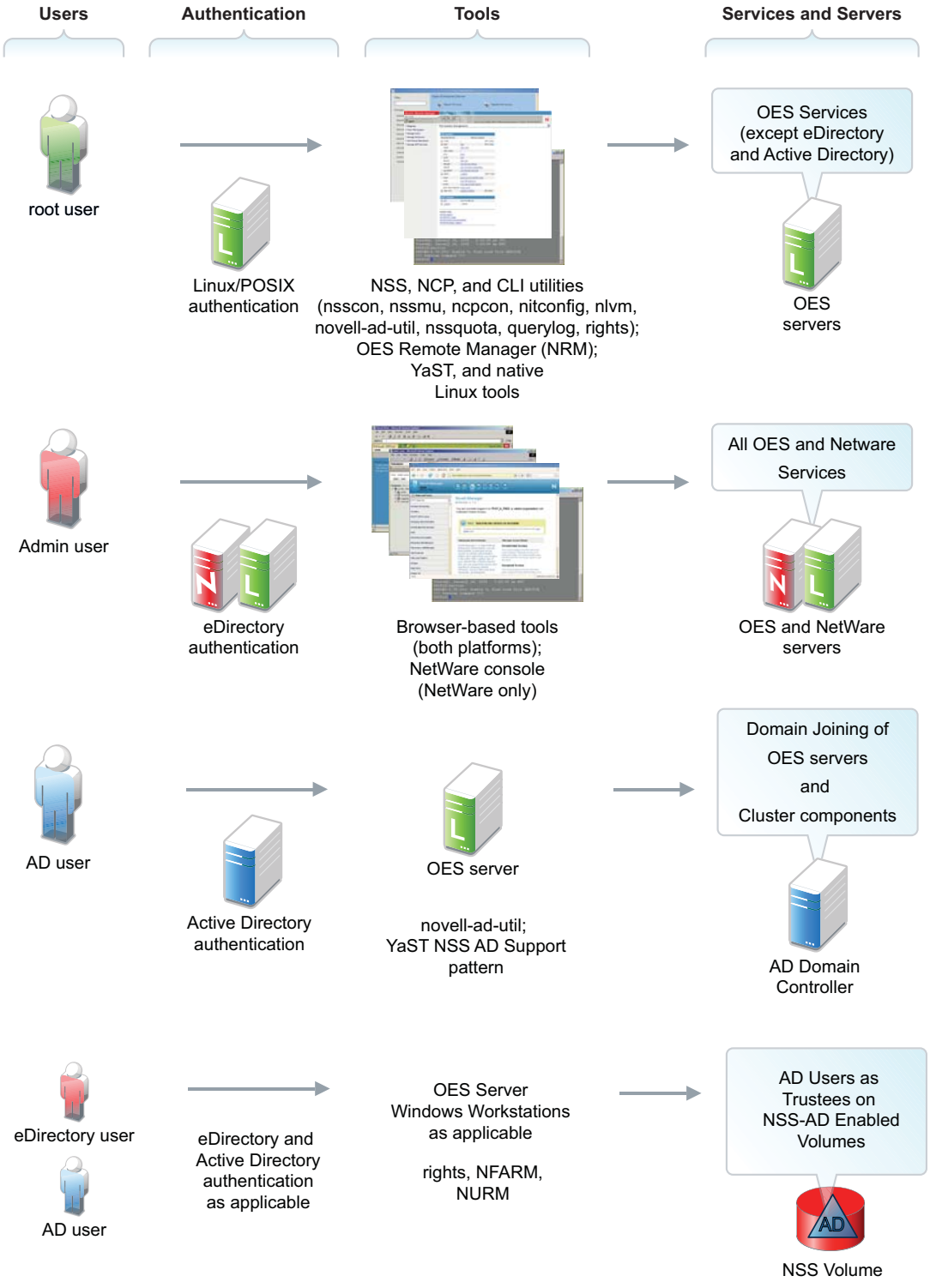
This section includes the following topics:

- Section 9.1, “Overview of Management Interfaces and Services,” on page 69
- Section 9.2, “OES Welcome Page,” on page 71
- Section 9.3, “Unified Management Console (UMC),” on page 72
- Section 9.4, “iManager and Self-Signed Certificates,” on page 72
- Section 9.5, “SSH Services on OES,” on page 73

9.1 Overview of Management Interfaces and Services

As shown in Figure 9-1, 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 servers require local authentication.

Figure 9-1 *Management Interfaces and Services*



Note:
Use Active Directory supported tools to manage AD users, AD groups, and ``Windows computers

9.2 OES Welcome Page

After you install an OES server, anyone with browser access to the server can access its Welcome Web site, which is a collection of dynamic Web pages that provides access to management tools and software.

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

- Section 9.2.1, “The Welcome Site Requires JavaScript, Apache, and Tomcat,” on page 71
- Section 9.2.2, “Accessing the Welcome Web Site,” on page 71
- Section 9.2.3, “The Welcome Web Site Is Available to All Users,” on page 72
- Section 9.2.4, “Administrative Access from the Welcome Web Site,” on page 72

9.2.1 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 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 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 server.

9.2.2 Accessing the Welcome Web Site

Anyone with browser access to an OES 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 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 *Installation Guide*.

9.2.3 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. Keep in mind, however, that the software in the **Client Software** link is static. For the latest client software, such as the iPrint client and Client for Open Enterprise Server, refer users to the OpenText download site.

9.2.4 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.

If a tool doesn't appear, that means that it or the service that it manages is not installed on the server.

9.3 Unified Management Console (UMC)

Unified Management Console (UMC) is a web-based remote management console designed for both small and large OES deployments. Once installed and configured, UMC directs you to its login page.

The UMC home page includes links to management tools, resources, forums, and downloads. You can manage various OES services such as NSS, Cluster, NCP, and CIFS.

NOTE: UMC replaces iManager, which offers limited support for OES services.

For more information, see Unified Management Console Administration Guide and Unified Management Console.

9.4 iManager and 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. For instructions on replacing the self-signed Apache/Tomcat certificate on OES, see Chapter 20, "Certificate Management," on page 209.

NOTE: Beginning with OES 23.4, iManager is deprecated and will not be available from OES 25.4. Unified Management Console (UMC) provides customized access to network administration utilities and content from virtually anywhere using the Internet and a web browser similar to iManager. For more information about UMC, see Unified Management Console.

9.5 SSH Services on OES

This section documents the following topics:

- Section 9.5.1, “Overview,” on page 73
- Section 9.5.2, “Setting Up SSH Access for LUM-enabled eDirectory Users,” on page 74

9.5.1 Overview

SSH services on SLES are provided by OpenSSH (http://www.openssh.org), a free version of SSH connectivity tools developed by the OpenBSD Project (http://www.openbsd.org/).

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

This section discusses the following topics:

- “When Is SSH Access Required?” on page 73
- “How SSH Access for eDirectory Users Works” on page 73
- “SSH Security Considerations” on page 74

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.

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 server does not 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:** 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.

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.

9.5.2 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 74
- "Adding SSH as an Allowed Service in LUM" on page 74
- "Enabling Users for LUM" on page 75
- "Restricting SSH Access to Only Certain LUM-Enabled Users" on page 75

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 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 75.

   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 server, open the YaST Control Center; then in the **Open Enterprise Server** group, click **OES Install and Configuration**.
3. Click **Accept**.

4 When the **OpenText 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 now shows SSH as an allowed service.

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). And finally, there are also command line options.

For specific instructions, refer to "Managing User and Group Objects in eDirectory" in the *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.

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 75.

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 server with iManager 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**.

10 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 10.1, “TCP/IP,” on page 77
- Section 10.2, “DNS and DHCP,” on page 78
- Section 10.3, “Time Services,” on page 80
- Section 10.4, “Discovery Services,” on page 92
- Section 10.5, “SLP,” on page 93

For links to more information and tasks, see the “network protocols” links in the OES online documentation.

10.1 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 includes the standard Linux TCP/IP support on SUSE Linux Enterprise Server 15 SP4.

10.1.1 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.

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

- Section 10.2.1, “DNS Differences Between NetWare and OES,” on page 78
- Section 10.2.2, “DHCP Differences Between NetWare and OES,” on page 79

10.2.1 DNS Differences Between NetWare and OES

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

Table 10-1 *DNS: NetWare 6.5 SP8 vs. OES 2018 SP3*

Feature or Command	NetWare 6.5 SP8	OES 2018 SP3
Auditing	Yes	No
Console commands:		
◆ Check Status	◆ `named status`	◆ `rcnovell-named status` or ◆ `systemctl status novell-named.service`
◆ Force Zone-in	◆ -zi *zone_name*	N/A
◆ Purge All Cache	◆ `-pa`	N/A
◆ Screen Logging	◆ `-s`	N/A
◆ Start the server	◆ `named`	◆ `rcnovell-named start` or ◆ `systemctl start novell-named.service`
◆ Stop the server	◆ `named stop`	◆ `rcnovell-named stop` or ◆ `systemctl stop novell-named.service`

Feature or Command	NetWare 6.5 SP8	OES 2018 SP3
◆ Unsupported `named` command parameters	◆ N/A	◆ [-dc categories] ◆ [-mstats] ◆ [-nno_of_cpus] ◆ [-qstats]
◆ Zone Information	◆ -info *file_name*	N/A
DNSMaint	Yes	Yes - `dns-maint`
Fault Tolerance	Yes	Yes
Filenames and paths:		
◆ Server binary	◆ `sys:/system/named.nlm`	◆ `/opt/novell/named/bin/novell-named`
◆ `.db`, `.jnl` file	◆ `sys:/etc/dns`	◆ `/etc/opt/novell/named/named.conf`
◆ Stat file, info file		◆ `/var/opt/novell/log/named/named.run`
Journal log size	Specify at the command prompt by using the jsize argument.	Specify using Java Console, **DNS Server Object>Advanced tab > max-journal-size field**.
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

10.2.2 DHCP Differences Between NetWare and OES

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

Table 10-2 *DHCP: NetWare 6.5 SP8 vs. OES 2018 SP3*

Feature or Command	NetWare 6.5 SP8	OES 2018 SP3
Auditing	Yes	No
Filenames and paths:		
◆ Conf file	◆ N/A	◆ `/etc/dhcpd.conf`
◆ Leases	◆ Stored in eDirectory	◆ `/var/lib/dhcp/db/dhcpd.leases`

Feature or Command	NetWare 6.5 SP8	OES 2018 SP3
• Log file	• `sys:/etc/dhcp/dhcpsrvr.log`	• `/var/log/dhcpd.log`
• Startup log	• N/A	• `/var/log/dhcp-ldap-startup.log` This is a dump of DHCP configurations read from eDirectory when the DHCP server starts.
Management	iManager 2.7 (Wizard-based)	Java Console Unlike the NetWare implementation, command line parameters cannot be passed when loading and unloading.
Migration	N/A	There is seamless migration support from NetWare.
Schema changes	N/A	There are separate locator and group objects for centralized management and easy rights management.
SNMP Support	Yes	No
Subnet naming	Yes	No

10.3 Time Services

The information in this section can help you understand your time services options as you move from NetWare to OES:

- Section 10.3.1, “Overview of Time Synchronization,” on page 81
- Section 10.3.2, “Planning for Time Synchronization,” on page 85
- Section 10.3.3, “Coexistence and Migration of Time Synchronization Services,” on page 88
- Section 10.3.4, “Implementing Time Synchronization,” on page 90
- Section 10.3.5, “Configuring and Administering Time Synchronization,” on page 91
- Section 10.3.6, “Daylight Saving Time,” on page 92

10.3.1 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 81
- "OES Servers as Time Providers" on page 83
- "OES Servers as Time Consumers" on page 84

Understanding Time Synchronization Modules

During the upgrade to OES 24.4, 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.

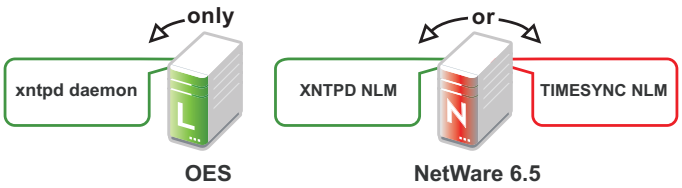
- "OES vs. NetWare 6.5" on page 81
- "OES Servers Use the Network Time Protocol (NTP) to Communicate" on page 81
- "Compatibility with Earlier Versions of NetWare" on page 82

OES vs. NetWare 6.5

As illustrated in Figure 10-1, 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.

OES must use the NTP daemon (xntpd).

Figure 10-1 *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.

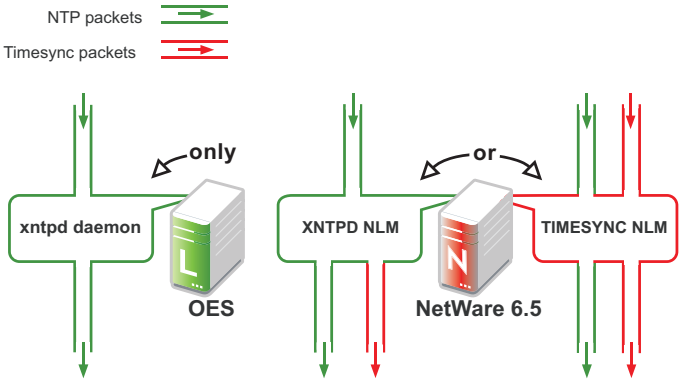
However, this does not limit your options on NetWare.

Figure 10-2 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 10-2 *NTP Packet Compatibilities with All OES Time Synchronization Modules*



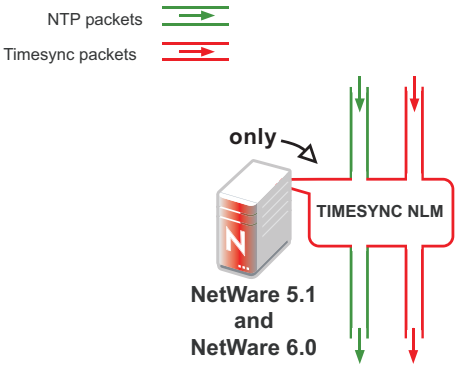
Compatibility with Earlier Versions of NetWare

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 10-3 illustrates that although NetWare 5.1 and 6.0 do not include an NTP time module, they can consume and deliver NTP time packets.

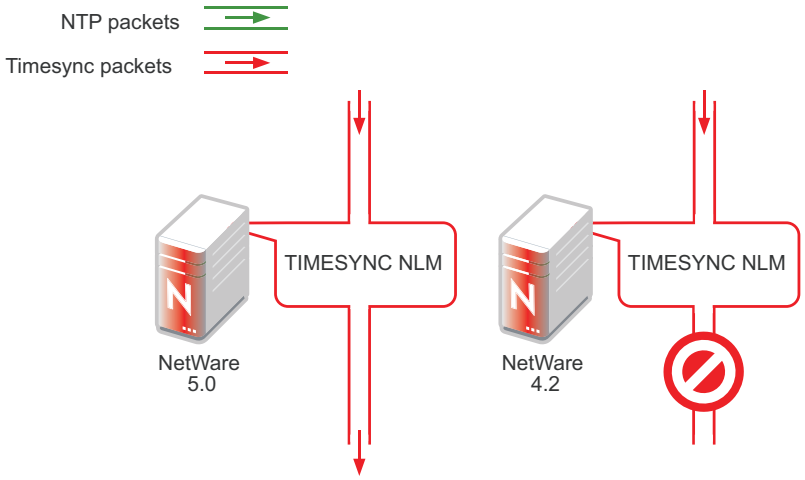
Figure 10-3 *NTP Compatibility of NetWare 5.1 and 6.0*



NetWare 5.0 and 4.2 Servers

Figure 10-4 illustrates that NetWare 4.2 and 5.0 servers can only consume and provide Timesync packets.

Figure 10-4 *Synchronizing Time on NetWare 5.0 and 4.2 Servers*



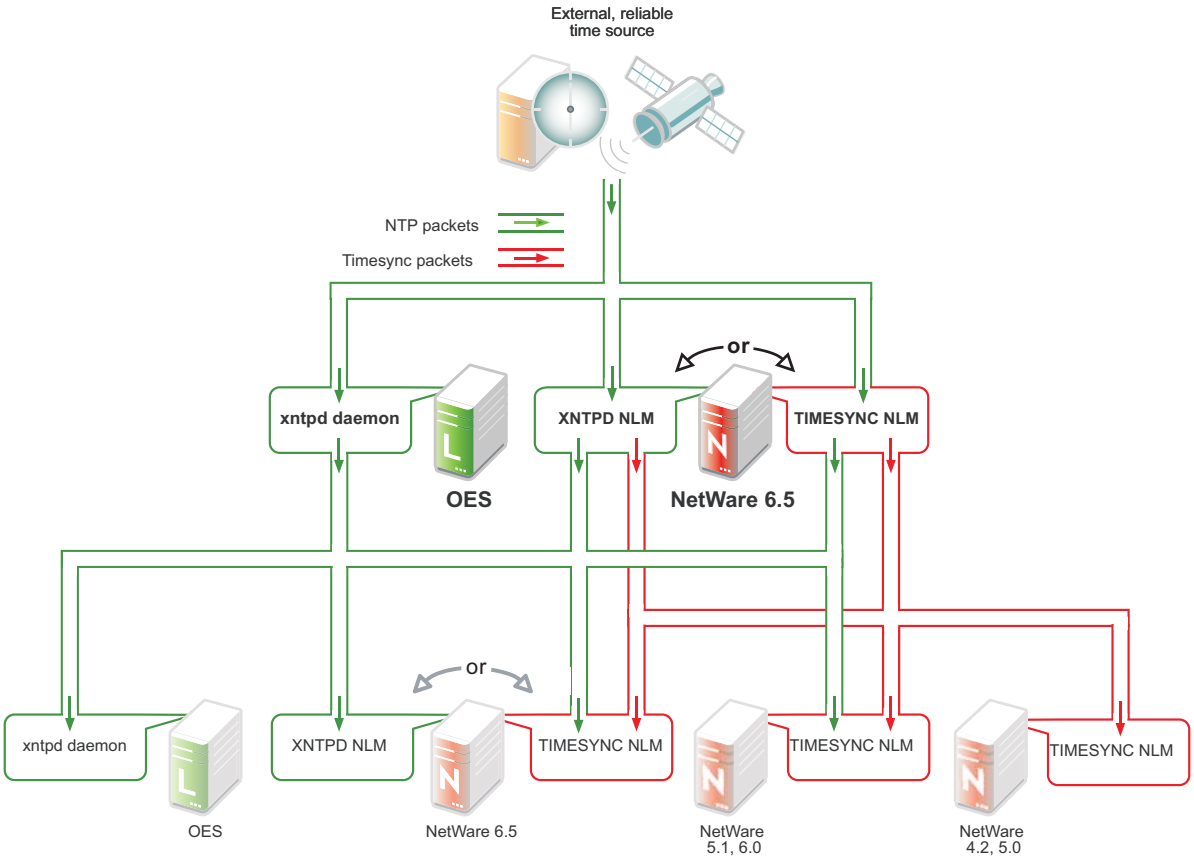
Therefore, if you have NetWare 4.2 or 5.0 servers in your eDirectory tree, and you want to install an OES server, you must have at least one NetWare 5.1 or later server to provide a “bridge” between NTP and Timesync time packets. Figure 10-5 on page 84 illustrates that these earlier server versions can synchronize through a NetWare 6.5 server.

IMPORTANT: As shown in Figure 10-4, we recommend that NetWare 4.2 servers not be used as a time source.

OES Servers as Time Providers

Figure 10-5 shows how OES servers can function as time providers to other OES servers and to NetWare servers, including NetWare 4.2 and later.

Figure 10-5 *OES Servers as Time Providers*

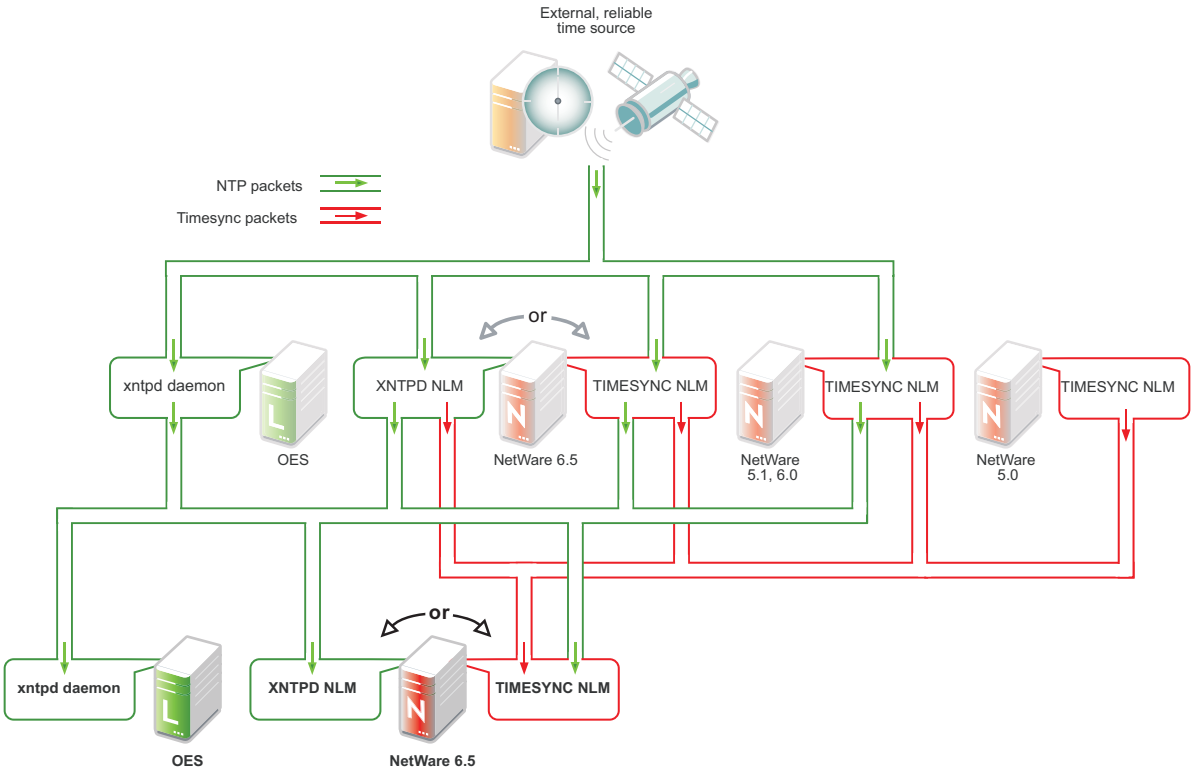


OES Servers as Time Consumers

Figure 10-6 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 10-6 *OES servers as Time Consumers*



10.3.2 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 86
- “Choose Timesync for Virtualized NetWare Only” on page 87
- “Planning a Time Synchronization Hierarchy before Installing OES” on page 87

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 86
- "Time Synchronization for Trees with More Than Thirty Servers" on page 86
- "Time Synchronization across Geographical Boundaries" on page 86

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 87.)

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 87.

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)

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

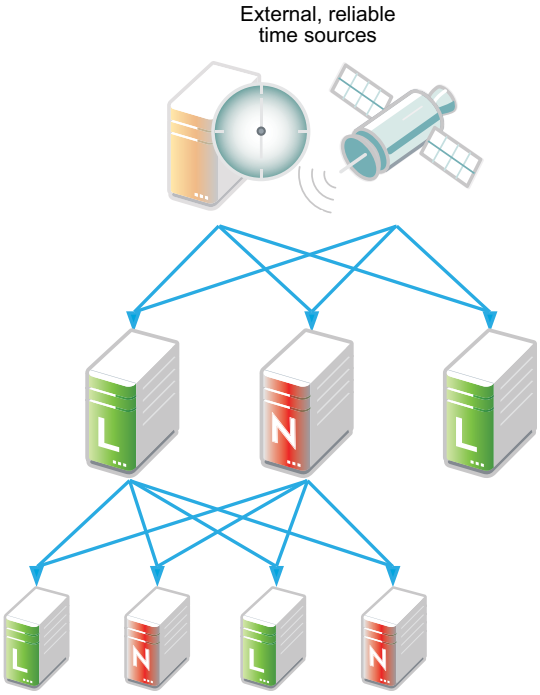
When you install a virtualized NetWare 6.5 server, you should always use Timesync and configure it to communicate using NTP.

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 10-7.

Figure 10-7 *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) 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 83.)

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 server in `/usr/share/doc/packages/xntp` and on the Web (http://www.cis.udel.edu/~mills/ntp.html)

10.3.3 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 88
- "Upgrading from NetWare to OES" on page 90

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 89
- "Coexistence Issues" on page 89

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 10-5 on page 84 and Figure 10-6 on page 85.

Table 10-3 *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.
XNTPD NLM (NetWare)	Can consume time from ◆ Any NTP daemon. Can provide time to ◆ All previous versions of Timesync. ◆ Any NTP daemon.
xntpd daemon (SLES 11)	Can consume time from ◆ Any NTP daemon. Can provide time to ◆ 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 82.

Upgrading from NetWare to OES

The OES Migration Tool can migrate time synchronization services from NetWare to Linux. For more information, see "Migrating NTP to OES 24.4" in the *Migration Tool Administration Guide*.

10.3.4 Implementing Time Synchronization

As you plan to implement your time synchronization hierarchy, you should know how the NetWare and OES 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 90
- "Existing Tree" on page 91

New Tree

By default, both the OES 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) on the Web.

- "OES" on page 90
- "NetWare 6.5 SP8" on page 90

OES

When you configure your eDirectory installation, the OES 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 87 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” on page 91
- “NetWare 6.5 SP8” on page 91

OES

If you are installing into an existing tree, the OES 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 87.

The OES 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 15 Server” on page 92.

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 87) 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.

10.3.5 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 15 Server” on page 92
- “Changing Time Synchronization Settings on a NetWare Server” on page 92

Changing Time Synchronization Settings on a SLES 15 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 15 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*

10.3.6 Daylight Saving Time

For information about daylight saving time (DST), go to the OpenText Support Knowledgebase (http://www.novell.com/support/kb/) and search for Daylight Saving Time.

10.4 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)

  For more information, see Section 10.5, “SLP,” on page 93.
- 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.

10.4.1 OpenSLP

For information, see Section 10.5, “SLP,” on page 93.

10.5 SLP

The OpenSLP services on OES are compatible and comparable with NetWare SLP services.

This section discusses the following topics:

- Section 10.5.1, “Overview,” on page 93
- Section 10.5.2, “Comparing Novell SLP and OpenSLP,” on page 95
- Section 10.5.3, “Setting Up OpenSLP on OES Networks,” on page 96
- Section 10.5.4, “Using Novell SLP on OES Networks,” on page 101
- Section 10.5.5, “TIDs and Other Help,” on page 106

10.5.1 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 93
- “About the Three SLP Agents and Their Roles” on page 93
- “Overcoming the Subnet Limitation” on page 94
- “An eDirectory Example” on page 94
- “What Happens When a DA Goes Down?” on page 94

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 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

OpenText 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 in the OpenText Support Knowledge base.

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 98.
- 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 99.

These changes provide, in effect, the same type of DA to DA communication for OES that has traditionally been available only on NetWare.

10.5.2 Comparing Novell SLP and OpenSLP

Table 10-4 *SLP Solutions*

Platform	NetWare	OES
SLP Solution	Novell SLP	OpenSLP
About the Solution	The Novell version of SLP adapted portions of the SLP standard to provide a more robust service advertising environment. Novell SLP remains the default discovery mechanism for NetWare 6.5 SP8 servers. However, all NetWare service components that engage in discovery, including Client for Open Enterprise Server software, can use alternative mechanisms such as DNS, eDirectory, or local host configuration files.	OpenSLP is an implementation of various IETF specifications, including RFC 2614 (SLP version 2.0). It is the default SLP service installed on SLES 15. In OES, 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 server is the fourth or later server added to a tree and doesn't have an eDirectory replica automatically installed.

Platform	NetWare	OES
Differences	Novell SLP directory agents (DAs) store service registrations for their SLP scope in eDirectory. 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. Also, when a Novell SLP DA starts up, it immediately populates its cache with the latest service information stored in eDirectory. **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.	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 98. OpenSLP is also capable of ensuring data persistence when DAs go down, as explained in "Backing Up Registrations and Managing Persistence" on page 99.
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.	"Configuring OpenSLP for eDirectory" in the *NetIQ eDirectory Administration Guide*.

10.5.3 Setting Up OpenSLP on OES Networks

SLP services are always installed as part of both NetWare and OES. 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 97
- "Setting Up an OpenSLP DA Server" on page 97
- "Synchronizing Data Between OpenSLP DAs and/or Novell SLP DAs" on page 98
- "Backing Up Registrations and Managing Persistence" on page 99
- "Configuring OES Servers to Access the OpenSLP DA" on page 99
- "Configuring NetWare Servers to Use the OpenSLP Service" on page 100

When Is OpenSLP Required?

The OES install automatically starts OpenSLP on your OES 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 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 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 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 server, do the following.

1. On the OES 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.

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 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 98)
- Backing Up Registrations and Managing Persistence (page 99)
- Configuring OES Servers to Access the OpenSLP DA (page 99)
- Configuring NetWare Servers to Use the OpenSLP Service (page 100)

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 Servers to Access the OpenSLP DA

If you created the OpenSLP DA on an OES 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 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 Installation" on page 99
- "Configuring for DA Access Before or After Installing OES" on page 100

Configuring for DA Access During the OES Installation

As you install OES by using the instructions in the "OES eDirectory Services" section of the *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 98. 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 97. You can also list additional DA addresses, separated by commas.

4. Return to the "NetIQ Modular Authentication Services" instructions in the *Installation Guide*.

Configuring for DA Access Before or After Installing OES

Whether you configure DA access before installing OES server or after install of OES, 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 98.

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 97.

```
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 101
- “Configuring for DA Access After Installing the NetWare Server” on page 101

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 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 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 cdbe
   set slp reset = on
   ```
4. Verify that SLP is functioning correctly by entering the following command:

   ```
   display slp services
   ```

10.5.4 Using Novell SLP on OES 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 until you are ready to switch to OpenSLP.

This section discusses the following:

- “NetWare Is Configured with Novell SLP By Default” on page 101
- “Configuring OES Servers to Access the Novell SLP DA” on page 102
- “Checking the Status of Novell SLP Services” on page 105

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 Servers to Access the Novell SLP DA

For each of the OES 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 Installation" on page 102
- "Configuring for DA Access Before or After Installing the OES Server" on page 102

Configuring for DA Access During the OES Installation

As you install OES, in the "OES eDirectory Services" section of the *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.

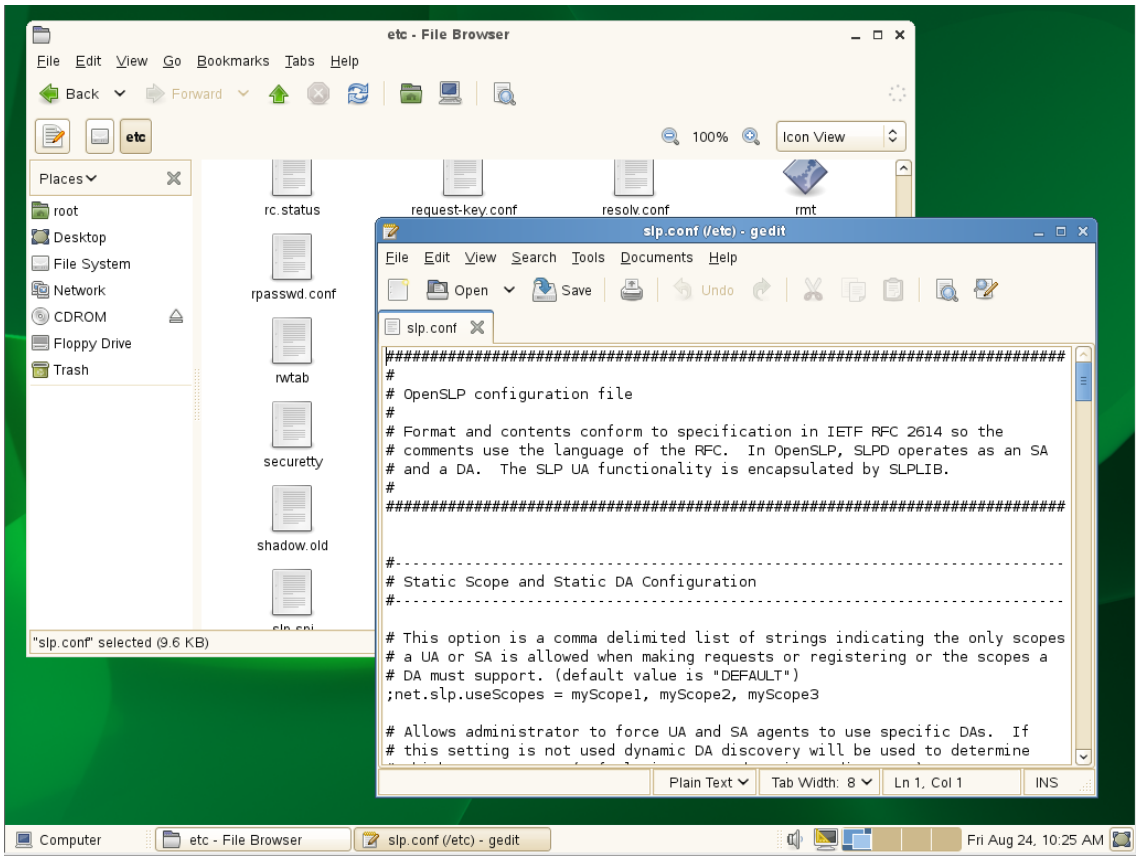
   You can also list additional DA addresses, separated by commas.

4. Return to the "OES eDirectory Services" instructions in the *Installation Guide*.

Configuring for DA Access Before or After Installing the OES Server

Whether you configure DA access before installing OES server or after install of OES, 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.

---

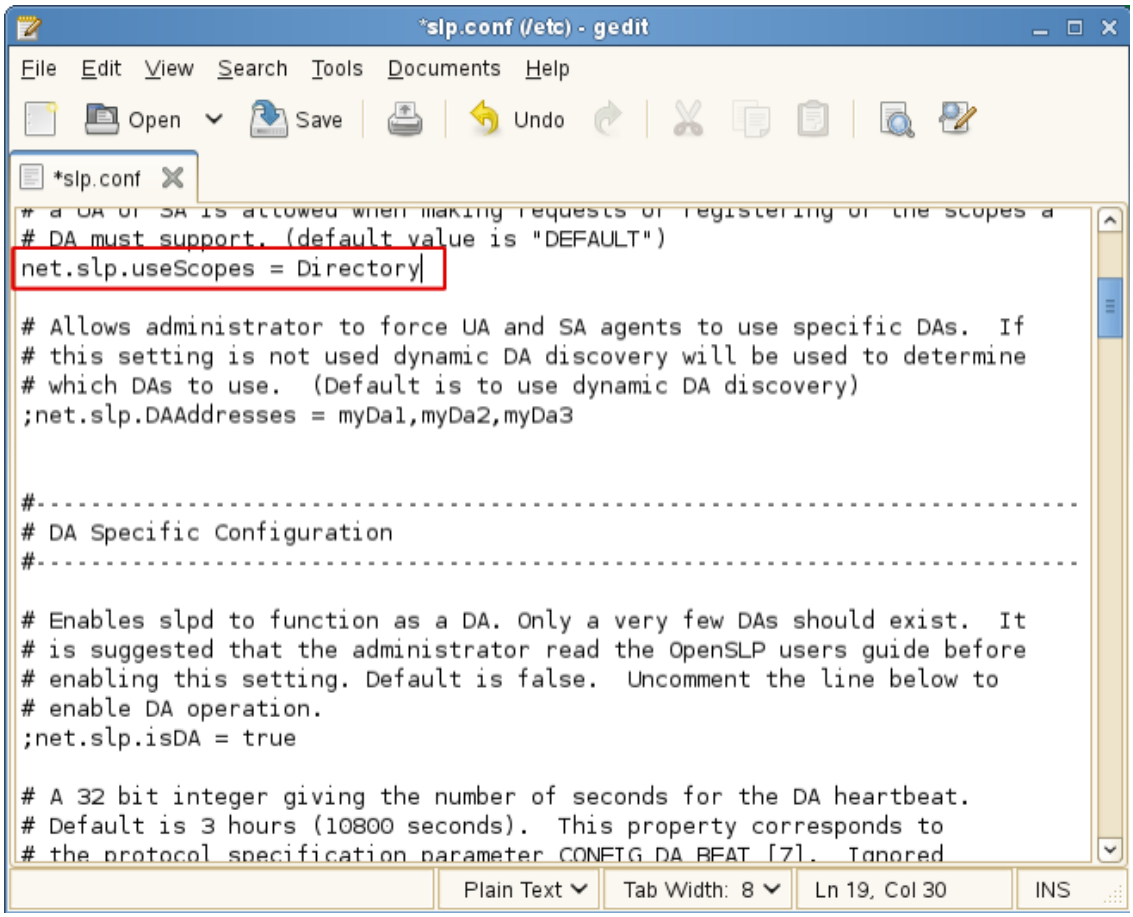
3 Modify the line by removing the semicolon and typing the name or names of the scopes you want this server to have access to.

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
```

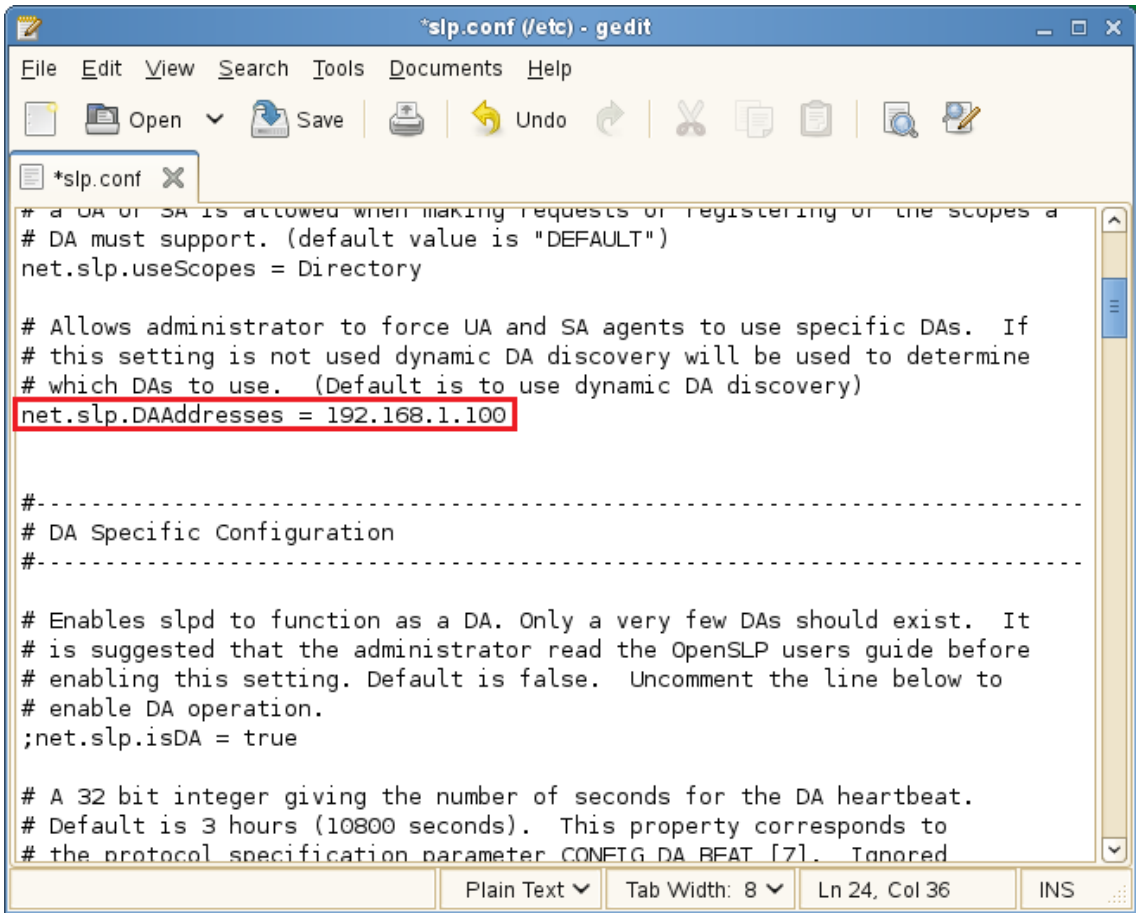


4 Find the following line:

```
;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, 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.

10.5.5 TIDs and Other Help

The SLP configuration file (etc/slp.conf) is self-documented regarding each of the configuration parameters. OpenText 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) 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) 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) explains how to solve the communication problem.
- OpenSLP Documentation on the Web (http://www.openslp.org/documentation.html)provides complete documentation of the OpenSLP services that OES leverages.

11 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 and then to plan a storage solution that meets your file system management needs.

The OES 24.4 Documentation Web site (https://www.microfocus.com/documentation/open-enterprise-server/23.4/) 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 11.1, “Overview of OES Storage,” on page 107
- Section 11.2, “Planning OES File Storage,” on page 112
- Section 11.3, “Coexistence and Migration of Storage Services,” on page 119
- Section 11.4, “Configuring and Maintaining Storage,” on page 121

Other storage-related topics in this guide are:

- Chapter 14, “Access Control and Authentication,” on page 149
- Section 14.2, “Authentication Services,” on page 161
- Appendix 15, “Backup Services,” on page 165
- Chapter 16, “File Services,” on page 167

11.1 Overview of OES Storage

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

- Section 11.1.1, “Databases,” on page 107
- Section 11.1.2, “iSCSI,” on page 108
- Section 11.1.3, “File System Support in OES,” on page 108
- Section 11.1.4, “Storage Basics by Platform,” on page 110
- Section 11.1.5, “Storage Options,” on page 111

11.1.1 Databases

See the MySQL documentation (http://dev.mysql.com/doc) on the Web.

11.1.2 iSCSI

See the topics in "iSCSI for Linux (https://documentation.suse.com/sles/15-SP4/#redirectmsg)" in the SLES online documentation.

11.1.3 File System Support in OES

As shown in Figure 11-1, both OES and NetWare support Novell Storage Services as well as their traditional file systems.

Figure 11-1 *File System Choices on OES and NetWare Servers*

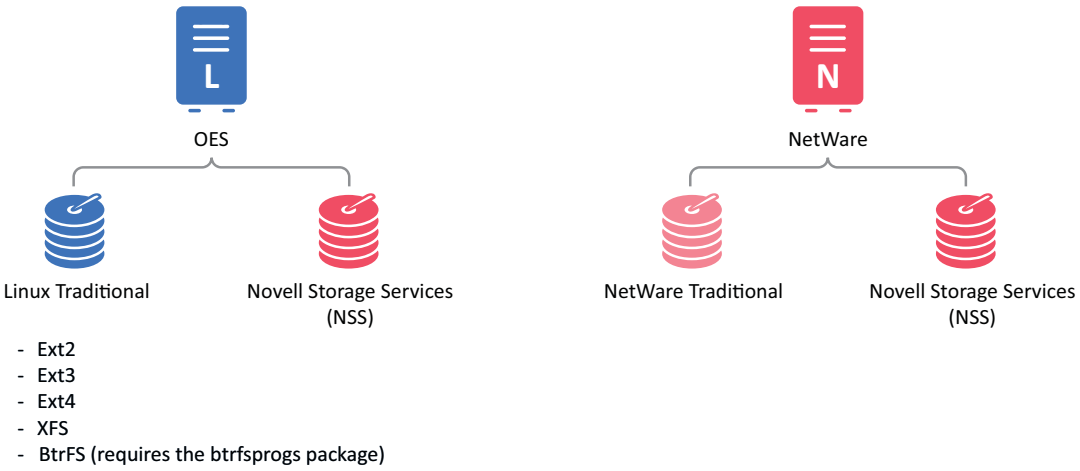


Table 11-1 summarizes OES file system types and provides links to more information.

Table 11-1 *File Systems Available on OES and NetWare Servers*

File System Type	OES	NetWare	Summary	Link for More Information
Linux POSIX File Systems	Y	N	SLES 15 SP4 includes a number of different file systems, the most common of which are Ext3, Ext4, XFS, and Btrfs (requires the btrfsprogs package). OES services are supported on Ext3, Ext4, XFS, and Btrfs.	For an overview of the supported file systems in OES, see "File Systems Overview" in the *OES 2023: File Systems Management Guide*. For an overview of Linux POSIX file systems, see Overview of File Systems in Linux in the *SLES 15: Storage Administration Guide*.
NetWare Traditional File System	N	Y	This is a legacy file system on NetWare servers that supports the Novell file service trustee access control model.	For more information, see the *NW6.5 SP8: Traditional File System Administration Guide*.

File System Type	OES	NetWare	Summary	Link for More Information
Storage Services (NSS)	Y	Y	NSS lets you manage your shared file storage for any size organization. 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. Most of these features are also supported on NSS on Linux. In addition, NSS supports two pool types: NSS32, the traditional NSS type that supports up to 8 Terabytes of data, and NSS64, the new NSS type that supports up to 8 Exabytes. For a feature comparison, see "List of NSS Features" in the *Storage Services File System (NSS) Administration Guide for Linux*.	For an overview of NSS, see "Overview of NSS" in the *Storage Services File System (NSS) Administration Guide for Linux*.

Storage Services (NSS)

The following sections summarize key points regarding NSS:

- "Understanding NSS Nomenclature" on page 109
- "Comparing NSS with Other File Systems" on page 110
- "NSS and Storage Devices" on page 110

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 *Storage Services File System (NSS) Administration Guide for Linux*.

Comparing NSS with Other File Systems

Because OES supports a variety of file systems, you might want to compare their features and benefits as outlined in the following sections of the *Storage Services File System (NSS) Administration Guide for Linux*:

- **NSS Linux vs. NSS NetWare:** "List of NSS Features"
- **NSS Linux vs. NCP Volumes on 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 *Storage Services File System (NSS) Administration Guide for Linux*.

11.1.4 Storage Basics by Platform

The following sections summarize storage basics for Linux and NetWare.

- "Linux and File Systems" on page 110
- "NSS on OES Storage Devices" on page 110
- "NetWare Directories" on page 110
- "NetWare Storage Devices" on page 111

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 2023: File Systems Management Guide*.

NSS on OES Storage Devices

See "Guidelines for NSS Storage" in the *Storage Services File System (NSS) Administration Guide for Linux*.

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 2023: 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*.

11.1.5 Storage Options

The following sections summarize OES storage options.

- "Dynamic Storage Technology" on page 111
- "Direct-Attached Storage Options (NSS and Traditional)" on page 111
- "Advanced Storage Options" on page 112

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 OES 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 SSH or OES 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.

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 *Dynamic Storage Technology Administration Guide*.

Direct-Attached Storage Options (NSS and Traditional)

As shown in Figure 11-1 on page 108, you can install traditional volumes and 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 2015 SP1: Storage and File Services Overview*.

Advanced Storage Options

NSS volumes support the following advanced storage solutions, as documented in the *OES 2015 SP1: Storage and File Services Overview*.

- Network Attached Storage Solutions

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

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

- Storage Area Network Solutions

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

  - 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: Multipath I/O software resolves multiple paths to a device into a single device and manages the traffic flow across the paths transparently for file systems on the devices. NSS on Linux does not provide an LVM-based software solution for managing multiple paths like the Media Manager multipath solution on NetWare. Instead, you can use Linux multipath I/O tools to configure and manage multiple paths for devices where you want to create NSS software RAIDS, pools, and volumes.
  - 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 *Storage Services File System (NSS) Administration Guide for Linux*.
  - Server Clusters: With 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 Cluster Services for Linux Administration Guide*. To convert a NetWare cluster to an OES cluster, see the *OES 2015 SP1: Novell Cluster Services NetWare to Linux Conversion Guide*.

11.2 Planning OES File Storage

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

- Section 11.2.1, "Directory Structures," on page 113
- Section 11.2.2, "File Service Support Considerations," on page 113
- Section 11.2.3, "General Requirements for Data Storage," on page 113

- Section 11.2.4, “OES Storage Planning Considerations,” on page 113
- Section 11.2.5, “NSS Planning Considerations,” on page 119

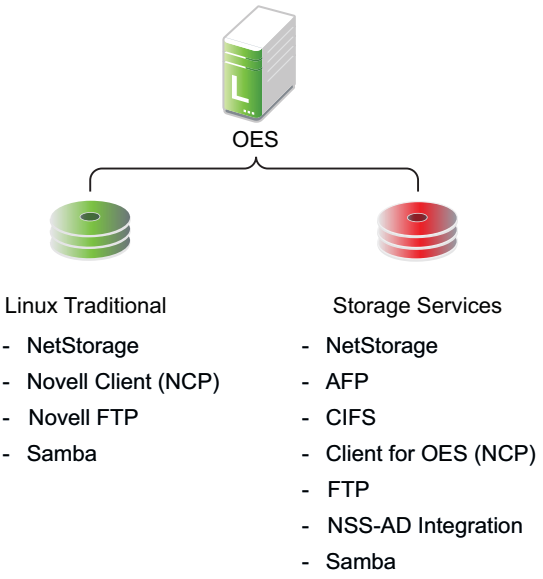
11.2.1 Directory Structures

To plan the directory structures you need on OES, see “Understanding Directory Structures in Linux POSIX File Systems” in the *OES 2023: File Systems Management Guide*.

11.2.2 File Service Support Considerations

Figure 11-2 shows which file services can access which volume types.

Figure 11-2 *File Services Supported on Volume Types*



11.2.3 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 2015 SP1: Storage and File Services Overview*.

11.2.4 OES 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 servers, and includes the following topics:

- “The Workgroup Environment” on page 114
- “File System Support” on page 114
- “File Access Protocol Support” on page 117
- “OES Workloads” on page 118

The Workgroup Environment

When selecting a file system, it is important to understand the environment in which it operates. For OES, 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 offers support for five six systems: Storage Services (NSS), Btrfs, Ext 2, Ext3, Ext4, and XFS. Following is an explanation of each file system and the pros and cons of using them in the workloads supported by OES.

- "Storage Services (NSS)" on page 114
- "Btrfs" on page 115
- "Ext2" on page 116
- "Ext3" on page 116
- "Ext4" on page 116
- "XFS" on page 117

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
- OES 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 Storage Services file system is used in NetWare 5.0 and above, is included in the 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 OES 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.

Both eDirectory and Active Directory are supported as identity sources, and OES enables the NSS file system to accept Active Directory identities as trustees. Active Directory users can authenticate to Active Directory and natively access the NSS resources using the CIFS protocol.

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 http and ftp files.
/tmp	Contains temporary files.
/var/log	Contains log files.
/var/opt	Contains run-time variable data for /opt.
/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 7.4, “Xen VMs Need Ext2 for the System /Boot Volume,” on page 38.

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 12 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.

Ext4

- Faster filesystem checking and recovery
- Best for extremely large file systems
- Online resizing
- Journaled
- POSIX extended access control

Ext4 is created as a successor to the popular Ext3 file system to address some of its limitations and shortcomings. Ext4 is a stable and default file system in many Linux distributions for desktop and server environments. Ext4 also offers strong reliability and data integrity features.

In conclusion, Ext4 is an established and well-tested file system suitable for Linux systems. It is a widely supported file system with a large user community, that can quickly find and resolve any issues or bugs.

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 offers support for a variety of file access protocols.

- **CIFS:** The Common Internet File Services (CIFS) protocol is the protocol for Windows networking and file services.

  OES CIFS is a ported version of the CIFS file service traditionally available only on NetWare. It supports OES Trustee model access for NSS volumes and Dynamic Storage Technology shadow volumes

  Both eDirectory and Active Directory users can natively access NSS resources using the CIFS protocol.
- **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 16.5, “FTP (Pure-FTPd) and OES,” on page 177.
- **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 OES Trustee Model and inheritance plus visibility when it runs on traditional POSIX file systems such as Ext3, Ext4, 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 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 11-2 *File System Support per Workload*

Workload Type	NSS File System	Btrfs	Ext3 File System	Ext4 File System	XFS File System
CIFS (OES CIFS)	Supported	Not Supported	Not Supported	Not Supported	Not Supported
Cluster Services	Recommended	Supported	Recommended	Recommended	Recommended
Collaboration (GroupWise)	Supported	Supported	Recommended	Recommended	Supported
Dynamic Storage Technology	Supported	Not Supported	Not Supported	Not Supported	Not Supported
File serving – Application server	Supported	Supported	Supported	Supported	Recommended
NCP (Client for Open Enterprise Server)	Recommended	Supported	Supported	Supported	Supported
NSS-AD Integration	Supported	Not Supported	Not Supported	Not Supported	Not Supported
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 11-2.

- "Collaboration (GroupWise)" on page 118
- "Dynamic Storage Technology" on page 119
- "File Serving" on page 119
- "Cluster Services" on page 119
- "Printing (iPrint)" on page 119

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 Ext4 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. Ext4 and XFS would be good choices in this environment. For file serving to end user workstations, the access control and security management capabilities of the NSS file systems with CIFS, and NCP file access protocols are important.

The NSS model does better than the other file systems for very large numbers of users. It allows for security between users and also allows for very fine granular sharing between given users and groups. NSS includes a visibility feature implemented in the file system that prevents unauthorized users from even seeing subdirectory structures they don't have rights to access.

Cluster Services

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.

11.2.5 NSS Planning Considerations

To plan for NSS volumes—including prerequisites and security considerations—see "Planning NSS Storage Solutions " in the *Storage Services File System (NSS) Administration Guide for Linux*.

11.3 Coexistence and Migration of Storage Services

The following sections summarize the coexistence and migration issues related to storage services.

- Section 11.3.1, "Databases," on page 119
- Section 11.3.2, "OES File System Options," on page 120

11.3.1 Databases

The SUSE Linux Enterprise Server 15 (SLES 15) SP4 platform on which OES services are installed, includes two open source databases:

- "MySQL" on page 120
- "PostgreSQL" on page 120

NOTE: Full OES support of these databases requires a product-specific OpenText support contract. Documentation and support are available through open source communities as outlined below.

MySQL

The SLES 15 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.

For overview of MySQL and for information about configuring it with Cluster Services, see "Configuring MySQL with Novell Cluster Services" in the *OES 2015 SP1: Web Services and Applications Guide*.

PostgreSQL

The more powerful PostgreSQL database server also comes with SLES 15. See the PostgreSQL documentation on the Web.

11.3.2 OES File System Options

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

- "NSS Volumes" on page 120
- "Linux POSIX File Systems" on page 121

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 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 *Storage Services File System (NSS) 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 *Storage Services File System (NSS) Administration Guide for Linux*.

Both eDirectory and Active Directory are supported as identity sources, and OES enables the NSS file system to accept eDirectory and Active Directory identities as trustees. For more information, see "Upgrading the NSS Media Format" in the *Storage Services File System (NSS) Administration Guide for Linux*.

Linux POSIX File Systems

IMPORTANT: Users can access data storage on OES servers through a number of methods. For more information, see “Overview of File Services” on page 167.

OES includes tools and services that help bridge the gap between traditional OES file services and Linux POSIX file services.

- “Management Tools” on page 121
- “NCP Server” on page 121
- “Novell Cluster Services” on page 121

Management Tools

Using NSSMU and the 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 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 Client for Open Enterprise Server 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 *NCP Server for Linux Administration Guide*.

Novell Cluster Services

For information about clustering LVM2 volume groups with Cluster Services, see “Configuring and Managing Cluster Resources for Shared LVM Volume Groups” in the *OES Cluster Services for Linux Administration Guide*.

11.4 Configuring and Maintaining Storage

- Section 11.4.1, “Managing Directories and Files,” on page 121
- Section 11.4.2, “Managing NSS,” on page 122
- Section 11.4.3, “Optimizing Storage Performance,” on page 124

11.4.1 Managing Directories and Files

To learn about managing directories and files on an OES server, see “Understanding Directory Structures in Linux POSIX File Systems” in the *OES 2023: File Systems Management Guide* and “Understanding Directory Structures for the NSS File System” in the *OES 2023: File Systems Management Guide*.

11.4.2 Managing NSS

Use the links in Table 11-3 to find information on the many management tasks associated with NSS volumes.

Table 11-3 *NSS Management*

Category/Feature	Description	Link
Compression	Conserve disk space and increase the amount of data a volume can store.	"Managing Compression on NSS Volumes" in the *Storage Services File System (NSS) Administration Guide for Linux*
Console Commands	Manage NSS volumes in an OES terminal console via the NSS Console (`nsscon`) utility. You can also issue Linux Volume Manager (NLVM) command line commands at the console prompt and in scripts.	"NSS Commands" and "NSS Utilities" in the *Storage Services File System (NSS) 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.	*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 *Storage Services File System (NSS) 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 *Storage Services File System (NSS) Administration Guide for Linux*
Monitoring	Monitor NSS file systems.	"Monitoring the Status of the NSS File System and Services" in the *Storage Services File System (NSS) 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 *Storage Services File System (NSS) Administration Guide for Linux*
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 23.4: NLVM Reference*

Category/Feature	Description	Link
Partitions	Manage partitions on NSS volumes.	"Managing Partitions" in the *Storage Services File System (NSS) Administration Guide for Linux*
Pools	Create and manage NSS pools.	"Managing NSS Pools" in the *Storage Services File System (NSS) Administration Guide for Linux*
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.	"Move" in the *OES 23.4: NLVM Reference* "Moving a Pool with NSSMU and NLVM" in the *Storage Services File System (NSS) 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 *Storage Services File System (NSS) Administration Guide for Linux*
RAID	Create and manage software RAIDs.	"Managing NSS Software RAID Devices" in the *Storage Services File System (NSS) 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 *Storage Services File System (NSS) Administration Guide for Linux*
Snapshots	Take pool snapshots.	"Managing NSS Pool Snapshots" in the *Storage Services File System (NSS) 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 *Storage Services File System (NSS) Administration Guide for Linux*
Troubleshooting	Troubleshoot NSS on OES and NetWare 6.5 SP8.	"Troubleshooting the NSS File System" in the *Storage Services File System (NSS) 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 *Storage Services File System (NSS) Administration Guide for Linux*
Volumes	Create and manage NSS volumes in NSS pools.	"Managing NSS Volumes" in the *Storage Services File System (NSS) Administration Guide for Linux*

11.4.3 Optimizing Storage Performance

See “Tuning NSS Performance” in the *Storage Services File System (NSS) Administration Guide for Linux*.

12 eDirectory, LDAP, NSS AD, and Domain Services for Windows

This section discusses the following topics:

- Section 12.1, “Overview of Directory Services,” on page 125
- Section 12.2, “eDirectory,” on page 126
- Section 12.3, “LDAP (eDirectory),” on page 128
- Section 12.4, “NSS AD Support,” on page 128
- Section 12.5, “Why Both NSS AD and DSfW?,” on page 129
- Section 12.6, “Domain Services for Windows,” on page 129

12.1 Overview of Directory Services

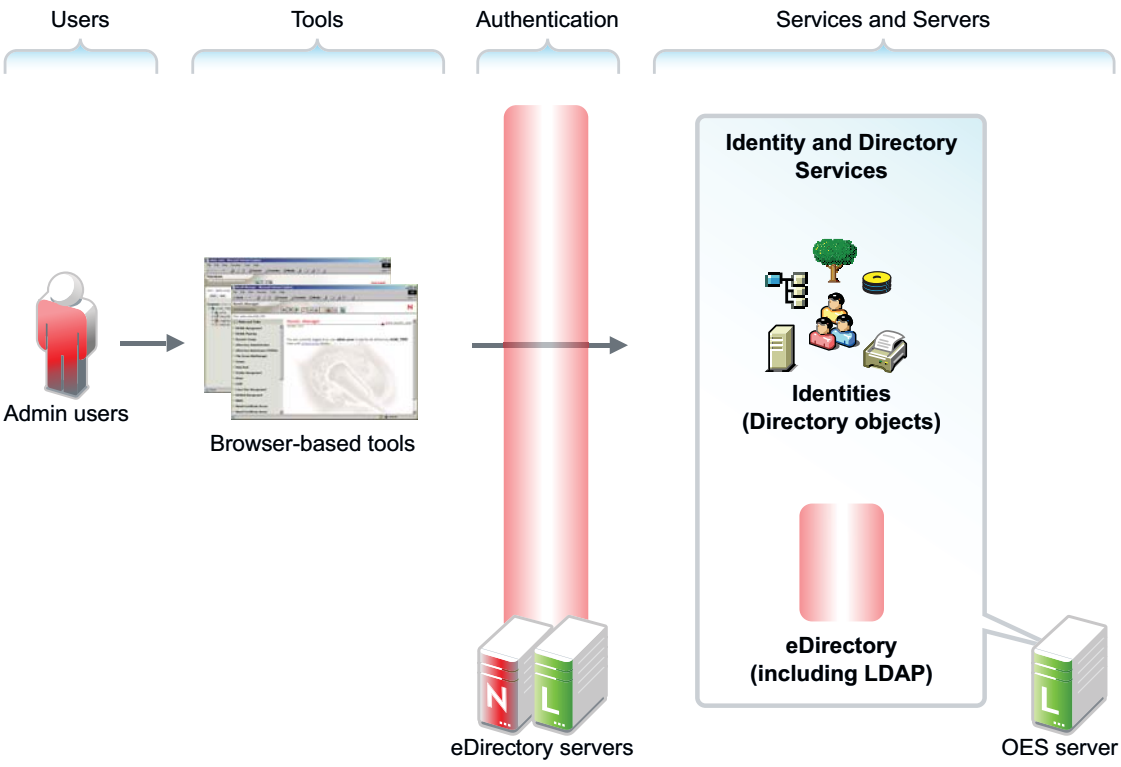
Storing and managing network identities in directory services is a fundamental expectation for networking.

In the simplest terms, 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.

Figure 12-1 *eDirectory Overview*



12.2 eDirectory

eDirectory is the central, key component of 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 12.2.1, “Installing and Managing eDirectory on OES,” on page 126
- Section 12.2.2, “Planning Your eDirectory Tree,” on page 127
- Section 12.2.3, “eDirectory Coexistence and Migration,” on page 127

12.2.1 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 127
- “iManager” on page 127

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*.

12.2.2 Planning Your eDirectory Tree

If you don't have eDirectory installed on your network, it is critical that you and your organization take time to plan and design your eDirectory tree prior to installing OES.

For detailed information on getting started using eDirectory, see "Designing Your NetIQ eDirectory Network" in the *NetIQ eDirectory Administration Guide*.

To learn what's new in eDirectory, see the NetIQ eDirectory 9.2.8 Release Notes (https://www.netiq.com/documentation/edirectory-92/edirectory928_releasenotes/data/edirectory928_releasenotes.html).

12.2.3 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. OES has consistently provided the migration tools and support required to migrate to new eDirectory versions.

OES includes eDirectory. For those upgrading an existing NetWare 6.5 SP6 server, eDirectory 8.7.3 is still available. The new NetWare installations require the eDirectory version that OES uses.

For complete coexistence and migration information and instructions, see "Migrating to eDirectory 9.2" in the *NetIQ eDirectory Installation Guide*.

12.3 LDAP (eDirectory)

This section contains information about LDAP support in OES.

- Section 12.3.1, “Overview of eDirectory LDAP Services,” on page 128
- Section 12.3.2, “Planning eDirectory LDAP Services,” on page 128
- Section 12.3.3, “Migration of eDirectory LDAP Services,” on page 128
- Section 12.3.4, “eDirectory LDAP Implementation Suggestions,” on page 128

12.3.1 Overview of eDirectory LDAP Services

Lightweight Directory Access Protocol (LDAP) Services for 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.

12.3.2 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 Administration Guide*.

12.3.3 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 Administration Guide*.

12.3.4 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 Administration Guide*.

12.4 NSS AD Support

Beginning with OES 2015, you can provide native CIFS access to NSS volumes by deploying the NSS AD Integration service.

For more information, see the *NSS AD Administration Guide*.

12.5 Why Both NSS AD and DSfW?

NSS AD Integration and Domain Services for Windows (DSfW) are very different services, from a directory standpoint.

Also, DSfW is broader in scope than NSS AD.

- **NSS AD:** Provides AD users with native CIFS access to NSS-based storage.
- **DSfW:** Provides eDirectory users with native access to Windows servers and services, including NTFS-based storage.

12.6 Domain Services for Windows

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 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 Client for Open Enterprise Server 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 12.6.1, “Graphical Overview of DSfW,” on page 129
- Section 12.6.2, “Planning Your DSfW Implementation,” on page 131
- Section 12.6.3, “Implementing DSfW on Your Network,” on page 132

12.6.1 Graphical Overview of DSfW

- “User Management” on page 130
- “Storage Management” on page 131

User Management

Figure 12-2 *DSfW User Management Overview*

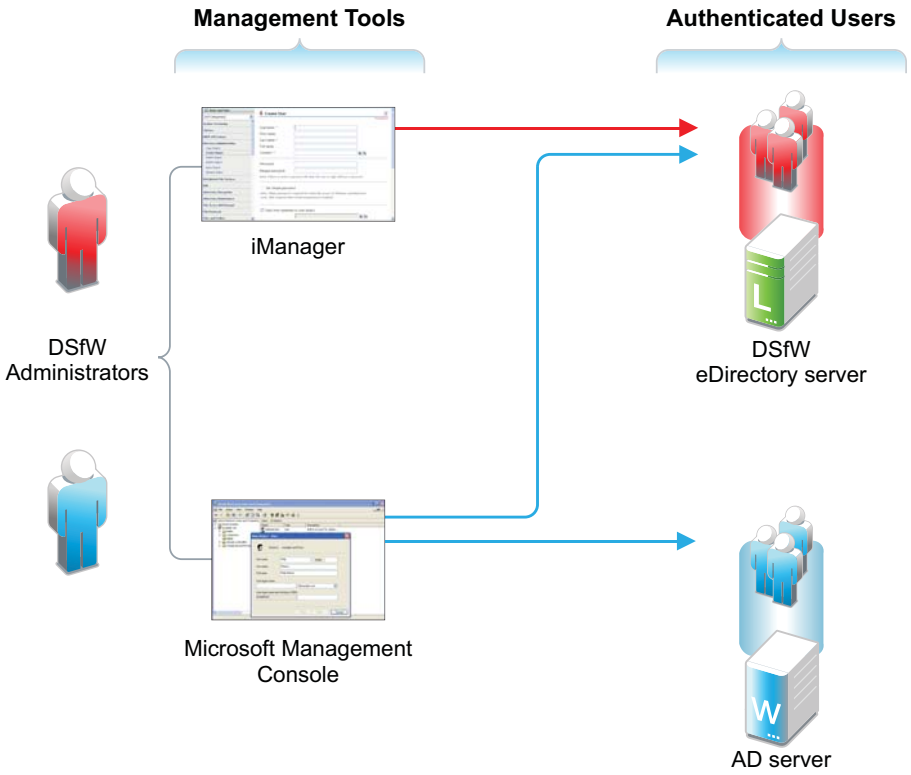


Table 12-1 *DSfW User Management*

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 12-3 *DSfW Storage Management Overview*

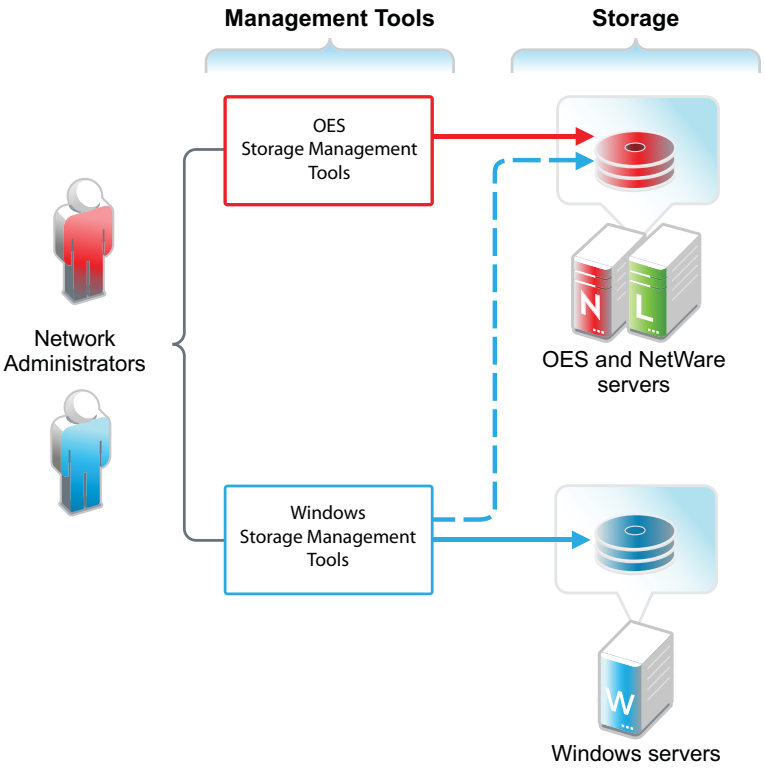


Table 12-2 *DSfW Storage Management*

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. 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.	Storage devices on OES servers can be either NSS or traditional Linux volumes. Samba management standards apply to both volume types.

12.6.2 Planning Your DSfW Implementation

For planning information, see the *Domain Services for Windows Administration Guide*.

12.6.3 Implementing DSfW on Your Network

This section highlights some of the potential caveats to consider when installing DSfW. For complete information, see the *Domain Services for Windows Administration Guide*, especially the "Troubleshooting DSfW" section.

- "Implement Universal Password Before DSfW in a Name-Mapped Scenario" on page 132
- "DSfW Must Be Installed at the Root of an eDirectory Partition" on page 132
- "Hierarchical Placement of Users in the eDirectory Tree" on page 132
- "OES Service Limitations" on page 132
- "Install DSfW on a New OES Server When Possible" on page 132
- "DNS Configuration" on page 133

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 Client for Open Enterprise Server 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 Service Limitations

Only designated OES services can be installed on a DSfW server. For more information, see "Unsupported Service Combinations" in the *Domain Services for Windows Administration Guide*.

Install DSfW on a New OES Server When Possible

Because of the service limitations mentioned in OES Service Limitations, OES 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.

13 Users and Groups

Networks exist to serve users and groups of users. Open Enterprise Server (OES) provides strong user and group management through eDirectory and its associated technologies.

- Section 13.1, “Creating Users and Groups,” on page 135
- Section 13.2, “Linux User Management: Access to Linux for eDirectory Users,” on page 135
- Section 13.3, “Identity Management Services,” on page 144
- Section 13.4, “Using the Identity Manager 4.8 Bundle Edition,” on page 144

13.1 Creating Users and Groups

OES services require you to create User objects to represent the users on your system. The Linux User Management (LUM) component on OES also requires you to create a LUM-enabled Group object to which you can assign the users.

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.

For detailed information on understanding, creating, and managing the various objects your organization might require, see the *NetIQ eDirectory Administration Guide*.

13.2 Linux User Management: Access to Linux for eDirectory Users

---

NOTE: Beginning with OES 2015, a new service named the Novell Identity Translator (NIT) is introduced, which is associated with the Linux User Management.

NIT represents a new approach to the service that LUM provides and works seamlessly with LUM to provide access to CIFS.

For more information about NIT, see NIT (Novell Identity Translator) in the NSS AD Administration Guide.

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, OES 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 OES LUM and cover the following topics:

- Section 13.2.1, “Overview,” on page 136
- Section 13.2.2, “LUM Changes,” on page 140
- Section 13.2.3, “Planning,” on page 140
- Section 13.2.4, “LUM Implementation Suggestions,” on page 141

13.2.1 Overview

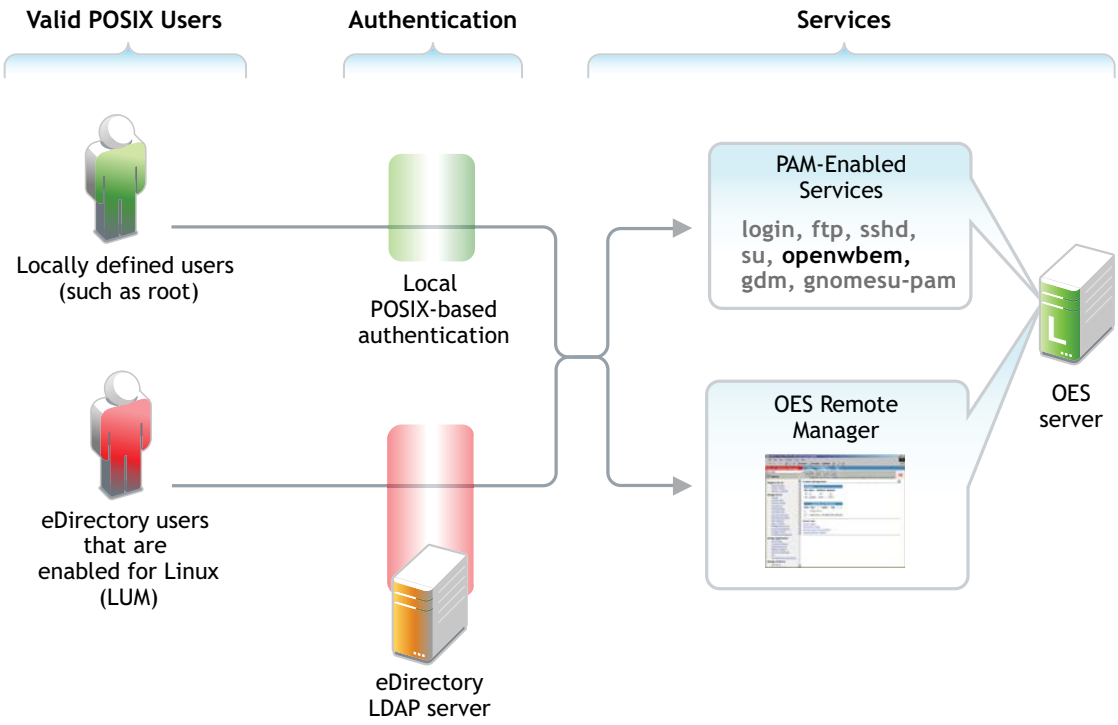
The topics in this section are designed to help you understand when LUM-enabled access is required so that your network services are accessible and work as expected. For more information about Linux User Management, see “Overview” in the *Linux User Management Administration Guide*.

- “A Graphical Preview of Linux User Management” on page 136
- “Linux Requires POSIX Users” on page 137
- “Linux Users Can Be Local or Remote” on page 138
- “The root User Is Never LUM-Enabled” on page 138
- “About Service Access on OES” on page 138
- “OES Services That Require LUM-Enabled Access” on page 138
- “OES Services That Do Not Require LUM-Enabled Access But Have Some LUM Requirements” on page 140
- “OES Services That Do Not Require LUM-enabled Access” on page 140
- “LUM-Enabling Does Not Provide Global Access to ALL OES Servers” on page 140
- “LUM-Enabling Required for Full Administrative Access” on page 140

A Graphical Preview of Linux User Management

Figure 13-1 illustrates how Linux User Management controls access to the OES server.

Figure 13-1 *LUM Provides POSIX Access for eDirectory Users*



The following table explains the information presented in Figure 13-1.

Table 13-1 *Linux User Management*

Valid POSIX Users	Authentication	eDirectory Authenticated Services
Some services on OES servers must be accessed by POSIX users. eDirectory users can function as POSIX users if they are enabled for Linux access (LUM).	When the system receives an action request, it can authenticate both local POSIX users and users who have been enabled for Linux access.	Users can potentially access PAM-enabled services, Samba shares, and OES Remote Manager as either local or eDirectory users. By default, only the `sfcb` 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.

- **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 OES Remote Manager and perform other system management tasks as the `root` user.

About Service Access on OES

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 141.

OES Services That Require LUM-Enabled Access

Some services on an OES server require that eDirectory users be LUM-enabled to use them:

- **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 19.2.2, "User Restrictions: Some OES Limitations," on page 203.

The core utilities available for PAM-enablement are summarized in Table 13-2.

Table 13-2 *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.
`sfcb`	Local host	Required for iPrint, NSS, SMS, OES 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`	◆ OES server ◆ SSH session with OES server	Temporarily become another user. This is most often used to temporarily become the `root` user, who is not a LUM user and is, therefore, not affected by LUM.

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 OES 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:

- **NSS:** eDirectory users that access NSS volumes directly through NCP (the Client for Open Enterprise Server) are not required to be LUM-enabled.

OES Services That Do Not Require LUM-enabled Access

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

- iPrint
- NCP Client to an NCP Volume
- NCP Client to an NSS Volume
- CIFS

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 142.

For more information on LUM, see the *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.

13.2.2 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.

13.2.3 Planning

The following sections summarize LUM planning considerations.

- "eDirectory Admin User Is Automatically Enabled for Linux Access" on page 141
- "Planning Which Users to Enable for Access" on page 141
- "Be Aware of System-Created Users and Groups" on page 141

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 138.
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 J, "System User and Group Management in OES," on page 239.

13.2.4 LUM Implementation Suggestions

The following sections summarize LUM implementation considerations.

- "About Enabling eDirectory Users for Linux Access" on page 141
- ""UNIX Workstation" and "Linux Workstation" Are the Same Thing" on page 142
- "Enabling eDirectory Groups and Users for Linux Access" on page 142

About Enabling eDirectory Users for Linux Access

You can enable eDirectory users for Linux User Management by using either iManager 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.

- **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 *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 142
- “Using iManager to Bulk-Enable Users in a LUM Group” on page 142
- “Using iManager to Bulk-Enable Users in a Container” on page 143
- “Using LUM Utilities at the Command Prompt” on page 143

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

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 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 Linux User Management Administration Guide.

13.3 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 Open Enterprise Server (OES) leverage 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 Client for Open Enterprise Server 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 16.6, “NCP Implementation and Maintenance,” on page 187 and Chapter 17, “Print Services,” on page 191.
- 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 13.2, “Linux User Management: Access to Linux for eDirectory Users,” on page 135.
- 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 13.4, “Using the Identity Manager 4.8 Bundle Edition,” on page 144.

13.4 Using the Identity Manager 4.8 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 13.4.1, “What Am I Entitled to Use?,” on page 144
- Section 13.4.2, “System Requirements,” on page 145
- Section 13.4.3, “Installation Considerations,” on page 145
- Section 13.4.4, “Getting Started,” on page 145
- Section 13.4.5, “Activating the Bundle Edition,” on page 146

13.4.1 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
- Identity Manager Driver for GroupWise

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*.

13.4.2 System Requirements

For the latest Identity Manager system requirements, see Technical Information page.

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.

13.4.3 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 146.

NOTE: To install IDM 4.8 + 4.8HF1 Bundle Edition, download the IDM 4.8 Standard Edition and use the IDM 4.8 Bundle Edition activation keys.

13.4.4 Getting Started

The following sections from the Identity Manager documentation will help you plan, install, and configure your Identity Manager Bundle Edition.

- Overview
- Planning
- Installing Identity Manager
- Installing Active Directory and eDirectory Drivers
- Password Synchronization across Connected Systems

See NetIQ Identity Manager Understanding Policies Guide for information about customizing your Identity Manager implementation.

13.4.5 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 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. Log in to OpenText Customer Center web site, and go to **Software > Entitled Software**.
2. Go to Identity Manager software and click the license download link, and then complete one of the following actions:
   - 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 ensure 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-----).
3. Log in to iManager.
4. Select **Identity Manager > Identity Manager Overview**.
5. To select a driver set in the tree structure, click the browse icon.
6. On the **Identity Manager Overview** page, click the driver set that contains the driver that you want to activate.
7. On the **Driver Set Overview** page, click **Activation** > **Installation**.
8. Select the driver set where you want to activate an Identity Manager component, and then click **Next**.
9. (Conditional) If you saved the Product Activation Credential file, specify the saved location.
10. (Conditional) If you copied the contents of the Product Activation Credential file, paste the contents into the text area.
11. Click **Next**.
12. 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 Reviewing Product Activations for Identity Manager and Drivers.

14 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 14.1, “Controlling Access to Services,” on page 149
- Section 14.2, “Authentication Services,” on page 161

14.1 Controlling Access to Services

IMPORTANT: With NSS-AD integration in OES 2015, OES CIFS supports Kerberos authentication for Active Directory users accessing NSS volumes. For more information, see the *NSS AD Administration Guide*.

OES supports a number of options for service access, including:

- Web browsers.
- File managers and applications on Linux, Macintosh, and Windows workstations.
- Client for Open Enterprise Server 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 14.1.1, “Overview of Access Control,” on page 150
- Section 14.1.2, “Planning for Service Access,” on page 156
- Section 14.1.3, “Coexistence and Migration of Access Services,” on page 159
- Section 14.1.4, “Access Implementation Suggestions,” on page 159
- Section 14.1.5, “Configuring and Administering Access to Services,” on page 159

14.1.1 Overview of Access Control

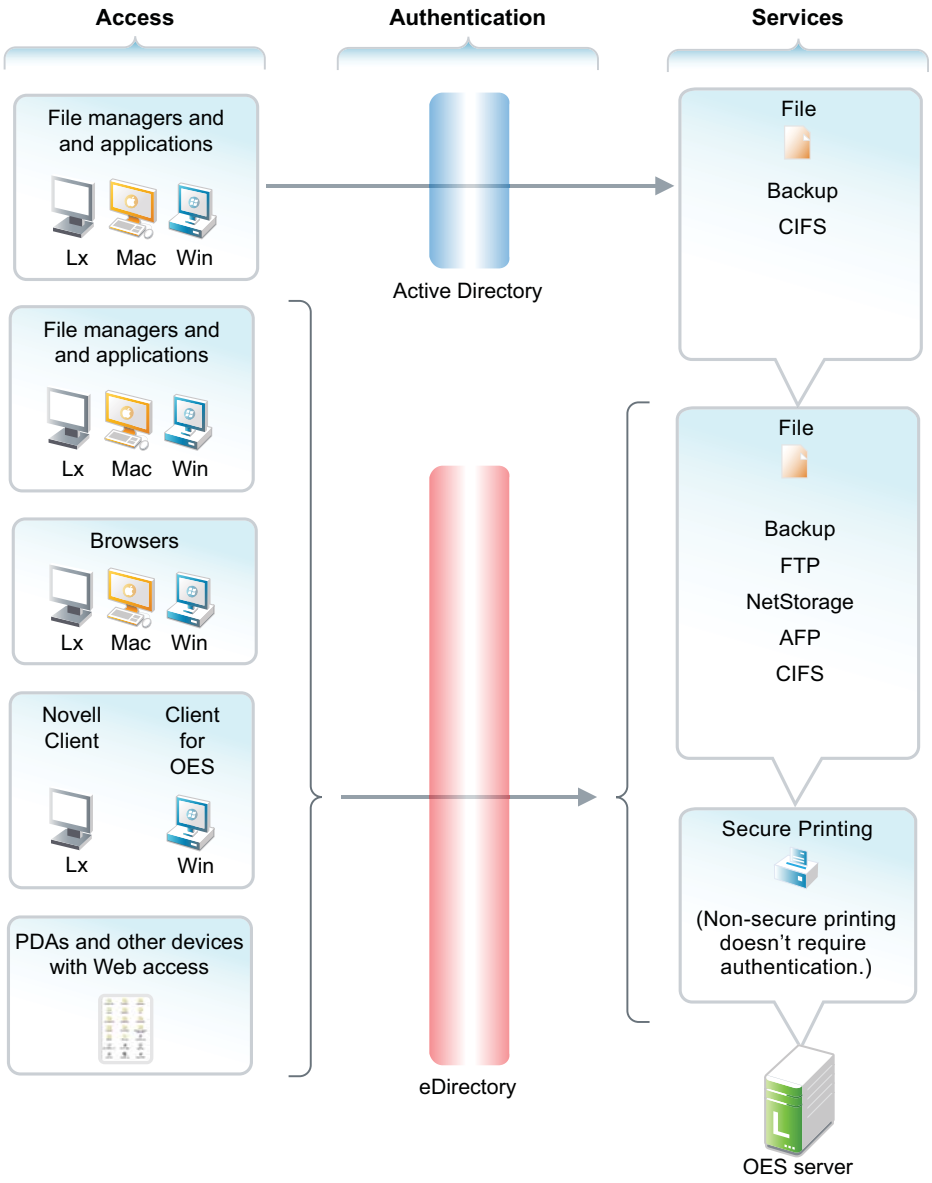
The following sections present overview of methods for accessing Open Enterprise Server services.

- "Access to OES Services" on page 150
- "Access Control Options in OES" on page 152
- "The Traditional Novell Access Control Model" on page 153
- "NSS Access Control on OES" on page 154
- "Client for Open Enterprise Server (NCP File Services) Access" on page 155
- "eDirectory User Access to OES Servers" on page 156
- "Active Directory User Access to OES Servers" on page 156

Access to OES Services

Figure 14-1 illustrates the access methods supported by OES services. eDirectory provides authentication to each service.

Figure 14-1 *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 CIFS and Windows workstations use the CIFS protocol for file services.
- Client for Open Enterprise Server uses the NetWare Core Protocol (NCP) to provide the file services.

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 158.

Access Control Options in OES

Because OES offers both traditional OES 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 14-1 provides links to documentation that discusses OES access control features.

Table 14-1 *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" (https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-security-acls.html) in the *SLES Security Guide* (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-security.html)
Aligning NCP and POSIX access rights	How to approximate the OES access control model on POSIX file systems.	"Section 16.4, "Aligning NCP and POSIX File Access Rights," on page 174"
Directory and file attributes	Directory and file attributes on NSS volumes.	"Understanding Directory and File Attributes for NSS Volumes" in the *OES 2023: File Systems Management Guide*
File system trustee rights	File system trustee rights on NetWare (NSS and traditional volumes), including how file system trustee rights work.	"Understanding the OES Trustee Model for File System Access" in the *OES 2023: File Systems Management Guide*
OES 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 *OES 2023: File Systems Management Guide*
POSIX file system rights and attributes on Linux	How to configure file system attributes on OES servers.	"Access Control Lists in Linux" (https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-security-acls.html) in the *SLES Security Guide* (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-security.html)
Security Equivalence in eDirectory	The concept of Security Equivalence in eDirectory.	"Security Equivalence" in the *OES 2023: File Systems Management Guide*

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 OES 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 14-2.

Figure 14-2 *Directory and File Access under the NetWare Access Control Model*

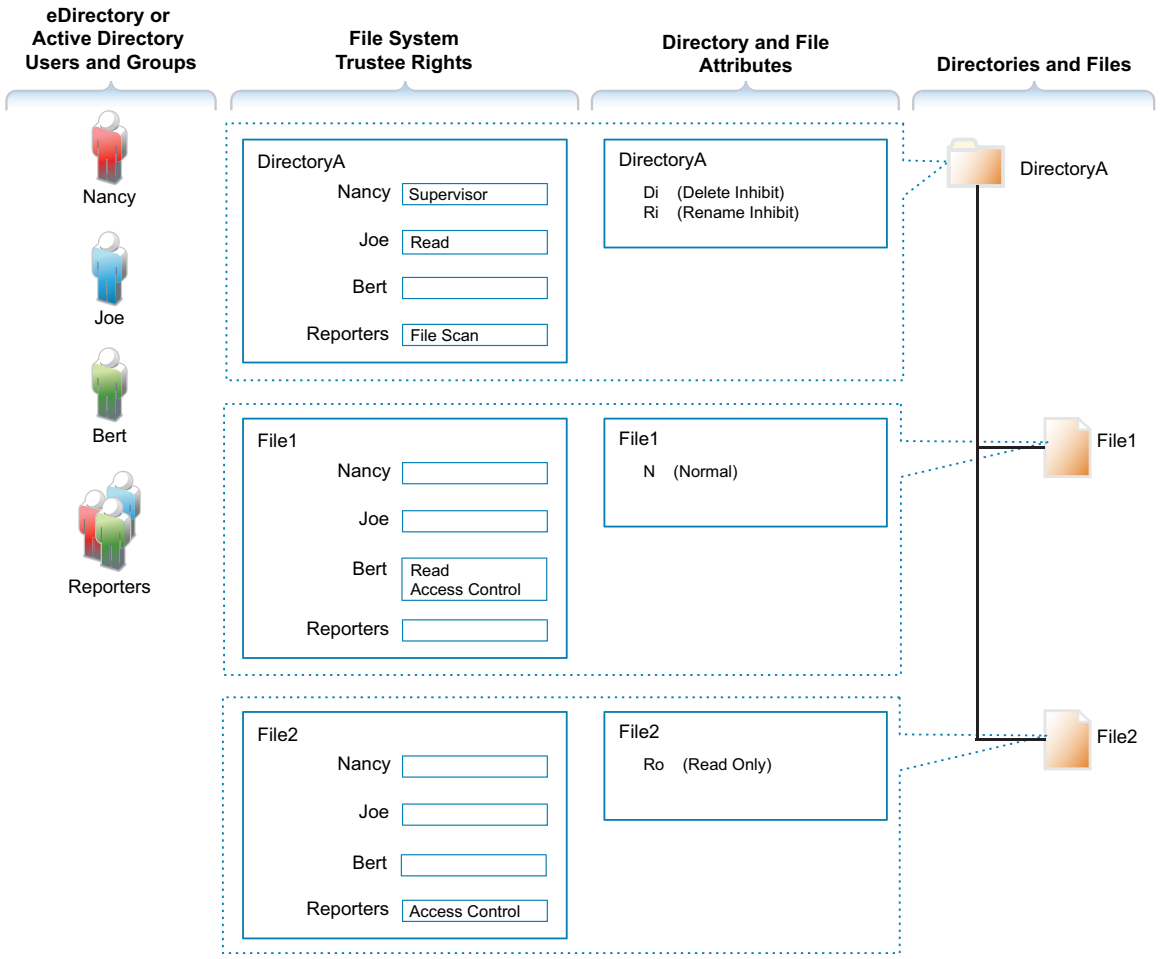


Table 14-2 explains the effective access rights illustrated in Figure 14-2.

Table 14-2 *Access Rights Explanation*

eDirectory or Active Directory Users and Groups	File System Trustee Rights	Directory and File Attributes	Directories and Files
eDirectory and AD users and groups gain access to the file system through their respective authentication mechanisms.	File system trustee rights govern access and usage for the directory or file to which the rights are granted. Trustee rights are overridden by directory and file attributes. 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. Of course, because she has the Supervisor right, Nancy could modify the file attributes so that File2 could then be deleted.	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. For example, a file that has the Read Only attribute is Read Only for all users. Attributes can be set by any trustee that has the Modify trustee right to the directory or file.	The possible actions by the users and group shown in this example are as follows: ◆ 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. 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. ◆ 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. Joe also has rights to open and read any files in DirectoryA and to execute any applications in DirectoryA. ◆ 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. Bert also has rights to open and read File1 and to execute it if it's an application. And Bert has rights to grant any eDirectory user access to File1. ◆ Because all three users are members of the Reporters group, they can grant any eDirectory user access to File2. Of course, for Nancy this is redundant because she has the Supervisor right at the directory level.

NSS Access Control on OES

Table 14-3 provides links to documentation that discusses the various NSS-specific access control features.

Table 14-3 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 *OES 2023: File Systems Management Guide*
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 *OES 2023: File Systems Management Guide*

Client for Open Enterprise Server (NCP File Services) Access

If you have not already determined whether to use the Client for Open Enterprise Server on your network, we recommend that you consider the following information:

- "About the Client for Open Enterprise Server" on page 155
- "Is the Client for Open Enterprise Server Right for Your Network?" on page 155

About the Client for Open Enterprise Server

The Client for Open Enterprise Server extends the capabilities of Windows desktops with access to OES servers.

After installing Client for Open Enterprise Server software, users can enjoy the full range of OES services, such as

- Authentication via NetIQ eDirectory
- Network browsing and service resolution
- Secure and reliable file system access
- Support for industry-standard protocols

The Client for Open Enterprise Server supports the traditional OES protocols (NDAP, NCP, and RSA) and interoperates with open protocols (LDAP, CIFS, and NFS).

Is the Client for Open Enterprise Server Right for Your Network?

Although OES offers services that don't require Client for Open Enterprise Server, (such as 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.

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, OES 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 135.

Beginning with OES 2015, the Novell Identity Translator (NIT) is supported. For more information, see NIT (Novell Identity Translator) in the NSS AD Administration Guide.

Active Directory User Access to OES Servers

Active Directory users can be granted access to CIFS shares on NSS volumes. The NSS AD integration service must be installed and the Novell Identity Translator must be configured to provide user IDs (UIDs) for AD users. For more information, see the *NSS AD Administration Guide*.

14.1.2 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 156
- "Planning Print Service Access" on page 157
- "Matching Protocols and Services to Check Access Requirements" on page 158

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 156
- "Feature Support" on page 157

Service Access to Volume Type Limitations

Supported combinations are outlined in Table 14-4.

Table 14-4 *Service Access to Volume Types*

File Service	Linux POSIX Volumes	NSS Volumes on Linux
CIFS	No	Yes-OES CIFS
NetWare Core Protocol (NCP)	Yes	Yes
NFS	Yes	Yes-NFSv3

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 158.

Feature Support

Table 14-5 *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

OES 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 23.4: OES iPrint Administration Guide*

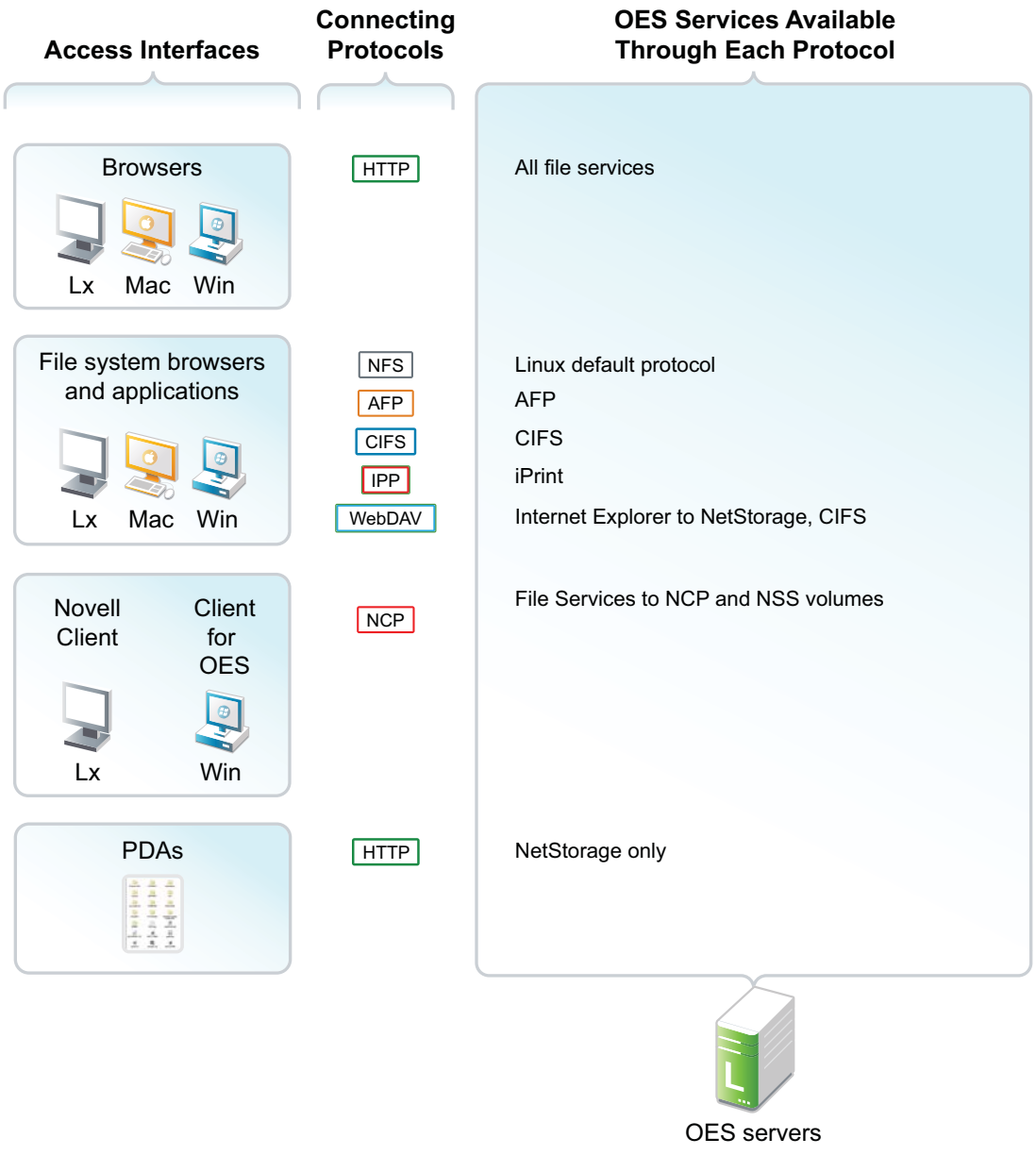
Matching Protocols and Services to Check Access Requirements

Figure 14-3 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 14-3 *Access Interfaces and Services, and the Protocols That Connect Them*



14.1.3 Coexistence and Migration of Access Services

Because NetWare Core Protocol (NCP) is available in OES, your Client for Open Enterprise Server 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 Client for Open Enterprise Server access. This means that Windows users with the Client for Open Enterprise Server installed can now be seamlessly transitioned to file services on OES.

For more information, see the *NCP Server for Linux Administration Guide*.

14.1.4 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 F, "Quick Reference to OES User Services," on page 229.

14.1.5 Configuring and Administering Access to Services

The following sections discuss administering access to services.

- "Password Management" on page 159
- "Linux (POSIX) File System Access Rights" on page 159
- "NSS File and Directory Trustee Management" on page 160

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 eDirectory 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 14-6 *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 `cd` 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 2023: File Systems Management Guide*.

NSS File and Directory Trustee Management

The *OES 2023: 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 iManager to Change File and Directory Attributes and Trustee Rights" on page 160
- "Using the Linux Command Prompt to Change File Attributes" on page 160
- "Using the Linux Command Prompt to Change Trustee Rights" on page 160
- "Using rights and NFARM to Manage AD Trustee Assignments on NSS Volumes" on page 161

Using iManager to Change File and Directory Attributes and Trustee Rights

You can use the iManager 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 2023: 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 2023: File Systems Management Guide*.

Using rights and NFARM to Manage AD Trustee Assignments on NSS Volumes

For information on `rights` utility and NFARM, see the *NSS AD Administration Guide*.

14.2 Authentication Services

This section briefly discusses the following topics:

- Section 14.2.1, "Overview of Authentication Services," on page 161
- Section 14.2.2, "Authentication Coexistence and Migration," on page 163

14.2.1 Overview of Authentication Services

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

- "NetIdentity Agent" on page 161
- "NetIQ Modular Authentication Services (NMAS)" on page 162
- "Password Support in OES" on page 162

NetIdentity Agent

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 Client for Open Enterprise Server 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 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

Client for Open Enterprise Server distributions include a number of NMAS login methods.

For more information on how to use NMAS, see Understanding eDirectory's Authentication Framework in the *NetIQ eDirectory Administration Guide*.

Password Support in OES

In the past, administrators have needed to manage multiple passwords (simple password and NDS 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 Managing Passwords in the *NetIQ eDirectory Administration Guide*.

All OpenText 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 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).

The password types supported in eDirectory are summarized in Table 14-7.

Table 14-7 *eDirectory Password Types*

Password Type	Description
NDS	The NDS password is stored in a hash form that is non-reversible 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.
CIFS	The CIFS users have Universal Password policies assigned by default. More information about password policy planning is available in Appendix L, "Coordinating Password Policies Among Multiple File Services," on page 263.
Simple	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. 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. 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.
Universal	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. 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. All the existing management tools that run on clients with the UP libraries automatically work with the Universal Password. Universal Password is not automatically enabled unless you install CIFS, or Domain Services for Windows on an OES server. The Client for Open Enterprise Server supports the Universal Password. It also supports the NDS password for older systems in the network. The Client for Open Enterprise Server automatically upgrades to use Universal Password when UP is deployed. For more information, see "Deploying Universal Password" in the *NetIQ eDirectory Administration Guide*.

14.2.2 Authentication Coexistence and Migration

For authentication and security coexistence and migration information, see "Chapter 19, "Security," on page 199 and Chapter 20, "Certificate Management," on page 209" in this guide.

15 Backup Services

The following sections briefly outline the backup services available in OES.

- Section 15.1, “Services for End Users,” on page 165
- Section 15.2, “System-Wide Services,” on page 165

15.1 Services for End Users

OES offers a number of services to automatically back up your network users’ data files.

- **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 so that 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. For more information, see “Understanding the NSS Salvage System” in the *Storage Services File System (NSS) Administration Guide for Linux*.

15.2 System-Wide Services

OES offers both Storage Management Services and services that are available as part of the SUSE Linux Enterprise Server distribution.

- Section 15.2.1, “List of Backup Software,” on page 165
- Section 15.2.2, “Storage Management Services (SMS),” on page 165
- Section 15.2.3, “SLES 15 Backup Services,” on page 166

15.2.1 List of Backup Software

Open Enterprise Server certifies the following backup software:

- SEP SESAM 5.0.0.11
- Catalogic DPX 4.8.1
- Micro Focus Data Protector A.11.01

NOTE: Micro Focus is now OpenText.

15.2.2 Storage Management Services (SMS)

- “Understanding SMS” on page 166
- “SMS Coexistence and Migration Issues” on page 166

Understanding SMS

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

The SMS API framework is available on SLES 15 so that there is a single consistent interface to back up file systems on NetWare, file systems on Linux, and applications such as Novell Groupwise, and eDirectory. 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 *Storage Management Services Administration Guide for Linux*.

15.2.3 SLES 15 Backup Services

Two SLES 15 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) in the SLES 15 High Availability Guide.
- **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 “Extended Attributes (XAttr) Commands” in the *Storage Services File System (NSS) Administration Guide for Linux*.

16 File Services

The file services in Open Enterprise Server let you provide Web-based and network-based file services to your network users.

This section contains the following information:

- Section 16.1, “Overview of File Services,” on page 167
- Section 16.2, “Planning for File Services,” on page 171
- Section 16.3, “Coexistence and Migration of File Services,” on page 173
- Section 16.4, “Aligning NCP and POSIX File Access Rights,” on page 174
- Section 16.5, “FTP (Pure-FTPd) and OES,” on page 177
- Section 16.6, “NCP Implementation and Maintenance,” on page 187
- Section 16.7, “OES CIFS Implementation and Maintenance,” on page 189

16.1 Overview of File Services

The file service components in OES include the following:

- FTP Services (page 167): Lets users securely transfer files to and from OES servers.
- NetWare Core Protocol (page 168): Provides NetWare Core Protocol (NCP) access to NCP volumes (including NSS volumes) that you define on OES server partitions.
- CIFS (page 169): Provides native Windows (CIFS and HTTP-WebDAV) access to files stored on an NSS volume on an OES server.

16.1.1 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 16.2, “Planning for File Services,” on page 171.

16.1.2 FTP Services

OES 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 **OES FTP Server** pattern in the OES 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. For migration instructions and a brief FAQ, see “Migrating FTP to OES 24.4” in the *Migration Tool Administration Guide*.

For documentation on Pure-FTP, visit the Pure-FTP Web site (http://pureftpd.sourceforge.net/documentation.shtml).

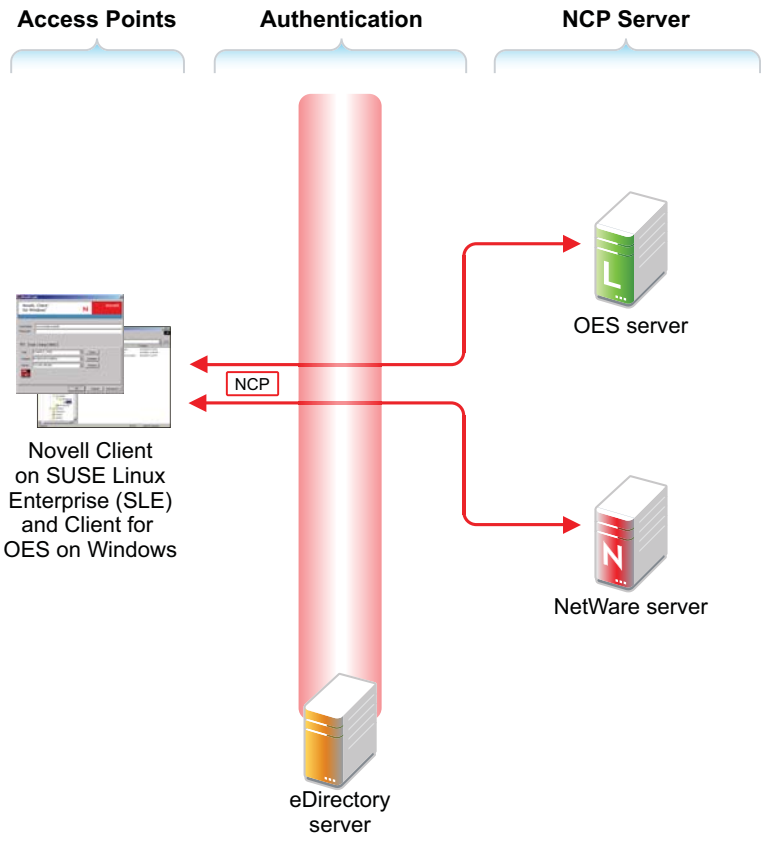
16.1.3 NetWare Core Protocol

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 OES NCP Server for Linux provides the rich file services that Novell is known for. Windows users who run Client for Open Enterprise Server software can access data, manage files and folders, map drives and so on, using the same methods as they do on NetWare servers.

Figure 16-1 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 149.

Figure 16-1 *NCP Services for Linux and NetWare*



The following table explains the information illustrated in Figure 16-1.

Table 16-1 *NCP Access*

Access Methods	Authentication	NCP Services
Access is through an NCP client—specifically, the Client for Open Enterprise Server.	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.

16.1.4 CIFS

The 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 Client for Open Enterprise Server.

Figure 16-2 *How Novell CIFS Works for eDirectory Users*

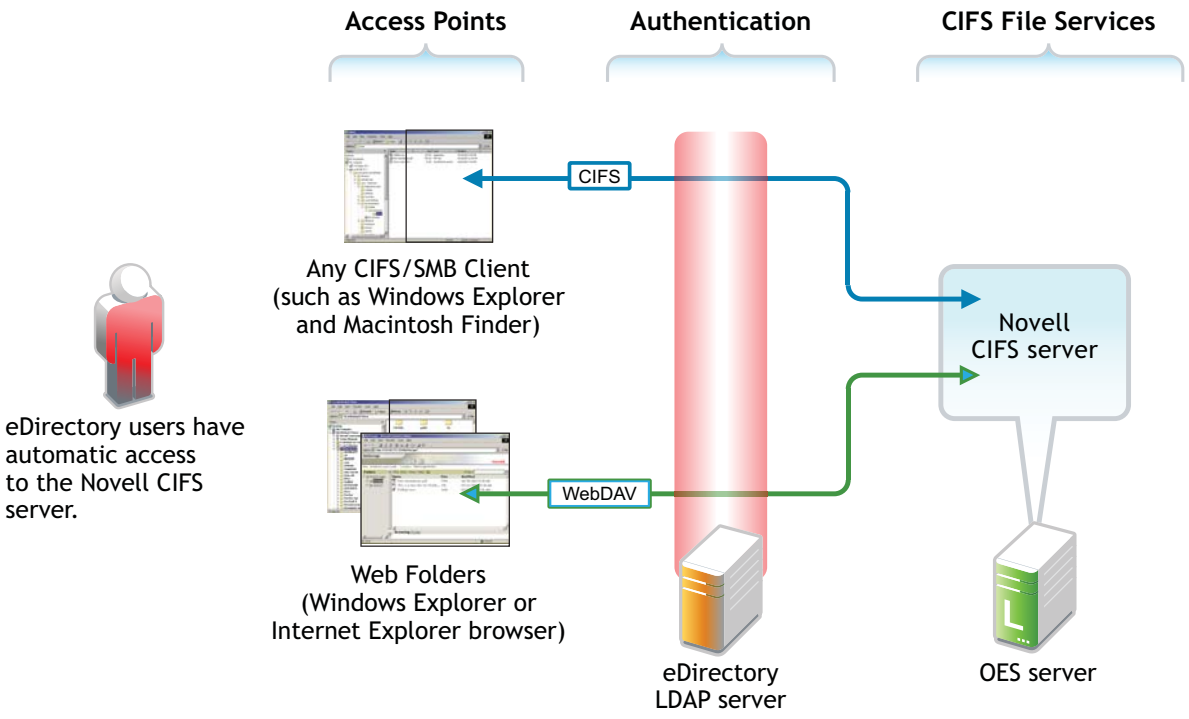


Table 16-2 *CIFS Access for eDirectory Users*

Access Methods	Authentication
eDirectory users on Windows workstations have two native Windows file access options: ◆ **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. Files on the OES server are accessed and maintained with the HTTP-WebDAV protocol.	All file service access is controlled by LDAP-based authentication through the eDirectory server.

Figure 16-3 *How CIFS Works for Active Directory Users*

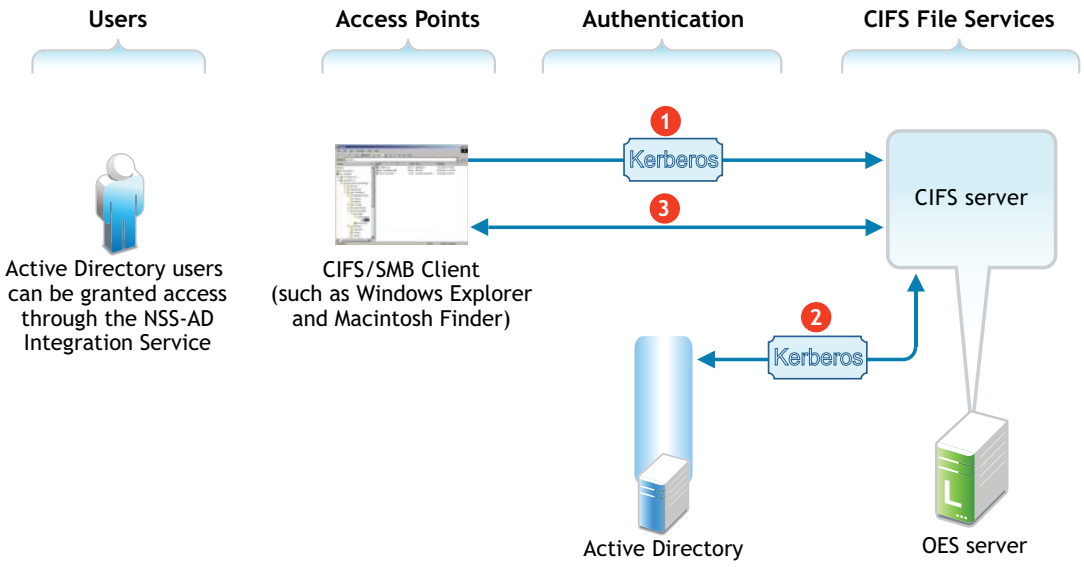


Table 16-3 *CIFS Access for Active Directory Users*

Access Methods	Authentication
Active Directory users gain access to CIFS file services as follows: 1. The user presents a Kerberos ticket obtained from Active Directory to the CIFS server. 2. The CIFS server validates the ticket with Active Directory. 3. After validation, files on the OES server are accessed and maintained through the CIFS protocol.	All CIFS file service access is controlled by Kerberos-based authentication and Active Directory.

16.2 Planning for File Services

Functional overviews of each file service product are included in Section 16.1, “Overview of File Services,” on page 167.

- Section 16.2.1, “Deciding Which Components Match Your Needs,” on page 171
- Section 16.2.2, “Comparing Your CIFS File Service Options,” on page 171
- Section 16.2.3, “Planning Your File Services,” on page 172

16.2.1 Deciding Which Components Match Your Needs

To decide which file service components to install, you should match service features listed in Table 16-4 to your network’s file service requirements.

Table 16-4 *OES File Services Feature Breakdown*

Service	Access Method Features	Back-End Storage Features	Security Features
NCP Server (NetWare Core Protocol)	Client for Open Enterprise Server (NCP client)	◆ Any Linux volumes (including NSS) that are defined as NCP volumes	◆ eDirectory Authentication
CIFS	◆ Any CIFS client ◆ Remote access (Web Folders in the Internet Explorer browser) ◆ Windows Explorer	◆ NSS volumes	◆ Secure LDAP Authentication

16.2.2 Comparing Your CIFS File Service Options

OES offers two file services that use the CIFS protocol: CIFS and Samba in Domain Services for Windows (DSfW).

Table 16-5 *Comparing OES CIFS Solutions*

Item	CIFS	Samba in DSfW
Authentication	A Universal Password Policy that allows the CIFS proxy user to retrieve passwords is required. The user who migrates ACLs for AD users to NSS must have the CIFS universal password policy applied. This includes the eDirectory Admin user if applicable. The authentication method for NSS AD access is Kerberos.	The Domain Services Password policy is required for DSfW users. The domain is set up as a trusted environment. DSfW uses Active Directory authentication methods, such as Kerberos, to ensure that only authorized users can log in to the domain.

Item	CIFS	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 *OES 2023: File Systems Management Guide*.
LUM and Samba enablement	LUM and Samba enablement are not required.	eDirectory users in the domain (eDirectory partition) are automatically Samba users and are enabled to access Samba shares. See "Creating Users" in the *Domain Services for Windows Administration Guide*. 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	Beginning with OES 2015, both eDirectory and Active Directory users can access CIFS.	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. 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 *OES 2023: File Systems Management Guide*.

16.2.3 Planning Your File Services

1. For the file services you plan to install, compute the total additional RAM required (above the basic system requirement).
   - **NCP:** There are no additional RAM requirements.
   - **Novell CIFS:** There are no additional RAM requirements.
2. Record the additional required RAM in your planning notes.

3 For the file services you plan to install, compute the total additional disk space required (above the basic system requirement).

- **NCP:** Allocate enough disk space to meet your users' file storage needs. On Linux, this space must exist on partitions you have designated as NCP volumes.
- **CIFS:** 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 installation guide that are indicated in the following table.

Note your planning choices on your planning sheet.

File Service Product	Linux Planning References
NCP	"NetWare Core Protocol (NCP) Server" in the *Installation Guide*
CIFS	"OES CIFS Services" in the *Installation Guide*
FTP	"OES FTP Services" in the *Installation Guide*

16.3 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 16.3.1, "Client for Open Enterprise Server (NCP)," on page 173
- Section 16.3.2, "CIFS," on page 173

16.3.1 Client for Open Enterprise Server (NCP)

Client for Open Enterprise Server is the long-standing software solution for providing NCP access to NetWare data from Windows workstations. The Client for Open Enterprise Server 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 Client for Open Enterprise Server, see the *Client for Open Enterprise Server Administration Guide*.

For more information on NCP Server for Linux, see the *NCP Server for Linux Administration Guide*.

16.3.2 CIFS

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 Client for Open Enterprise Server software is required.

For information on migrating CIFS services from NetWare to OES, see "Migrating CIFS to OES 24.4" in the *Migration Tool Administration Guide*.

16.4 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 19.2.1, "Comparing the Linux and the OES Trustee File Security Models," on page 201) 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 16.4.1, "Managing Access Rights," on page 174
- Section 16.4.2, "Providing a Private Work Directory," on page 175
- Section 16.4.3, "Providing a Group Work Area," on page 176
- Section 16.4.4, "Providing a Public Work Area," on page 176
- Section 16.4.5, "Setting Up Rights Inheritance," on page 177

16.4.1 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" (https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-security-acls.html) in the *SLES Security Guide* (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-security.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 rwx rights to the owner, r-x rights to the group, and no rights to other users.

For more information about the chmod command, see the chmod man page on your OES server.

16.4.2 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 a LUM-enabled user 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 LUM-enabled 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.

16.4.3 Providing a Group Work Area

On an NCP volume, you can provide a group work area by assigning users to a LUM-enabled 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 LUM-enabled 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 LUM-enabled 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 16.4.1, "Managing Access Rights," on page 174."

16.4.4 Providing a Public Work Area

On an NCP volume, you can provide a public work area by assigning [Public] as a trustee and then granting the required trustee rights to the directory.

For the work area itself, you would set permissions for the owner, group, and all others to read, write, and execute rights (rwx rwx rwx) (`chmod 777`).

All others must also have read and execute rights on the system in each parent directory in the path all the way to the root of the Linux system. This means that you set permissions for all parent directories to rwx --- r-x.

To provide a public work area on a Linux POSIX volume:

1. Use the `chown` command to assign all rights (rwx) to other (all users). For example, you could enter

   ```
   chmod -R 707 /path/group_dir
   ```

   where *path* is the file path to the work area, and *group_dir* is the group work directory. The third 7 grants rwx to the group. (The example assumes that the owner of the directory should also retain all rights and that the group setting is irrelevant.)

2. Check each parent directory in the path up to the `root (/)` directory, making sure that all users (other) have read and execute rights (r-x) in each directory as shown by the third group of permissions (. . . . . rwx). (Owner and group permissions are represented by dots because their settings are irrelevant.)

   Use the chmod command to adjust this where necessary by specifying the number 5 for the other permission. For more information, see "Managing Access Rights" at the beginning of this section.

16.4.5 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 *NCP Server for Linux Administration Guide*.

16.5 FTP (Pure-FTPd) and OES

FTP file services on OES 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 and offers a level of integration between eDirectory and Pure-FTP that allows users to authenticate to eDirectory for FTP access to the server.

A new module `oesftpipc.service` is introduced for OES FTP server (`pure-ftpd`) to fetch the user details of eDirectory (FQDN) and Active Directory (User ID, home directory, AD domain name) during authentication.

The `pure-ftpd.service` and `oesftpipc.service` must be running on OES server for FTP functionality to work.

The OES implementation also includes support for FTP gateway functionality between Active Directory (AD) and Pure-FTPd that allows users to authenticate to AD for FTP access to the server. For more information, see FTP (Pure-FTPd) and OES for AD Users in the NSS AD Administration Guide.

This section discusses the following topics:

- Section 16.5.1, "Planning for Pure-FTPd," on page 178
- Section 16.5.2, "Installing Pure-FTPd," on page 178
- Section 16.5.3, "Home Directory Support in Pure-FTPd," on page 178
- Section 16.5.4, "Configuring Pure-FTPd on an OES Server," on page 179
- Section 16.5.5, "Configuring Pure-FTPd for Secure Connections with TLS," on page 179

- Section 16.5.6, “Administering and Managing Pure-FTPd on an OES Server,” on page 181
- Section 16.5.7, “Cluster Enabling Pure-FTPd in an OES Environment,” on page 186
- Section 16.5.8, “SMB Access for eDirectory Users,” on page 187
- Section 16.5.9, “Migrating Pure-FTPd From NetWare to Linux,” on page 187

16.5.1 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.

16.5.2 Installing Pure-FTPd

To install Pure-FTPd, select the **OES FTP** pattern in the OES installation.

16.5.3 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.

16.5.4 Configuring Pure-FTPd on an OES Server

To configure the Pure-FTPd server on OES, 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 more information, see the `pure-ftpd` man page.

Refer to the `/usr/share/doc/packages/pure-ftpd/README.TLS` file for SSL/TLS configuration.

16.5.5 Configuring Pure-FTPd for Secure Connections with TLS

FTP configured servers that support TLS use certificates such as CA signed certificate, self signed certificate, or eDirectory certificate to check the security and identity of servers.

Prerequisites for Configuring FTP Server

- A valid third-party CA-signed certificate or an eDirectory server certificate must be available on the server along with the private key.
- The private key and the certificate must be a single file with name `pure-ftpd.pem`.

Combining the Certificate and Private Key into a Single File

To combine the files, execute the following command:

```
cat certificate.pem private_key.pem > /etc/ssl/private/pure-ftpd.pem
```

The file path is `/etc/ssl/private/` by default and can be changed.

Example: For combining eDirectory certificate and private key

```
cat /etc/ssl/servercerts/servercert.pem /etc/ssl/servercerts/serverkey.pem
> /etc/ssl/private/pure-ftpd.pem
```

Modifying TLS for FTP Server

1. Open the `/etc/pure-ftpd/pure-ftpd.conf` configuration file in a text editor.
2. Update the TLS value as per your security requirement.

TLS Value	Functions
0	Disables the TLS support. By default, TLS is disabled.
1	Server accepts both secure and non-secure connections with TLS layer.
2	Server accepts only secure connections.

3. Uncomment and provide required inputs for `TLS`, `TLSCipherSuite`, and `CertFile`.

   The `CertFile` is the location of the `pure-ftpd.pem` file.

```
# This option can accept three values :
# 0 : disable SSL/TLS encryption layer (default).
# 1 : accept both traditional and encrypted sessions.
# 2 : refuse connections that don't use SSL/TLS security mechanisms,
#     including anonymous sessions.
# Do _not_ uncomment this blindly. Be sure that :
# 1) Your server has been compiled with SSL/TLS support (--with-tls),
# 2) A valid certificate is in place,
# 3) Only compatible clients will log in.

 TLS     1


# OpenSSL ciphers suite for TLS sessions.
# Prefix with -C: in order to require valid client certificates.
# If -C: is used, make sure that clients' public keys are installed
# on the server.
# SSL,TLS 1.0 and 1.1 are disabled. TLS 1.2 and 1.3 are available.

 TLSCipherSuite     HIGH



# Certificate file, for TLS

 CertFile     /etc/ssl/private/pure-ftpd.pem
```

4. Save the configuration file.
5. Restart the Pure-FTPd daemon with the following command:

   ```
   systemctl restart pure-ftpd.service
   ```

NOTE: Pure-FTPd daemon fails to start if the `pure-ftpd.pem` certificate is corrupted.

Verifying the Certificate Used

To check which certificate is used, execute the following command:

```
openssl s_client -connect hostname/server_ip:21 -starttls ftp
```

This command displays the details of the certificate used by FTP.

16.5.6 Administering and Managing Pure-FTPd on an OES Server

- “Starting Pure-FTPd” on page 182
- “Verifying Pure-FTPd” on page 182
- “Initializing Multiple Instances” on page 182
- “Unloading Specific Instances” on page 183
- “Pure-FTPd Remote Server Navigation” on page 183

Starting Pure-FTPd

Start the Pure-FTPd server using the `systemctl restart pure-ftpd.service` command.

Verifying Pure-FTPd

To verify the status of Pure-FTPd, run the following commands:

```
systemctl status oesftpipc.service
```

```
systemctl status pure-ftpd.service
```

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-ftpd/pure-ftpd.conf` file is loaded at the boot time. 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-ftpd/pure-ftpd.conf` to a different location. Rename the file to `pure-ftpd1.conf` and move it to `/etc/opt/novell/pure-ftpd1.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-ftpd instance. PID file is used for unloading a particular instance of pure-ftpd. 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-ftpd 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-ftpd instances bind to different IP addresses or port combinations.

     also, modify the settings in the `/etc/pure-ftpd/pure-ftpd.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-ftpd 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-ftpd1.conf` loads an instance using the config file `/etc/opt/novell/pureftpd-confs/pure-ftpd1.conf`.

Verifying the Load of a New Instance

Use the following methods to verify that the new instance of pure-ftpd is successfully loaded:

- The `ps –eaf | grep pure-ftpd` command lists all the instances of pure-ftpd 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-ftpd 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

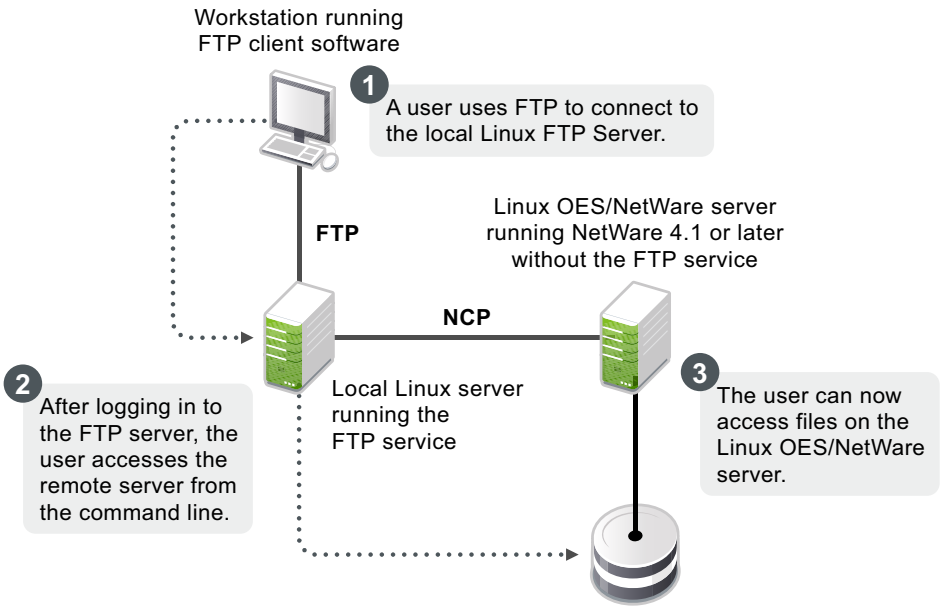
- The PID file specified using the `PIDFile` entry in the configuration file has been deleted.
- The number of instances displayed by `ps –eaf | grep pure-ftpd` is reduced.
- An FTP connection request to the server errors out.

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 FTP” on page 184
- “Path Formats” on page 185
- “SITE Command” on page 185
- “Disable-ascii” on page 186



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 FTP

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

The configuration parameters for remote server navigation are as follows:

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

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

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

Path Formats

Table 16-6 *Linux FTP Server path formats*

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

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 16-7 provides the SITE command along with the description:

Table 16-7 *Linux FTP SITE command*

Command	Description
SLIST	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.

16.5.7 Cluster Enabling Pure-FTPd in an OES Environment

You can configure Pure-FTPd server in active/active mode of Cluster Services.

- "Prerequisites" on page 186
- "Active/Active Mode" on page 186

Prerequisites

- Cluster Services is installed and setup.

  For step-by-step information on setting up Cluster Services, refer to "Installing, Configuring, and Repairing OES Cluster Services" in the "*OES 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 **OES FTP** in the OES install.
2. Enable hard links on the shared NSS volumes. For more information on hard links, see "Hard Links Commands" in the*Storage Services File System (NSS) Administration Guide for Linux*.
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.

16.5.8 SMB Access for eDirectory Users

By default, eDirectory users access files through NCP protocol. Beginning with OES 2018 SP3, they can also access files through SMB protocol. To do this, enable the entry `use_smb_for_edir_users` to "yes" in the `/etc/pure-ftpd/pure-ftpd.conf` on the FTP server.

```
# Use SMB for remote access by eDirectory users
use_smb_for_edir_users yes
```

Universal Password must be enabled for eDirectory users to access files through SMB protocol.

16.5.9 Migrating Pure-FTPd From NetWare to Linux

You can also migrate an existing FTP server configuration from a NetWare server to OES. For migration instructions and a brief FAQ, see "Migrating FTP to OES 24.4" in the *Migration Tool Administration Guide*.

16.6 NCP Implementation and Maintenance

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

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

- Section 16.6.1, "The Default NCP Volume," on page 188
- Section 16.6.2, "Creating NCP Home and Data Volume Pointers," on page 188
- Section 16.6.3, "Assigning File Trustee Rights," on page 188
- Section 16.6.4, "NCP Caveats," on page 188
- Section 16.6.5, "NCP Maintenance," on page 189

16.6.1 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.

16.6.2 Creating NCP Home and Data Volume Pointers

Initially, there are no NCP home directories or data volumes available to Client for Open Enterprise Server 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 Client for Open Enterprise Server 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.

16.6.3 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 Client for Open Enterprise Server 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 *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.)

16.6.4 NCP Caveats

Cross-protocol file locking (CPL) is enabled by default on all new servers with NCP installed.

16.6.5 NCP Maintenance

Because NCP provides Client for Open Enterprise Server access to files on NetWare and OES servers, the service is covered by maintenance tasks that apply to file systems on these servers. For more information, see "OES online documentation (https://www.novell.com/documentation/oes2018/)".

16.7 OES CIFS Implementation and Maintenance

To use the CIFS file services on your OES server, you must install the service by using the instructions in the *Installation Guide* (for a new installation) or install it after the initial OES installation, as explained in "Installing CIFS after the OES Installation" in the *OES CIFS for Linux Administration Guide*.

- Section 16.7.1, "Implementing OES CIFS File Services," on page 189
- Section 16.7.2, "Maintaining OES CIFS File Services," on page 189

16.7.1 Implementing OES CIFS File Services

All eDirectory users can access the CIFS file services on an OES server as they would any Windows workgroup server.

Active Directory users can also be granted access through the NSS AD integration service starting in OES 2015.

For instructions on implementing OES CIFS, see "Planning and Implementing CIFS" in the *OES CIFS for Linux Administration Guide*.

16.7.2 Maintaining OES CIFS File Services

Information on maintaining your CIFS installation is found in the *OES CIFS for Linux Administration Guide*.

17 Print Services

Open Enterprise Server includes iPrint, a powerful and easy-to-implement printing solution that provides print-anywhere functionality to network users.

NOTE: OES iPrint and OES iPrint Advanced patterns are merged. Thus, OES iPrint Advanced is available along with OES iPrint capabilities.

This section contains the following information:

- Section 17.1, “Overview of Print Services,” on page 191
- Section 17.2, “Planning for Print Services,” on page 194
- Section 17.3, “Coexistence and Migration of Print Services,” on page 194
- Section 17.4, “Print Services Implementation Suggestions,” on page 194
- Section 17.5, “Print Services Maintenance Suggestions,” on page 196

17.1 Overview of Print Services

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 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 17.1.1, “Using This Overview,” on page 191
- Section 17.1.2, “iPrint Components,” on page 192
- Section 17.1.3, “iPrint Functionality,” on page 192

17.1.1 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 17.2, “Planning for Print Services,” on page 194.

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

17.1.2 iPrint Components

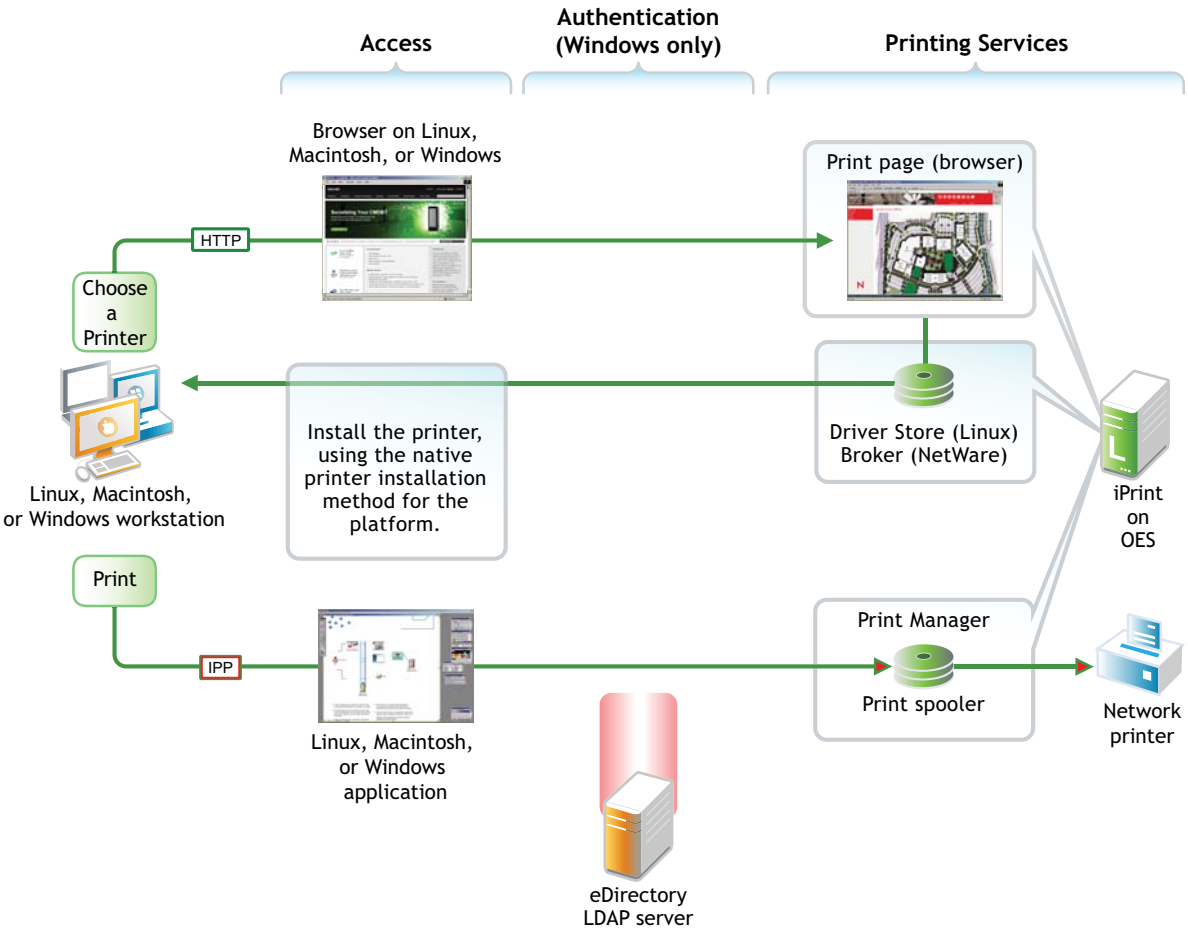
The iPrint installation consists of various components, most of which are represented by objects in your eDirectory tree:

- **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.

17.1.3 iPrint Functionality

Figure 17-1 describes how iPrint functions from a user workstation perspective.

Figure 17-1 *How iPrint Works*



The following table explains the information illustrated in Figure 17-1.

Table 17-1 *iPrint Functionality*

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

17.2 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 "OES iPrint Advanced" in the *Installation Guide*.

17.3 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 15 packages, CUPS is disabled to avoid port 631 conflicts.

For information on upgrading from NetWare queue-based printing, 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 OES iPrint Advanced Server in the OES iPrint Advanced Administration Guide

Migrating iPrint services from a NetWare server to an OES 24.4 server is supported by the OES Migration Tool. For more information, see "Migrating iPrint to OES 24.4" in the *Migration Tool Administration Guide*.

17.4 Print Services Implementation Suggestions

This section provides only summary implementation information. For complete iPrint documentation, see the *OES iPrint Advanced Administration Guide*.

- Section 17.4.1, "Initial Setup," on page 194
- Section 17.4.2, "Other Implementation Tasks," on page 195

17.4.1 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 iPrint Advanced Administration Guide*.

2 Add a printer driver to the Driver Store for each printer/platform combination needed.

For example, If you have Windows XP 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 iPrint Advanced 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 iPrint Advanced 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 iPrint Advanced 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 iPrint Advanced 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; iPrint does the rest.

17.4.2 Other Implementation Tasks

In addition to the tasks described in Section 17.4.1, "Initial Setup," on page 194, there are additional tasks you might want or need to consider. For more information, see "iPrint documentation (https://www.microfocus.com/documentation/open-enterprise-server/24.4/)" in the OES online documentation.

17.5 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 iPrint Advanced Administration Guide*.

For more information on iPrint and its functionality within OES, see the "iPrint documentation (https://www.microfocus.com/documentation/open-enterprise-server/24.4/)" in the OES online documentation.

18 Web Services

The Web and application services in Open Enterprise Server 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 2015 SP1: Web Services and Applications Guide*.

Apache

OES includes Apache 2.4, the most popular Web server on the Internet.

For additional information, see the Apache.org Web site (http://httpd.apache.org/docs/2.4/).

Tomcat

OES includes Tomcat 8.0, which is used to run basic Java servlet and JavaServer Pages (JSP) applications.

For information, see the Apache Tomcat 8.0 Web site (http://tomcat.apache.org/tomcat-8.0-doc/index.html).

19 Security

This section contains the following topics:

- Section 19.1, “Overview of OES Security Services,” on page 199
- Section 19.2, “Planning for Security,” on page 201
- Section 19.3, “OES and Security Scanners,” on page 206
- Section 19.4, “Links to Product Security Considerations,” on page 206
- Section 19.5, “List of Antivirus Software,” on page 207
- Section 19.6, “TLS Version Support,” on page 207

19.1 Overview of OES Security Services

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

- Section 19.1.1, “Application Security (AppArmor),” on page 199
- Section 19.1.2, “NSS Auditing Engine,” on page 199
- Section 19.1.3, “Encryption (NICI),” on page 200
- Section 19.1.4, “General Security Issues,” on page 201

19.1.1 Application Security (AppArmor)

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 AppArmor Documentation Web site (http://www.novell.com/documentation/apparmor/index.html).

19.1.2 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 OpenText Web site (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 Server 90-Day Free Trial

Novell Sentinel Log Manager runs on a 64-bit SLES host. You can download the suite from the Software Licenses and Downloads (SLD) (https://sld.microfocus.com/mysoftware/index). For installation and usage instructions, see the Novell Sentinel Readme and Release Notes included as a link on the download page.

Third-Party Partner Applications

For information about third-party partner applications that leverage the NSS Auditing Engine, see the OES partners' page.

19.1.3 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 NICI Configuration Files

In the early days of NICI development, some NICI problems could be solved only by deleting the NICI configuration files and starting over. The issues that required this were solved years ago, but as is often the case, the practice persists, and some administrators attempt to use this as a remedy when they encounter a NICI problem.

No one should ever delete the NICI configuration files unless they are directly told to do so by a member of the NICI development team. And in that rare case, they should be sure to back up the files before doing so. Failure to do this makes restoring NICI impossible.

More Information

For more information on how to use NICI, see the *Novell International Cryptographic Infrastructure (NICI) 2.7.6 Administration Guide*.

19.1.4 General Security Issues

In addition to the information explained and referenced in this section, the OES online documentation contains links to "security issues" (https://www.novell.com/documentation/open-enterprise-server-2018/).

19.2 Planning for Security

This section discusses the following topics. For additional planning topics, see the OES online documentation (https://www.novell.com/documentation/open-enterprise-server-2018/).

- Section 19.2.1, "Comparing the Linux and the OES Trustee File Security Models," on page 201
- Section 19.2.2, "User Restrictions: Some OES Limitations," on page 203
- Section 19.2.3, "Ports Used by OES," on page 204
- Section 19.2.4, "Configuring and Administering Security," on page 206

19.2.1 Comparing the Linux and the OES Trustee File Security Models

The OES Trustee and Linux (POSIX) security models are quite different, as presented in Table 19-1.

Table 19-1 *POSIX vs. NSS/NCP File Security Models*

Feature	POSIX / Linux	Trustee Model on OES
Administrative principles	Permissions are individually controlled and managed for each file and subdirectory. Because of the nature of the POSIX security model, users usually have read rights to most of the system. To make directories and files private, permissions must be removed. For more information on making existing directories private, see Section 16.4.2, "Providing a Private Work Directory," on page 175.	Trustee assignments are made to directories and files and flow down from directories to everything below unless specifically reassigned.
Default accessibility	Users have permissions to see most of the file system. The contents of a few directories, such as the `/root` home directory, can only be viewed by the `root` user. Some system configuration files can be read by everyone, but the most critical files, such as `/etc/fstab`, can only be read and modified by `root`.	Users can see only the directories and files for which they are trustees (or members of a group that is a trustee).
Home directories—an example of default accessibility	By default, all users can see the names of directories and files in home directories. During LUM installation, you can specify that newly created home directories will be private. For more information on making existing home directories private, see Section 16.4.2, "Providing a Private Work Directory," on page 175.	By default, only the system administrator and the home directory owner can see a home directory. Files in the directory are secure. 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.
Inheritance from parents	Nothing is inherited. Granting permission to a directory or file affects only the directory or file.	Rights are inherited in all child subdirectories and files unless specifically reassigned. A trustee assignment can potentially give a user rights to a large number of subdirectories and files.
Privacy	Because users have permissions to see most of the file system for reasons stated above, most directories and files are only private when you make them private.	Directories and files are private by default.

Feature	POSIX / Linux	Trustee Model on OES
Subdirectory and file visibility	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. After permissions are granted, users can see the entire contents (subdirectories and files) of each directory in the path.	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 *NCP Server for Linux Administration Guide*, particularly the "NCP on Linux Security" section.

19.2.2 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 9.5, "SSH Services on OES," on page 73.

For more information on Linux User Management, see "Linux User Management: Access to Linux for eDirectory Users" on page 135. For more information on the services that can be PAM-enabled, see Table 13-2 on page 139.

19.2.3 Ports Used by OES

The ports used by OES services are listed in Table 19-3.

Table 19-2 *Open Enterprise Server Services and Ports*

Service	Default Ports
Domain Services for Windows	◆ 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	◆ 389 (LDAP) ◆ 636 (secure LDAP) **IMPORTANT:** The scripts that manage the common proxy user require port 636 for secure LDAP communications. ◆ 8028 (HTTP for iMonitor) ◆ 8030 (secure HTTP for iMonitor) ◆ 524 (NCP)
iManager	◆ 80 (HTTP) ◆ 443 (secure HTTP)
iPrint	◆ 80 (HTTP) ◆ 443 (secure HTTP) ◆ 631 (IPP)
Novell Identity Translator	◆ 3268 ◆ 389
OES CIFS	◆ 139 (Netbios) ◆ 445 (Microsoft-ds)

Service	Default Ports
Cloud Integrated Storage (CIS)	**Infrastructure services:** ◆ 2181 (ZooKeeper) ◆ 2282 (secure ZooKeeper) ◆ 9092 (Kafka) ◆ 9094 (secure Kafka) ◆ 9400 (Elasticsearch) ◆ 2377, 7946 (Docker Swarm) ◆ 2888, 3888 (Communication between ZooKeeper servers and leader election) **CIS core services:** ◆ 3306 (MariaDB) ◆ 8000 (Agent) ◆ 8105 (CIS configuration) ◆ 8343 (secure Gateway) ◆ 8344 (CIS management)) ◆ 8346 (secure Datascale Gateway) ◆ 8347 (secure Datascale Data service) ◆ 24224 (Fluentbit)
OES Cluster Service	◆ 7023
OES DHCP	◆ 67
OES DNS	◆ 953 (secure HTTP) ◆ 53 (TCP) ◆ 53 (UDP)
OES FTP	◆ 21
OES Information Portal	◆ 80 (HTTP) ◆ 443 (secure HTTP)
OES NetWare Core Protocol (NCP)	◆ 524
OES Remote Manager	◆ 8008 (HTTP) ◆ 8009 (secure HTTP)
NURM (Deprecated)	◆ 80 ◆ 443
SFCB	◆ 5988 (HTTP) ◆ 5989 (secure HTTP)
Secure Shell	◆ 22
Storage Management Services (Backup)	◆ 40193 (smdr daemon)

Service	Default Ports
Unified Management Console (UMC)	• 5432 (database)
Time Synchronization	• 323 (Network Time Protocol UDP)

19.2.4 Configuring and Administering Security

For a list of configuration and administration topics, see the OES online documentation (https://www.novell.com/documentation/open-enterprise-server-2018/).

19.3 OES and Security Scanners

OpenText software development processes include the performance of regular and rigorous security scans. All issues that are discovered as part of these scans are resolved prior to product releases.

As you perform security scans inside your organization, if you discover security issues that involve OES or other OpenText products, and if you are unable to resolve them, please contact OpenText Support for help.

19.4 Links to Product Security Considerations

The following product documentation contains additional security information:

Table 19-3 *Security Consideration Links*

Product/Technology	Security Considerations Section Link
OES Installation	Security Considerations in the *Installation Guide*
Multifactor Authentication	Multifactor Authentication Service in the *Installation Guide*
OES CIFS	Security Guidelines for CIFS in the *OES CIFS for Linux Administration Guide*.
OES Cluster Services	Security Considerations in the OES Cluster Services for Linux Administration Guide
Cloud Integrated Storage	Best Practices and Common Questions in the Cloud Integrated Storage Administration Guide
Domain Services for Windows	*OES 23.4: OES Domain Services for Windows Security Guide*
Distributed Files Services (DFS)	Security Considerations in the Distributed File Services Administration Guide for Linux
Dynamic Storage Technology	Security Considerations in the *Dynamic Storage Technology Administration Guide*
eDirectory	Security Considerations in the NetIQ eDirectory Administration Guide

Product/Technology	Security Considerations Section Link
File Systems	*OES 2023: File Systems Management Guide* (information throughout the guide)
Identity Manager 4.7	Security Best Practices in the NetIQ Identity Manager Security Guide.
iPrint for OES	Setting Up a Secure Printing Environment in the *OES 23.4: OES iPrint Administration Guide*
Linux User Management	Security Considerations in the *Linux User Management Administration Guide*
Client for Open Enterprise Server	Security Considerations in the Client for Open Enterprise Server Administration Guide
NCP Server for Linux	Security Considerations for NCP Server in the NCP Server for Linux Administration Guide
OES Remote Manager	Security Considerations in the *OES 23.4: OES Remote Manager Administration Guide*
Storage Services	Securing Access to NSS Volumes, Directories, and Files and Security Considerations in the *Storage Services File System (NSS) Administration Guide for Linux*
OES Migration Tools	Security Considerations for Data Migration in the *Migration Tool Administration Guide*
firewalld	Masquerading and Firewalls in the *SLES Security* Guide

19.5 List of Antivirus Software

Open Enterprise Server certifies the following antivirus software:

- Trellix Command Line Scanner for Linux Version 7.0.4
- Trellix Endpoint Security for Linux 10.7.17-1369
- Sophos Server Protection for Linux 2023.3

  For more information about configuring Sophos with the OES server, see Sophos Server Protection 2023.3 configuration with OES 23.4.

19.6 TLS Version Support

The TLS versions supported by OES Services are listed in the following table.

In the table, for the services where the TLS default versions are not explicitly mentioned, consider all the supported versions as the default versions.

Table 19-4 *TLS Support Matrix*

Service	OES 2023	OES 24.4
Pure-FTPd	TLSv1.2	TLSv1.3 and TLSv1.2
NCP File Server	TLSv1.2	TLSv1.3 and TLSv1.2
OES Remote Manager (NRM)	TLSv1.2, TLSv1.1 and TLSv1.0	TLSv1.3 and TLSv1.2
iPrint	TLSv1.2, TLSv1.1 and TLSv1.0	TLSv1.3, TLSv1.2 andTLSv1.1
	Default: TLSv1.2 and TLSv1.1	**Default:** TLSv1.3 and TLSv1.2
iPrint Clients	TLSv1.2 and TLSv1.1	TLSv1.2 and TLSv1.1
iManager	TLSv1.2, TLSv1.1 and TLSv1.0	TLSv1.3, TLSv1.2 andTLSv1.1
	Default: TLSv1.2 and TLSv1.1	**Default:** TLSv1.3 and TLSv1.2
NURM (Deprecated)	TLSv1.2, TLSv1.1 and TLSv1.0	TLSv1.3, TLSv1.2 and TLSv1.1
	Default: TLSv1.2 and TLSv1.1	**Default:** TLSv1.3 and TLSv1.2
NetStorage	TLSv1.2, TLSv1.1 and TLSv1.0	NA
	Default: TLSv1.2 and TLSv1.1	
eDirectory - LDAP Service	TLSv1.2, TLSv1.1 and TLSv1.0	TLSv1.2 and TLSv1.1
	Default: TLSv1.2	**Default:** TLSv1.2
eDirectory - iMonitor	TLSv1.2, TLSv1.1 and TLSv1.0	TLSv1.2 and TLSv1.1
Cloud Integrated Storage (CIS)	TLSv1.2	TLSv1.3 and TLSv1.2
Storage Management Services (SMS)	TLSv1.2, TLSv1.1 and TLSv1.0	TLSv1.3 andTLSv1.2
Domain Services for Windows	TLSv1.2, TLSv1.1 and TLSv1.0	TLSv1.2, TLSv1.1 and TLSv1.0
	Default: TLSv1.2	**Default:** TLSv1.2
SFCB	TLSv1.2, TLSv1.1 and TLSv1.0	TLSv1.3, TLSv1.2, TLSv1.1, and TLSv1.0
	Default: TLSv1.2 and TLSv1.1	**Default:** TLSv1.3, TLSv1.2 and TLSv1.1
Unified Management Console (UMC)	NA	TLSv1.3 and TLSv1.2
		Default: TLSv1.3 and TLSv1.2

20 Certificate Management

NetIQ Certificate Server is automatically installed when you install eDirectory. Certificate Server provides public key cryptography services that are natively integrated into eDirectory and that allow you to mint, issue, and manage both user and server certificates. These services allow you to protect confidential data transmissions over public communications channels such as the Internet.

For more information on Certificate Server, see Understanding the Certificate Server in the NetIQ eDirectory Administration Guide.

A Product Improvement

Product Improvement enables OpenText to collect statistical data about your usage of services on the OES server. This data enables us to ensure that you have the best possible experience with OES services. Weekly once the data is sent to the OpenText server.

Terms Used:

- **Product Improvement (Telemetry):** The service used to collect statistical data for usage of OES services.
- **Telemetry Server or server:** The server that participated (configured) in the Product Improvement program by selecting the checkbox through YaST.
- **Telemetry Agents or agents:** The OES servers that are enabled for telemetry because they are in the same context as the server configured for telemetry.

A.1 Overview

The Product Improvement (telemetry) package is part of the base OES 24.4 package.

Before configuring the OES server with telemetry ensure the following:

- The OES LDAP user has write permission on the container where the telemetry server resides.
- Ensure sufficient space is available to store the data. The data is stored at `/var/opt/novell/telemetry/data/`.
- The coreagent agent service must be running for communication between the server and agents.
- Port 8000 must be opened on agents to communicate with the server.

When an OES server is configured for telemetry:

- All the servers in the same context as this server are automatically enabled for telemetry.
- The telemetry agent service runs on all the servers that are configured and enabled for telemetry.
- The eDirectory schema is extended with `oes-telemetry-info` attribute.
- The `oes-telemetry-info` attribute includes the server IP address of the server that was configured with telemetry.

The telemetry agent walks up the tree in search of `oes-telemetry-info` attribute. If this attribute is found then the agent continues to run else after trying three times it stops. The agent is restarted once every week to discover a telemetry server. It continues running if it finds a server, or it stops again.

A.2 Data That is Collected for Product Improvement

Cloud Integrated Storage (CIS)

Table A-1 *CIS Telemetry Attributes*

Attributes	Description
configurationType	CIS is configured in Standalone, Infrastructure, Core or Scale mode
infraCount	Number of infrastructure servers deployed
gatewayCount	Number of CIS gateway servers deployed
datascaleCount	Number of data scale servers deployed
numPolicies	Number of migration and recall policies defined
numRuns	Number of migrations and recalls done

Distributed Files Services (DFS)

Table A-2 *DFS Telemetry Attributes*

Attributes	Description
Total Requests Processed	Total number of requests processed by VLDB.
Number of VLDBs	Number of VLDB servers in the Management Context.

iPrint Advanced

Table A-3 *iPrint Advanced Telemetry Attributes*

Attributes	Description
OESService	OES Pattern (OES iPrint / OES iPrint Advanced).
timestamp	Timestamp of Telemetry Data Collection
totalPrinters	Total Number of Printers
mobileEnabledPrinters	Total Number of Mobile Enabled Printers
securePrinters	Total Number of Secure Printers
totalWalkupPrinters	Total Number of Walkup Printers
mobileEnabledWalkupPrinters	Total Number of Mobile Enabled Walkup Printers
ippPrinters	Total Number of IPP Printers
remoteRenderers	Total Number of Remote Renderers
secureRemoteRenderers	Total Number of Secure Remote Renderers

Attributes	Description
nonSecureRemoteRenderers	Total Number of Non-Secure Remote Renderers
globalEmailConfigured	Global Email Configuration (Enabled / Disabled)
privateEmailConfigured	Total Number of Private Email Printers Configured
directPrinterEnabled	Total Number of Printers Enabled for Direct Printing
auditEnabledPrinters	Total Number of Printers Enabled for Auditing
accountingEnabledPrinters	Total Number of Printers Enabled for Accounting
lprEnabledPrinters	Total Number of Printers Enabled for LPR Printing
azureConfigured	Microsoft Identity Source Configured (Yes / No)
eDirUsers	Total Number of eDirectory Users
cluster	Is it a Cluster (Yes / No)

NCP and DST

Table A-4 *NCP and DST Telemetry Attributes*

Attributes	Description
CPUAffinity	NCP CPU Affinity is enabled
Encryption	NCP Encryption is Disabled/Enabled/Enforced at OES server level
EnforcedMFA	MFA enforcement for NCP connections at OES server level is set
DSTVolumes	Number of DST volumes configured on OES server
CISVolumes	Number of DST volumes configured on CIS cloud
ClusterVolumes	Number of NSS volumes configured on OES cluster services

Cluster Services (NCS)

Table A-5 *NCS Telemetry Attributes*

Attributes	Description
load_unload_histogram	The time taken for the load and unload of resources which were performed previously. This info is captured by taking the count of how many times the unload/load is performed <=15secs, <=30secs.....
node_count	No.of nodes in the cluster.
resource_count	No.of resources in the cluster.
protocol_settings	GIPC Protocol settings which include heartbeat, tolerance, slave watchdog, master watchdog and maximum retransmissions for a message.
email_notification_enabled	NCS Email notification mechanism enablement
sbd_partition	SBD partition configuration details which include the size and mirrored status
version_info	Identifying the homogeneity of the cluster and the version of each node.
nds_monitor_enabled	NDS Monitoring enablement
resource_monitor_info	No.of resources on which resource monitoring is enabled which are running on this node.

NSS Auditing

Table A-6 *NSS Auditing Telemetry Attributes*

Attributes	Description
Registered Clients	Number of active OES Storage Services Auditing Clients
Requested Format	List of requested output formats.

Pure-FTD

Table A-7 *Pure-FTD Telemetry Attributes*

Attributes	Description
ChrootEveryone	chroot is enabled for all users on ftp server
TLS	TLS setting set to allow SSL/TLS connections
remote_server	Remote server navigation for ftp server
DefaultHomeDirectory	Path of default shared home directory
DefaultHomeDirectoryServer	Server hosting default shared home directory
EnableRemoteHomeDirectory	User's home directory as the default mount point
use_smb_for_edir_users	SMB for remote access by eDirectory users

Storage Management Services (SMS)

Table A-8 *SMS Telemetry Attributes*

Attributes	Description
TSAs	List of loaded Target Service Agents(TSA)
TLS version	The TLS version used for encrypting the data when performing a remote backup.

Storage Services (NSS)

Table A-9 *NSS Telemetry Attributes*

Attributes	Description
Devices	
Number of devices	Number of devices
Device format	The partitioning format of the device (GPT or DOS)
Free:	Amount of unpartitioned space on the device
RAID	RAID configuration of the device
Shared	If device is shared for cluster (YES/NO)
Size	Size of device
Used	Amount of partitioned space on the device

Attributes	Description
Pools	
Number of pools	Number of pools
ADMediaSupport	Status of AD media support
AutoDiscard	Status of Auto discard
Free	Free space on pool
IsSnap	Status of Pool Snapshot
Media Name	Name of the Pool Media
Media Version	Version of pool media
Move	Displays whether pool move is enabled for the given pool (YES/NO)
Segs	Number of segments the pool consists of
Shared	Status of Pool share
Size	Size of Pool
State	State of Pool
Type	Type of Pool type (NSS64, NSS32)
Used	Used space on pool
Vols	Number of volumes on pool
RAID	
Number of Raid devices	Number of RAID devices
Raid controller	
Enabled	Status of RAID controller
Format	Displays whether pool move is enabled for the given pool (YES/NO)
Free	Amount of free space
Raid	Raid configuration (0,1,5)
Shared	If device is shared for clustering (Yes/no)
Size	Size allotted for RAID
Used	Amount of space used

Novell Identity Translator (NIT)

Table A-10 *NIT Telemetry Attributes*

Attributes	Description
AD_mode	Displays if AD mode is enabled
DomainLocalGroupsEnabled	Displays if Domain Local Groups are used for NSS file system permissions
AD_UseEfficientSevFetch	Display whether efficient SEV fetch option is enabled
AD_SupervisorGroup	Displays AD Group having supervisor rights on locally mounted NSS volumes
AD_NumOfTrustWhiteList	Number of AD trusts added to White list
AD_NumOfTrusts	Number of AD trusts to OES joined Active Directory forest
AD_DomainFunctionalLevel	Displays the Domain Functional level of AD domain to which OES server is joined
AD_DomainControllerFuncLevel	Displays the Domain Controller Functional level of OES joined AD domain
S2G_DB_EntriesCount	Number of entries in the Sid-to-GUID mapping database

A.3 How the Server Receives the Data

The telemetry server requests (pulls) the data from the telemetry agents. The data is stored at /var/opt/novell/telemetry/data/.

A unique GUID is generated for the agent when first time the agent sends the data to the server. By default, the agent communicates through 8000 port to push the data to the server. After the server receives the data successfully, the agent deletes the data from its location.

The telemetry server transfers the data to the OpenText server. If the transfer is unsuccessful, the system attempts to send it again during the next weekly cycle. No attempts to send the data is made outside of the weekly cycles.

The data is not encrypted because no sensitive or identifying information is included.

B OES Dashboard

OES dashboard (OES Health) provides a rich dashboard to monitor the health of all the servers (and its services) that are child nodes installed below the Cloud Integrated Storage (CIS) context in the same eDirectory tree. The CIS server contacts all the servers to provide a real-time health status.

B.1 Overview

The **OES Health** tab available in the CIS Management GUI displays the health status of the OES services. To use the dashboard functionality, you can deploy CIS as a Standalone server. For more information, see Configure CIS as a Standalone Server in NSS Media in the Cloud Integrated Storage Administration Guide.

On installing OES 24.4 the `coreagent` and `dashboardagent` services are installed. The `coreagent` service continues to work though the `dashboardagent` service stops working after three tries if it is unable to contact the CIS server.

When configuring CIS, ensure that the CIS server is configured in the highest context in the eDirectory tree. The `dashboard` agent walks up the tree in search of `cis-host-info` attribute and registers to the CIS server. If this attribute is found then the `dashboardagent` continues to run else after trying three times it stops.

If you install the CIS server later than OES 2018 SP3, the `dashboardagent` would have stopped running. You need to manually start the `dashboardagent` service.

When you click **OES Health** tab in the CIS Management GUI, the CIS server requests data from the service agents and real-time health data of the services is displayed in the GUI.

B.2 Prerequisites

- CIS is installed and configured. For more information, see Planning Your Cloud Integrated Storage Server Environment in the Cloud Integrated Storage Administration Guide.
- Port 8000 must be opened on all OES servers where core and dashboard agents are running. So the agents can communicate with the CIS server.
- Ensure that the coreagent and dashboardagent services are running.

For more details of **OES Health** tab, see OES Health in the Cloud Integrated Storage Administration Guide.

C 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 during installation or post installation.

To add services to an existing OES server, follow the instructions in "Installing or Configuring OES Services on an Existing OES Server" in the *Installation Guide*.

D Changing an OES Server's IP Address

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

- Section D.1, "Caveats and Disclaimers," on page 223
- Section D.2, "Prerequisites," on page 223
- Section D.3, "Changing the Server's Address Configuration," on page 224
- Section D.4, "Reconfiguring the OES Services," on page 224
- Section D.5, "Repairing the eDirectory Certificates," on page 225
- Section D.6, "Completing the Server Reconfiguration," on page 225
- Section D.7, "Modifying a Cluster," on page 226
- Section D.8, "Reconfiguring Services on Other Servers That Point to This Server," on page 226

D.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 host name of the server.

D.2 Prerequisites

- Section D.2.1, "General," on page 223
- Section D.2.2, "iPrint," on page 224
- Section D.2.3, "Clustering," on page 224

D.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.

D.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 23.4: OES iPrint Administration Guide*.

D.2.3 Clustering

If the server is running Cluster Services:

1. Check your plans against the prerequisites for clusters in "IP Address Requirements" in the *OES Cluster Services for Linux Administration Guide*.
2. Follow the instructions in "Changing the IP Addresses of Cluster Resources" in the same guide.

D.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 server, to the `root` (`/`) partition of the OES 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 D.2.1, "General," on page 223 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 D.2.1, "General," on page 223, changing each of the following as necessary:
   - IP Address
   - Subnet Mask
   - Router (Gateway)
7. Close YaST, then continue with Section D.4, "Reconfiguring the OES Services," on page 224.

D.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
```

D.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.

D.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 D.6.1, "DHCP," on page 226
- Section D.6.2, "iPrint," on page 226

D.6.1 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 *DNS/DHCP Services for Linux Administration Guide*.

D.6.2 iPrint

1 Using your favorite text editor, open the following configuration file:

`/etc/opt/novell/iprint/conf/`*`DN_of_PSM`*`ipsmd.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 23.4: OES iPrint Administration Guide*.

D.7 Modifying a Cluster

If the server is running OES Cluster Services™, complete the instructions in "Modifying the Cluster Configuration Information" in the *OES Cluster Services for Linux Administration Guide*.

D.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.

E Updating/Patching OES 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 server and running the patch process, see "Updating (Patching) an OES Server" in the *Installation Guide*.

F Quick Reference to OES User Services

Use Table F-1 as a quick reference for providing your network users with instructions for accessing each OES service.

Table F-1 *OES User Services Quick Reference*

services	Access Method or URL	Notes
iPrint	http://*server_ip_address_or_dns_name/ipp* https://*server_ip_address_or_dns_name:443/ipp*	
Client for Open Enterprise Server	1. Install the Client for Open Enterprise Server on a supported Windows workstation. For Macintosh support, see Novell Kanaka for Mac. 2. Log in to eDirectory. 3. Access NCP volumes on NetWare or Linux that you have the appropriate file trustee rights to.	
OES CIFS	Map a network drive in Windows, Linux, or Mac Finder. Create a Web Folder in Internet Explorer. For more information, see the *OES CIFS for Linux Administration Guide*.	
OES Remote Manager	http://*server_ip_address_or_dns_name*:8008	Any LUM-enabled user can see their directories and files on OES servers.

G OES Browser Support

As a general rule, Open Enterprise Server management tools support the following browsers as they are available on the workstation platforms listed in "Client/Workstation OS Support" on page 233:

- Mozilla Firefox 64-bit on Windows, Macintosh, and Linux
- Microsoft Edge on windows 11
- Apple Safari on Mac 10.15.x, Mac 11 and Mac 12
- Google Chrome latest version on Windows

Table G-1 provides service-specific links and information about browser support in OES.

Table G-1 *Browser Support in OES*

Management Tool	Supported Browser Information Link
iManager	• "System Requirements for iManager Server" in the *NetIQ iManager Installation Guide* 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. 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. To avoid problems, set the first language preference to a supported language.
iMonitor	• "System Requirements" in "Using NetIQ iMonitor " in the *NetIQ eDirectory Administration Guide*
iPrint	• "Supported Browsers for iPrint" in the *OES 23.4: OES iPrint Administration Guide*
OES Remote Manager	• "System Requirements" in the *OES 23.4: OES Remote Manager Administration Guide*

H Client/Workstation OS Support

As a general rule, Open Enterprise Server services can be accessed and administered from workstations running the following operating systems:

- SUSE Linux Enterprise Server 15 SP.x
- Windows Server 2022
- Windows 10 and 11
- Macintosh 11 and 12

For specific information on a given service, consult the service documentation.

OES Service Scripts

Open Enterprise Server services rely on specific service scripts located in `/usr/lib/systemd/system`. The scripts used by OES, some of which are standard Linux scripts, are listed in Table I-1.

IMPORTANT: For managing OES services, we strongly recommend using the browser-based tools outlined in Section 9.1, "Overview of Management Interfaces and Services," on page 69. 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 I-1 *OES Service Scripts in /usr/lib/systemd/system*

Services Associated with Scripts	Script Name	Notes
Apache Web server	`apache2.service`	This lets you start, stop, and restart the Apache Web Server.
Distributed File Services	`novell-dfs.service`	This lets you start and stop the VLDB service.
DNS (NetIQ eDirectory enhanced)	`novell-named.service`	This works in connection with `named` to provide eDirectory DNS services.
Domain services Daemon	`xadsd.service`	
Dynamic Storage Technology	`novell-shadowfs.service`	This script starts and stops the shadowfs daemon and the kernel module fuse.
eDirectory	`ndsd.service`	This lets you start and stop eDirectory. It executes the `/usr/sbin/ndsd` binary.
eDirectory LDAP support	`nldap`	This lets you load and unload the LDAP library that eDirectory uses to provide LDAP support. It is not actually a service.
FTP	`pure-ftpd.service`	This is used by the OES FTP pattern.

Services Associated with Scripts	Script Name	Notes
iPrint	cups novell-idsd.service novell-ipsmd.service	These scripts are required by iPrint 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. novell-ipsmd.service lets you to start and stop the ipsmd daemon that manages printers that are assigned under a Print Manager. novell-idsd.service lets you to start and stop the idsd daemon that manages drivers that are assigned under a Driver Store.
Kerberos KDC Service	xad-krb5kdc.service	
Kerberos Password Change Server	xad-kpasswdd.service	
Linux User Management	namcd.service nscd.service	These daemons are required by Linux User Management and work together to ensure good performance. The namcd daemon caches user and group names and IDs from eDirectory, speeding subsequent lookups of cached users and groups. The nscd daemon caches host names and addresses.
Logging	rsyslog.service	This is used for logging by many OES services.
Name Service Cache Daemon	nscd.service	
OES CIFS	novell-cifs.service	This script starts and stops the cifsd daemon, which is the CIFS service daemon
DHCP	dhcpd.service	
Cluster Services (NCS)	adminfs.service	This is used for NCS through iManager and the command line interface.

Services Associated with Scripts	Script Name	Notes
Cluster Services (NCS)	`novell-ncs.service`	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. 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.
Novell Identity Translator	`novell-nit.service`	This script runs by default on every OES 2015 SP1 and later server with NSS volumes and provides user IDs (UIDs) for NSS file access. Use `rcnovell-nit` followed by `start`, `stop`, `restart`, or `status` to view or alter the run state as needed. or Use `systemctl start/stop/restart/status novell-nit.service` to start, stop, restart or view the status.
OES Remote Manager (NRM)	`novell-httpstkd.service`	This script runs by default on every OES server and enables access to NRM for Linux through a browser. 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.
Storage Services	`novell-nss.service`	This script runs by default on every OES server with NSS volumes and enables access to the NSS runtime environment. To see if the NSS kernel modules and NSS admin volume are running, enter `systemctl status novell-nss.service`, or `rcnovell-nss status` at a command prompt. If they are not running, use the `start` option to start them. You cannot stop NSS.
NSS Auditing	`novell-vigil.service`	This is the NSS auditing daemon.
NTP	`chronyd.service`	This is the SLES 15 Network Time Protocol daemon.
rsync daemon	`rsyncd.service`	DSfW depends on this

Services Associated with Scripts	Script Name	Notes
SFCB CIMOM	`sblim-sfcb.service`	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. CIFS, iPrint, and NRM also use SFCB. OES Remote Manager on OES gets its server health information from CIMOM.
SLP support	`slpd.service`	This lets you start and stop OpenSLP, which is a key component for eDirectory and certain other services and clients.
sshd service	`sshd.service`	DSfW depends on this
Storage Management Services	`novell-smdrd.service`	This lets you start and stop the SMDR daemon precess. It also loads and unloads the NSS zapi kernel module used by SMS to back up the NSS volumes.
Tomcat	`novell-tomcat.service`	This script sets up the Tomcat included with SLES 15 specifically for OES services, such as the Welcome pages.

J System User and Group Management in OES

This section discusses the users and groups that are used by Open Enterprise Server. Administrative users are discussed in Appendix K, “Administrative Users and Groups in OES,” on page 261.

- Section J.1, “About System Users and Groups,” on page 239
- Section J.2, “Understanding Proxy Users,” on page 241
- Section J.3, “Common Proxy User,” on page 244
- Section J.4, “Planning Your Proxy Users,” on page 248
- Section J.5, “Implementing Your Proxy User Plan,” on page 255
- Section J.6, “Proxy Users and Domain Services for Windows,” on page 257
- Section J.7, “System Users,” on page 257
- Section J.8, “System Groups,” on page 258
- Section J.9, “Auditing System Users,” on page 259

J.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 J.1.1, “Types of OES System Users and Groups,” on page 239
- Section J.1.2, “OES System Users and Groups by Name,” on page 240

J.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 J-1.

Table J-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 ◆ Retrieving passwords and service attributes ◆ Writing Service information in eDirectory. ◆ Providing a user ID (uid) that the associated service daemon uses to run.	◆ cifsProxyUser-*servername* ◆ *LUM_Proxy_user*
System Group	◆ Facilitate the management of system users ◆ Provide access rights to service data on the server or in the eDirectory tree.	◆ DHCP ◆ DNSDHCP
System User	The daemons associated with the respective services run as these users.	◆ wwwrun ◆ iprint

J.1.2 OES System Users and Groups by Name

Table J-2 lists the users and groups that OES services depend on and use.

Table J-2 *System User and Groups Listing*

System User or Group	Object Type	Associated Service
CifsProxyUser-*servername*	Proxy User	CIFS
*cluster_name*_MGT_GRP.*context*	System Group	NCS
DHCP LDAP Proxy	Proxy User	DHCP
dhcpd	System User	DHCP
DHCPGroup	System Group	DHCP
DNS Proxy	Proxy User	DNS
DNSDHCP-GROUP	System Group	DNS
iPrint	System User	iPrint
iPrint (POSIX) iPrintgrp (eDirectory)	System Group	iPrint
LUM proxy (optional)	Proxy User	Linux User Management

System User or Group	Object Type	Associated Service
named	System User	DNS
novell_nobody	System User	CIMOM
novell_nogroup	System Group	CIMOM
novlxregd	System User	XTier
novlxsrvd	System User	XTier
novlxtier	System Group	XTier
OESCommonProxy_*hostname*	System User	CIFS, DNS, DHCP, Clustering (NCS), Linux User Management (optional)
*server_name*admin	Proxy User	NSS
www	System Group	Apache Tomcat
wwwrun	System User	Apache

J.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 J.2.1, "What Are Proxy Users?," on page 241
- Section J.2.2, "Why Are Proxy Users Needed on OES?," on page 242
- Section J.2.3, "Which Services Require Proxy Users and Why?," on page 242
- Section J.2.4, "What Rights Do Proxy Users Have?," on page 243

J.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 242). Proxy user creation and/or configuration is therefore an integral part of configuring OES.

None of the OES services require that you specify proxy user information during the OES installation, but some, such as DNS/DHCP, and CIFS, give you the option to do so. Others, such as NCS and NSS create proxy users without user input.

J.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 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.

J.2.3 Which Services Require Proxy Users and Why?

The following services utilize a proxy user.

Table J-3 *Proxy Users Functions Listed by Service*

Associated Service	Example Proxy User Name	Services That the User Provides
CIFS	OESCommonProxy_*hostname*	Retrieves CIFS user information.
Clustering (NCS)	OESCommonProxy_*hostname*	The clustering administrator and the proxy user can be two separate users. For more information, see "OES Common Proxy User " in the *OES Cluster Services for Linux Administration Guide*.
DHCP	OESCommonProxy_*hostname*	Lets the service access DHCP objects in eDirectory.
DNS	OESCommonProxy_*hostname*	Lets the service access DNS objects in eDirectory.
Linux User Management	OESCommonProxy_*hostname*	Searches the tree for LUM users.

Associated Service	Example Proxy User Name	Services That the User Provides
NSS	*server_name*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.

J.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 J-4.

Table J-4 *Proxy Users Rights*

Associated Service	Example Proxy User Name	Default Rights Granted
CIFS	CifsProxyUser-*servername*	◆ This proxy user has Compare and Read rights to the specified CIFS user search context.
Clustering (NCS)	OESCommonProxy_*hostname* 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.
DHCP	DHCP_LDAP_Proxy	◆ No rights are assigned directly, but membership in the DHCPGroup, which does have assigned rights, provides the rights it needs.
DNS	DNS_Proxy	◆ No rights are assigned directly, but membership in the DNS-DHCPGroup, which does have assigned rights, provides the rights it needs.
Linux User Management	*LUM_proxy*	◆ If created, this proxy user has Search rights on Unix Config & Unix Workstation Objects.
NSS	*server_name*admin	◆ Additional eDirectory rights: Supervisor right to the container it was created in.

J.3 Common Proxy User

- Section J.3.1, “Common Proxy User FAQ,” on page 244
- Section J.3.2, “Managing Common Proxy Users,” on page 247

J.3.1 Common Proxy User FAQ

- “Why Would I Want to Specify Common Proxy Users?” on page 245
- “Why Was a Proxy User Added to Cluster Services?” on page 245
- “Which Services Can and Cannot Leverage the Common Proxy User?” on page 245
- “Can a Common Proxy User Service Multiple Servers?” on page 246
- “Can I Change the Common Proxy User Name and Context?” on page 246
- “Can I Assign the Common Proxy User After Services Are Installed?” on page 246
- “What About Upgraded Servers Using a Common Proxy?” on page 246

Why Would I Want to Specify Common Proxy Users?

The implementation of a common proxy user in OES 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 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 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 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 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 245
- "Service That Cannot Leverage the Common Proxy User" on page 246

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):

- CIFS
- Cluster Services
- DNS
- DHCP

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)

Service That Cannot Leverage the Common Proxy User

The following service that use proxy users do not leverage the Common Proxy user for the reasons listed:

Service	Reason
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 247.

What About Upgraded Servers Using a Common Proxy?

You can change the services running on an upgraded OES server to leverage a Common Proxy user. See “Assigning the Common Proxy to Existing Services” on page 247.

J.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 247
- "Assigning the Common Proxy to Existing Services" on page 247
- "Changing Proxy Passwords Automatically" on page 248

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 as a New Installation" in the *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 245 using the `move_to_common_proxy.sh` script on your OES server. In fact, if you have upgraded from OES 11 SP2 and the server does not 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-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 latest OES server.
- 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

   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.

J.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 J.4.1, “About Proxy User Creation,” on page 248
- Section J.4.2, “There Are No Proxy User Impacts on User Connection Licenses,” on page 251
- Section J.4.3, “Limiting the Number of Proxy Users in Your Tree,” on page 251
- Section J.4.4, “Password Management and Proxy Users,” on page 253

J.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 248
- “Do Not Manually Configure Proxy Users” on page 250
- “Avoid Assigning an Admin User As a Proxy User” on page 251

Creation Options

Table J-2 presents information about the creation options for each OES proxy user.

Table J-5 *Proxy User Creation Options*

Associated Service	Service Proxy User Name if Applicable	Creation Information
CIFS	OESCommonProxy_*hostname* Or CifsProxyUser-*servername*	◆ **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: ◆ Creates a proxy user named cifsProxyUser-*servername* in the same context as the server. ◆ Generates a password, and stores it in either OCS or in an encrypted file on the server, depending on which option you select. 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.
Clustering (NCS)	OESCommonProxy_*hostname* Or installing admin user	◆ **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.
DHCP	OESCommonProxy_*hostname* Or installing administrator	◆ **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.

Associated Service	Service Proxy User Name if Applicable	Creation Information
DNS	OESCommonProxy_*hostname* Or installing administrator	◆ **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_*hostname* Or DNS	◆ **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.
Linux User Management	OESCommonProxy_*hostname* Or *LUM_proxy* (optional)	By default, no LUM proxy user is created. ◆ **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. If you assign a previously created user as the LUM proxy user, it must have the Read right to the LDAP service.
NSS	*server_name*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.

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 244 and "Limiting the Number of Proxy Users in Your Tree" on page 251.

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 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 as the proxy user credentials for some of the OES service installations. Consequently, the credentials were stored in OCS for use when the OES services came up.

Because the Admin password had changed, the OCS credentials had expired and service authentication requests were failing, resulting in the intruder detection lockout.

J.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.

J.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 J-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 J-6 *Options for Limiting the Number of Proxy Users*

Approach	Security Considerations	Manageability Considerations
Per Service per Server	For CIFS this is the most secure option. By default, the passwords for these are system-generated and not known by anyone. For LUM there is no option to have a system-generated password. For DNS and DHCP, 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 251.	This approach requires no proxy user planning. Services are installed at the same time as the OES server. This is a good option for small organizations or installations where only a few services are used. This is not a good option if security policies dictate that all passwords must be reset periodically.
Per Server	This confines any security vulnerabilities to individual servers and is the scenario for which the Common Proxy User was developed.	This requires that a proxy user for the server is created before the server is installed. 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. 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. 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.
Per Partition	This confines any security vulnerabilities to individual partitions.	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. This is a good approach for organizations where eDirectory administration is done at a partition level. This requires that a proxy user for the first server in the partition is created before services are installed in the partition. The install admin must know the proxy user's password.

Approach	Security Considerations	Manageability Considerations
Per Service	This confines any security vulnerabilities to individual services. 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	For example, you might have one proxy user for CIFS, one for DNS/DHCP, one for iPrint etc. This is useful in trees where the users and servers are not co-located, and different services are administered by different administrators. This requires that a proxy user for the service is created before the service is installed in the tree. The install admin must know the proxy user's password.
Per Tree	This exposes all OES services and servers in the tree to any security vulnerabilities.	A proxy user for the tree must be created before any OES services are installed in the tree. This is suitable for organizations that have ◆ 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. The install admin must know the proxy user's password.

J.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 253
- "Passwords Are Stored on the Server" on page 254
- "Avoid Password Expiration Problems" on page 254
- "Changing Proxy Passwords Automatically" on page 255
- "Changing Proxy Passwords Manually" on page 255

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 and CIFS Proxy User 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 251.

Passwords Are Stored on the Server

Of course all proxy user passwords are stored in eDirectory. Table J-7 explains where they are stored on the server and how they can be reset if needed.

Table J-7 *Password Storage Locations*

Associated Service	Where the Password Is Stored Locally	How the Password Can Be Reset
CIFS	If the service-specific proxy user is used, the password is stored in either OCS or in an encrypted file, depending on the configuration option specified during service installation.	You can use iManager to reset the password in OCS or in the encrypted file, or the oescredstore tool if it is stored in OCS.
Common Proxy User	This password is stored in OCS.	We recommend that you only use the `change_proxy_pwd.sh` script to manage Common Proxy User passwords.
DHCP	The service-specific password is stored in OCS.	You can set the password using the oescredstore tool.
DNS	If the service-specific proxy user is used, the service-specific password is stored in OCS if it is available. If OCS is not available, it is stored in an encrypted file.	
Linux User Management	If the service-specific proxy user is used, the service-specific is stored in OCS.	This can be changed in iManager through the Linux User Management plug-in.
NSS		This password is system-generated at install time and cannot be reset.

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 251.

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 255.

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 J-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.

J.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 J-5 on page 249). In most cases a default configuration assigns the install admin as the proxy user for the service.

- Section J.5.1, “Tree-Wide Proxy Users,” on page 256
- Section J.5.2, “Service-Specific Proxy Users,” on page 256
- Section J.5.3, “Partition-Wide Proxy Users,” on page 256
- Section J.5.4, “Server-Wide Proxy User,” on page 257
- Section J.5.5, “Individual Proxy User Per-Server-Per-Service,” on page 257

J.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.

J.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.

J.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.

J.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.

J.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 J-6, “Options for Limiting the Number of Proxy Users,” on page 252.

J.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.

J.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 J-2 lists the various system users that are used by OES services.

Table J-8 *System User Purposes*

System User or Group Name	Associated Service	Purpose
dhcpd	DHCP	DHCP accesses local resources through this or an alternatively specified user. If the DHCP lease and configuration files are stored on NSS, the user must be moved to eDirectory and LUM enabled. dhcpd is used by default, but any local user can be used.
iprint	iPrint	The iPrint daemons run as this user. If iPrint is moved to NSS, this user is created in eDirectory and the local user is removed.
named	DNS	This system user lets DNS access local resources. In case of clusters, DNS data is on NSS volume, and so the user has to be created in eDirectory as well. named is used by default, but any local user can be used.
novell_nobody	CIMOM	This user is created by CIMOM but is not currently used.
novlxregd	XTier	The XTier Registry Daemon (novell-xregd) runs as this user. When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.
novlxsrvd	XTier	The XTier Server Daemon (novell-xsrvd) runs as this user. When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.
wwwrun	Apache	The Apache daemon runs as this user. When NSS is installed on the Linux server, this user is removed from the local system and created as LUM-enabled user in eDirectory. This is required because it must have access to NSS data, and all NSS access is controlled through eDirectory.

J.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 J-2 lists the system groups that are used by OES services.

Table J-9 *System Group Purposes*

System User or Group Name	Associated Service	Purpose
Iprint (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	`ncsclient` 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 (wwwrun) 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.
www	Apache Tomcat	Apache (wwwrun) and tomcat (novlwww) use the group ID (gid) of this group to run. User `novlxsrvd` is in the group because it needs access to an Apache domain socket. When NSS is installed on the Linux server, this group is removed from the local system and created in eDirectory. This is required because members of this group must have access to NSS data, and all NSS access is controlled through eDirectory.

J.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/) 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).

K Administrative Users and Groups in OES

- Section K.1, “eDirectory Administrative Users and Groups,” on page 261
- Section K.2, “Active Directory Administrative Users and Groups,” on page 261

K.1 eDirectory Administrative Users and Groups

Every OES network requires at least one administrative-level user to manage regular network users and system users.

Table K-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.

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*.

K.2 Active Directory Administrative Users and Groups

Administrative access to NSS AD service components is controlled by the AD users and groups summarized in Table K-2.

Table K-2 *Administrative Users and Groups*

Administrative Group	Associated Service	Object Type	Purpose
Administrator	Active Directory	Admin user	The Active directory administrator that has all rights to manage the Active Directory Domain
Delegated Administrator	Active Directory	Admin user	These administrators are usually responsible for administering within a specific OU. They might be assigned only enough rights to install servers or they might be assigned to specific roles. These are similar to eDirectory Container Administrators.
Domain Admins	NSS AD	AD Group	Members of this group in the domain the OES server has joined, have Supervisor rights on the AD-enabled volumes associated with those servers. A different group can be designated through the `nitconfig` utility or by manually editing the `nitd.conf` file.
OESAccessGrp	NSS AD	AD Group	Members of this group have rights to manage trustee assignments, file attributes, and so forth on AD-enabled NSS volumes as their trustee assignments allow. If the group doesn't exist, all AD users with the required trustee assignments can perform management tasks on AD-enabled volumes.

L Coordinating Password Policies Among Multiple File Services

- Section L.1, “Overview,” on page 263
- Section L.2, “Concepts and Prerequisites,” on page 263
- Section L.3, “Examples,” on page 264
- Section L.4, “Deployment Guidelines for Different Servers and Deployment Scenarios,” on page 267

L.1 Overview

OES includes native file services for Windows and Macintosh workstations:

Macintosh Workstations	Windows Workstations
◆ OES CIFS	◆ OES CIFS ◆ Domain Services for Windows (DSfW) DSfW is not classified as a file service, but it includes a customized version of Samba.

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.

L.2 Concepts and Prerequisites

Prerequisites for CIFS access are explained in the following sections:

- Section L.2.1, “Prerequisites for File Service Access,” on page 263
- Section L.2.2, “eDirectory contexts,” on page 264
- Section L.2.3, “Password Policies and Assignments,” on page 264

L.2.1 Prerequisites for File Service Access

The following are the prerequisites for user access to CIFS 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 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 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.

L.2.2 eDirectory contexts

- **CIFS:** The eDirectory contexts of users can be specified either in the domain name format (Active Directory format) or in the X.509 format.

L.2.3 Password Policies and Assignments

- **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.

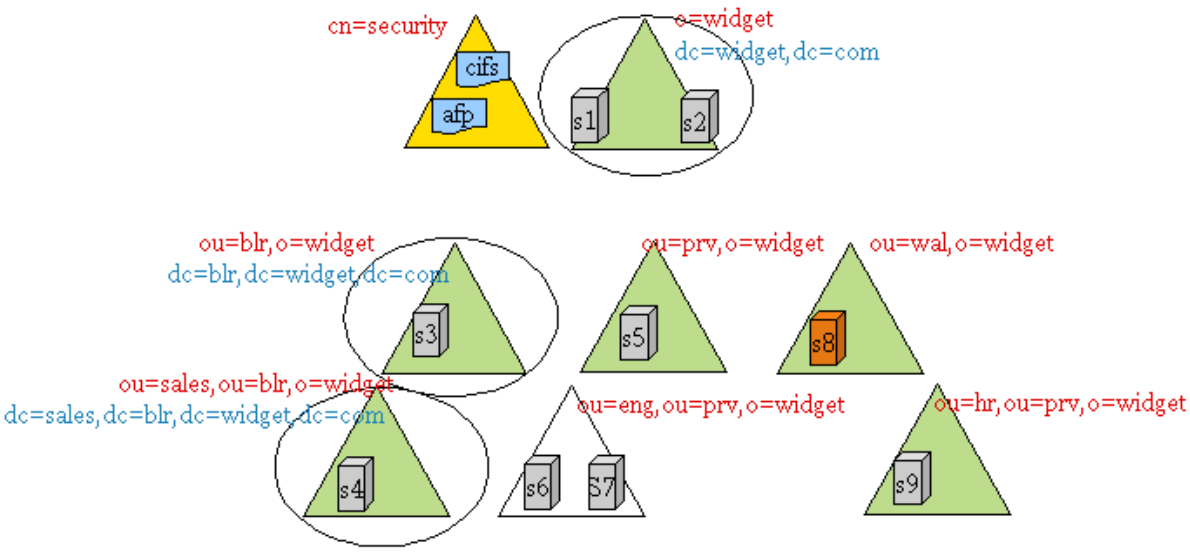
L.3 Examples

- Section L.3.1, “Example 1: Complex Mixed Tree with a Mix of File Access Services and Users from across the Tree,” on page 264
- Section L.3.2, “Example 2: Mutually Exclusive Users,” on page 266

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

- “Tree Setup” on page 265
- “OES/NetWare Servers” on page 265
- “File Services” on page 265
- “User Access to Services” on page 266
- “Rights Required for Installation and Administration” on page 266

Figure L-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 NCP
- S6 serves its volumes over CIFS and NCP
- S7 serves its volumes over CIFS, and NCP
- S8 serves its volumes over NetWare CIFS, and NCP
- S9 serves its volumes over NCP

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 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

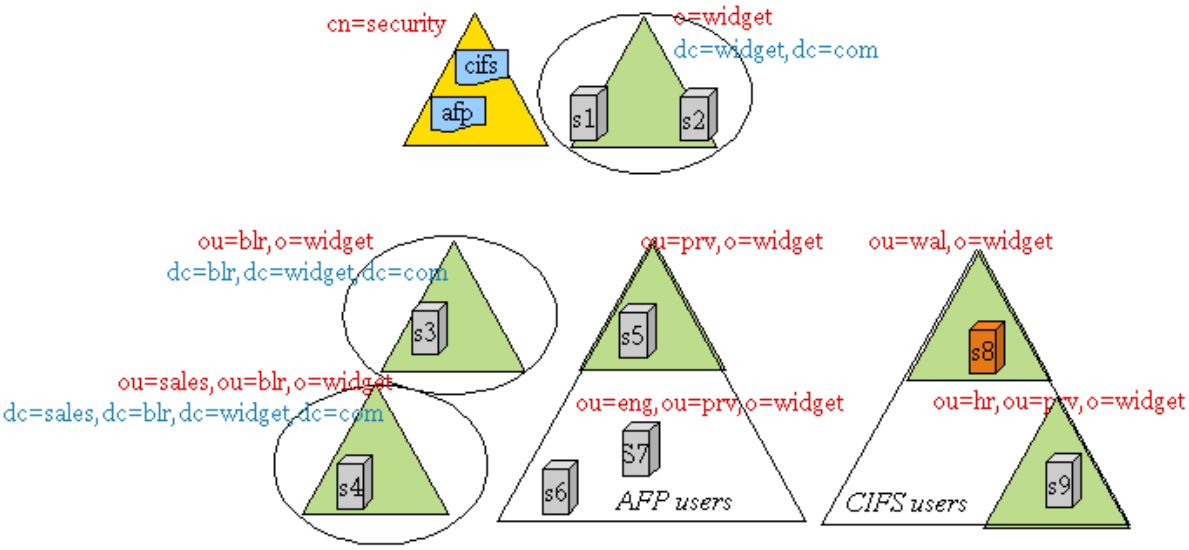
Installation and configuration in iManager must be done by an OES administrator. This is typically a container administrator in eDirectory who has supervisory privileges over the container where the server is being installed. This need not be the tree administrator.

L.3.2 Example 2: Mutually Exclusive Users

- "File Services" on page 266
- "Users" on page 267

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 L-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 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.

L.4 Deployment Guidelines for Different Servers and Deployment Scenarios

- Section L.4.1, “Deployment Scenario 1: Complex Mixed Scenario with a Mix of File Access Services,” on page 267
- Section L.4.2, “Deployment Scenario 2: Mutually /Exclusive Users,” on page 269
- Section L.4.3, “Deployment Scenario 3: Simple deployments,” on page 269
- Section L.4.4, “Modifying User Password Policies after Samba/DSfW Is Installed,” on page 269
- Section L.4.5, “Adding New User eDirectory Contexts to CIFS after CIFS/DSfW Is Installed.,” on page 269
- Section L.4.6, “Enabling File Access for DSfW Servers Across Domains,” on page 270

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

- “First Server in a New Tree (Example1)” on page 267
- “Subsequent Servers in a Tree (Example 1)” on page 268

First Server in a New Tree (Example1)

- “Not recommended—non-name-mapped (new tree) S1 (DSfW) server” on page 267
- “Non-DSfW Server” on page 268

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. CIFS cannot 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 CIFS 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 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 CIFS users.
5. If the CIFS 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 268
- "S5" on page 268
- "S6" on page 268
- "S7" on page 268
- "S8" on page 268
- "S9" on page 269

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 *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

- 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 CIFS users.
- If this NetWare box is migrated to OES and CIFS users should be enabled for Universal Password by having a password policy configured. CIFS users need to log in through NCP (Client for Open Enterprise Server) 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.

L.4.2 Deployment Scenario 2: Mutually /Exclusive Users

In some trees, CIFS might be employed, but the users are partitioned in such a way that each user has access to CIFS, 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.

L.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.

L.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.

L.4.5 Adding New User eDirectory Contexts to CIFS after CIFS/DSfW Is Installed.

If users from additional or different eDirectory contexts need to be allowed to access CIFS, rerun the YaST–based configuration and modify or add the required eDirectory user contexts.

L.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.

M Configuration and Log Files

- Section M.1, “CIFS,” on page 271
- Section M.2, “CIS,” on page 272
- Section M.3, “Common Proxy,” on page 272
- Section M.4, “DFS,” on page 273
- Section M.5, “DHCP,” on page 273
- Section M.6, “DNS,” on page 273
- Section M.7, “Domain Services for Windows,” on page 274
- Section M.8, “Pure-FTPd,” on page 276
- Section M.9, “Install,” on page 276
- Section M.10, “iPrint,” on page 277
- Section M.11, “Linux User Management,” on page 278
- Section M.12, “Migration Tool,” on page 278
- Section M.13, “Cluster Services,” on page 280
- Section M.14, “OES File Access Rights Management (NFARM),” on page 280
- Section M.15, “Novell Identity Translator (NIT),” on page 281
- Section M.16, “Linux Volume Manager (NLVM),” on page 281
- Section M.17, “Storage Services,” on page 281
- Section M.18, “novell-ad-util,” on page 282
- Section M.19, “NCP,” on page 282
- Section M.20, “SMS,” on page 283
- Section M.21, “Vigil,” on page 284

M.1 CIFS

Table M-1 *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 M-2 *CIFS Log Files*

Path	Description
/var/opt/novell/log/cifs.log	CIFS server run-time

M.2 CIS

Table M-3 *CIS Configuration Files*

Path	Description
/etc/opt/novell/cis/config	CIS server configuration
/etc/opt/novell/cis/fluentbit/config	CIS server log configuration
/etc/opt/novell/cis/fluentbit/fluentd.conf	Fluent Bit configuration for CIS server
/etc/opt/novell/cis/certs/rootCAs	If secure communication is used with the target cloud or object store, copy the CA bundle in PEM format to this location.

Table M-4 *CIS Log Files*

Path	Description
/var/log/messages	CIS server logs
/var/opt/novell/log/cis/microservices	Common log location of all the CIS services
/var/opt/novell/log/coreagent/coreagent.log	Contains log messages of OES Core agent
/var/opt/novell/log/cisagent/agent.log	Contains log messages of OES server agent
/var/opt/novell/log/cisagent/recallagent.log	Contains log messages of OES server recall agent
/var/opt/novell/log/cisagent/cisscanner.log	Contains log messages of OES server scanner
/var/opt/novell/log/dashboardgent/dashboard.log	Contains log messages of OES dashboard agent
/var/log/mysql/mysqld.log	MariaDB server logs
/var/log/elasticsearch/elasticsearch.log	Elasticsearch logs

M.3 Common Proxy

Table M-5 *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 M-6 *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	

M.4 DFS

Table M-7 *DFS Log Files*

Path	Description
/var/log/messages	DFS Logs
/var/opt/novell/tomcat/webapps/nps/WEB-INF/logs/debug.html	iManager Logs
/var/opt/novell/log/dfs/vlrpr.log	VLDB Repair Logs

M.5 DHCP

Table M-8 *DHCP Configuration Files*

Path	Description
/etc/dhcpd.conf	

Table M-9 *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

M.6 DNS

Table M-10 *DNS Configuration Files*

Path	Description
/etc/opt/novell/named/named.conf	configuration file loaded from e-directory

Table M-11 *DNS Log Files*

Path	Description
/var/opt/novell/log/named_zones.info	
/var/opt/novell/log/named.run	

M.7 Domain Services for Windows

Table M-12 *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/ndsmodules.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.
/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 M-13 *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 “rdndctrace 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-kpasswdd) 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.

M.8 Pure-FTPd

Table M-14 *Pure-FTPd Log and Message Files)*

Path	Description
/etc/opt/novell/oes-ftp-ipc/oesftpipc.yaml	Configuration file for oesftpipc daemon. You can modify the log level (Debug, Information, or Error), which is case-sensitive. The default setting is Information.
/etc/pure-ftpd/pure-ftpd.conf	Configuration file of pure-ftpd daemon.
/var/log/messages	Contains log messages of pure-ftpd daemon and oesftpipc daemon.

M.9 Install

Table M-15 *Install Framework Configuration Files*

Path	Description
/etc/sysconfig/novell/cmmn	
/etc/sysconfig/novell/edir	
/etc/sysconfig/novell/iman	
/etc/sysconfig/novell/iprnt	
/etc/sysconfig/novell/ldap_servers	
/etc/sysconfig/novell/lum	
/etc/sysconfig/novell/ncpsrvr	
/etc/sysconfig/novell/ncs	
/etc/sysconfig/novell/nss	
/etc/sysconfig/novell/nssad	
/etc/sysconfig/novell/NvlCifs	
/etc/sysconfig/novell/NvlDhcp	
/etc/sysconfig/novell/NvlDns	
/etc/sysconfig/novell/oes-cis	
/etc/sysconfig/novell/oes-ldap	
/etc/sysconfig/novell/schematool	
/etc/sysconfig/novell/sms_	
/etc/sysconfig/novell/xad	

Table M-16 *Install Framework Log Files*

Path	Description
/var/opt/novell/eDirectory/log/oes_schema.log	

M.10 iPrint

Table M-17 *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 M-18 *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
`journalctl -u novell-tomcat`	Command to view log information for iManager activities

M.11 Linux User Management

Table M-19 *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 M-20 *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.

M.12 Migration Tool

Table M-21 *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 M-22 *Migration Tool Log Files*

Path	Description
<project_folder>/data.log	The output and errors encountered during execution of migedir command.
<project_folder>/mignds.log	The log file created during edirectory dib copy
<project_folder>/mignds check.log	The log file created for nds time sync check
<project_folder>/log/av.log	This stores the information about the command sequence and errors encountered during AV migration.

Path	Description
<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.
<project_folder>/log/filesystem.log	This stores the information about the command sequence and errors encountered during File System migration.
<project_folder>/log/filesystem.delete.log	This stores list of files deleted from the target server because they were not available on the source server when performing the migration. This log file is updated with list of deleted files if you have selected the option **Delete Files Not On Source** in the File Options tab.
<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/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 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/migmatchup.log	migmatchup 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

Path	Description
/var/opt/novell/log/migration/migrights.log	migrights debug log
/var/opt/novell/log/migration/volmount.log vol	mount debug log

M.13 Cluster Services

Table M-23 *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 M-24 *NCS Log Files*

Path	Description
/var/log/messages	Cluster event log. Events are viewable in 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
/var/opt/novell/log/ncs/repair.log	Repair option messages (new in OES 2015)

M.14 OES File Access Rights Management (NFARM)

This is a Windows shell extension. There is no configuration file involved.

Table M-25 *NFARM Log Files*

Path	Description
C:\Users\<Logged_in_user>\AppData\Roaming\NFARM\nfarm_all.log	All NFARM transactions log
C:\Users\<Logged_in_user>\AppData\Roaming\NFARM\nfarm_error.log	NFARM error log

M.15 Novell Identity Translator (NIT)

Table M-26 *NIT Configuration Files*

Path	Description
/etc/opt/novell/nit/nitd.conf	NIT configuration file

Table M-27 *NIT Log Files*

Path	Description
/var/opt/novell/log/nit/nit.log	Default path to NIT daemon log
/var/opt/novell/log/nit/nitconfig.log	nitconfig utility log

M.16 Linux Volume Manager (NLVM)

Table M-28 *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 M-29 *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.

M.17 Storage Services

Table M-30 *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 M-31 *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.

M.18 novell-ad-util

Table M-32 *Configuration Files Associated with novell-ad-util*

Path	Description
novell-ad-util doesn't have configuration files. However, when an OES 2015 or later server join an AD domain as required by the NSS AD integration service, the following files are updated.	
/etc/krb5.conf	The OES server's Kerberos configuration
/etc/krb5.keytab	The default keytab file that contains the Service Principals of the OES server and the OES cluster resource if the server is functioning as a cluster node.

Table M-33 *novell-ad-util Log Files*

Path	Description
/var/opt/novell/log/oes/novell-ad-util/novell-ad-util.log	
/var/log/novell-ad-util/novell-ad-util.log	

M.19 NCP

Table M-34 *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

Path	Description of Configuration File
/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 M-35 *NCP Log Files*

Path	Description of Log File
/var/opt/novell/log/libnrm2ncp.log	Communication between NRM (OES 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

M.20 SMS

Table M-36 *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 M-37 *SMS Log Files*

Path	Description of Log File
/var/log/messages	Default path
/var/opt/novell/log/sms/smdrd_debug_MYPID.log	When debug is enabled, logs for SMDRD calls (related to PID)
/var/opt/novell/log/sms/tsafs_debug_MYPID.log	When debug is enabled, logs of TSAFS calls (related to PID)

M.21 Vigil

Table M-38 *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 M-39 *Vigil Log Files*

Path	Description of Log File
/var/log/audit/vlog/<clientName>/	Log files represent the auditing data stream between the NSS Auditing Engine and vlog

N Small Footprint CIM Broker (SFCB)

- Section N.1, “Overview,” on page 285
- Section N.2, “OES CIM Providers,” on page 286
- Section N.3, “SFCB Is Automatically Installed with OES,” on page 286
- Section N.4, “Coexistence with NRM and iManager in Earlier Releases,” on page 286
- Section N.5, “SFCB and Linux User Management (LUM),” on page 287
- Section N.6, “Links to More Information about WBEM and SFCB,” on page 287

N.1 Overview

OES services are managed using Web-Based Enterprise Management (WBEM) as proposed by the Distributed Management Task Force (DMTF) (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 15 provides SFCB as default CIMOM and CIM clients. OES uses these because they are part of the base OS.

N.2 OES CIM Providers

Package (RPM)	Description
novell-lum-providers	Used by the Linux User Management iManager plug-in (novell-usermanagement-imanager-plugin) to read lum configuration from /etc/nam.conf and lum enabled services information from /etc/pam.d
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 and CIFS.
novell-sms-cmpi-provider	Reads and modifies the SMS configuration files and is also used for administration of NSS, CIFS, NCS, and DFS. The providers are compiled and located in the `/opt/novell/lib64/sfcb/cmpi` folder.

N.3 SFCB Is Automatically Installed with OES

When you install any OES components that depend on WBEM, SFCB and all of its corresponding packages are installed with the components.

N.4 Coexistence with NRM and iManager in Earlier Releases

The SFCB-based CIM providers in OES 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).

N.5 SFCB and Linux User Management (LUM)

SFCB is automatically PAM-enabled for LUM as part of OES installation. Users not enabled for LUM cannot use the CIM providers to manage OES.

N.6 Links to More Information about WBEM and SFCB

For more information about WBEM, CIM, and SFCB, see the following:

- "Web Based Enterprise Management" (https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-wbem.html) in the SLES documentation (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-administration.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.sourceforge.net/wiki/index.php/Sfcb) Web site.