opentext™

Open Enterprise Server 24.4
Installation 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 What's New or Changed in OES Install 13

1.1 What's New or Changed in OES 25.3 . . . 13
1.2 What's New or Changed in OES 25.2 . . . 13
1.2.1 Identity Console . . . 13
1.2.2 SUSE Manager . . . 13
1.3 What's New or Changed in OES 25.1 . . . 13
1.3.1 Allowlist to Exempt from MFA . . . 13
1.3.2 SSRF through Host Header Injection . . . 14
1.3.3 SUSE Manager Support . . . 14
1.3.4 ZENworks Support . . . 14
1.4 What's New or Changed in OES 24.4.1 . . . 14
1.5 What's New or Changed in OES 24.4 . . . 14
1.5.1 OES MFA on CIFS Service . . . 14
1.5.2 iPrint Advanced . . . 14
1.5.3 OES Database . . . 14
1.5.4 OES FTP Server . . . 15
1.5.5 Unified Management Console . . . 15

2 Preparing to Install OES 17

2.1 Before You Install . . . 17
2.2 Meeting All Server Software and Hardware Requirements . . . 17
2.2.1 Server Software . . . 17
2.2.2 Server Hardware . . . 18
2.3 OES eDirectory Rights Needed for Installing OES . . . 19
2.3.1 Rights to Install the First OES Server in a Tree . . . 19
2.3.2 Rights to Install the First Three Servers in an eDirectory Tree . . . 19
2.3.3 Rights to Install the First Three Servers in any eDirectory Partition . . . 19
2.4 Installing and Configuring OES as a Subcontainer Administrator . . . 19
2.4.1 Rights Required for Subcontainer Administrators . . . 20
2.4.2 Starting a New Installation as a Subcontainer Administrator . . . 22
2.4.3 Adding/Configuring OES Services as a Different Administrator . . . 23
2.5 Preparing eDirectory for OES . . . 23
2.5.1 Extending the Schema . . . 23
2.6 Deciding What Patterns to Install . . . 25
2.7 Obtaining OES Software . . . 33
2.8 Preparing Physical Media for a New Server Installation . . . 33
2.9 Setting Up a Network Installation Source . . . 34
2.9.1 SUSE Linux as a Network Installation Source Server . . . 34
2.9.2 Windows as a Network Installation Source Server . . . 37
2.10 Install Only One Server at a Time . . . 37
2.11 What's Next . . . 37

3 Installing OES as a New Installation 39

3.1 Linux Software RAIDs Are Not Cluster Aware . . . 39
3.2 Linux Software RAIDs. . . . 40
3.3 Starting the OES Installation . . . 40
3.3.1 Installing from Physical Media . . . 40
3.3.2 Installing from a Network Source . . . 41
3.4 Specifying Network Settings . . . 42
3.5 Specifying Customer Center Configuration Settings . . . 42
3.6 Specifying the Add-On Product Installation Information . . . 43
3.7 System Role in OES 24.4 . . . 44
3.7.1 OES System Roles . . . 44
3.8 Setting Up Disk Partitions . . . 45
3.8.1 Guidelines . . . 45
3.8.2 NSS on the System Disk . . . 46
3.8.3 Security Flag Recommendations . . . 47
3.8.4 Partitioning X86 Machines . . . 47
3.8.5 Disk Partition Statistics . . . 48
3.8.6 Combining Hard Disk Partitions . . . 48
3.9 Setting Up the Clock and Time Zone . . . 48
3.10 Creating Local User . . . 48
3.11 Authentication for the System Administrator “root” . . . 49
3.12 Specifying the Installation Settings . . . 49
3.12.1 Customizing the Software Selections . . . 49
3.12.2 Configuring the Firewall Settings. . . . 51
3.12.3 Setting Systemd Target . . . 53
3.12.4 Accepting the Installation Settings . . . 53
3.13 Configuring Open Enterprise Server . . . 54
3.13.1 Typical Configuration . . . 54
3.13.2 Custom Configuration . . . 55
3.13.3 Specifying eDirectory Configuration Settings . . . 55
3.13.4 Specifying LDAP Configuration Settings . . . 61
3.13.5 Configuring OES Services . . . 61
3.13.6 Configuration Guidelines for OES Services . . . 63
3.14 Product Improvement . . . 83
3.14.1 How is Data Sent to the Micro Focus Server . . . 83
3.14.2 Opt Out of Product Improvement . . . 83
3.15 Finishing the Installation . . . 84
3.16 Verifying that the Installation was Successful . . . 84
3.17 What's Next . . . 86

4 Installing or Configuring OES Services on an Existing OES Server 87

4.1 Adding/Configuring OES Services on an Existing Server. . . . 87
4.2 Adding/Configuring OES Services on a Server That Another Administrator Installed . . . 89
4.3 What's Next . . . 90

5 Upgrading OES 91

5.1 Supported OES Upgrade Paths . . . 91
5.2 Planning for the Upgrade . . . 92
5.2.1 Be Sure to Check the Release Notes . . . 92

5.2.2 Understanding the Implications for Other Products Currently Installed on the Server . . . 92
5.2.3 Upgrading the OES Cluster Nodes . . . 92
5.3 Meeting the Upgrade Requirements . . . 93
5.3.1 Removing Identity Console . . . 94
5.3.2 Securing Current Data . . . 94
5.3.3 Ensuring That There Is Adequate Storage Space on the Root Partition . . . 94
5.3.4 Converting ReiserFS to Btrfs File System . . . 95
5.3.5 Preparing the Server You Are Upgrading . . . 95
5.3.6 Checking the Server's DNS Name . . . 95
5.3.7 Ensuring That the Server Has a Server Certificate . . . 95
5.3.8 Changing the Mount Options Before an Upgrade . . . 96
5.3.9 Preparing an Installation Source . . . 96
5.3.10 Synchronizing the OES Configuration Information before Starting an Upgrade . . . 96
5.4 Upgrading OES . . . 97
5.4.1 Using Physical Media to Upgrade . . . 98
5.4.2 Specifying the Partition to Update . . . 98
5.4.3 Reviewing the Previously Used Repositories . . . 99
5.4.4 Specifying Customer Center Configuration Settings . . . 99
5.4.5 Specifying the Add-On Product Installation Information . . . 101
5.4.6 Verifying and Customizing the Update Options in Installation Settings . . . 101
5.4.7 Accepting the Installation Settings . . . 103
5.4.8 Specifying Configuration Information . . . 103
5.4.9 Participating in Product Improvement Consent Screen . . . 107
5.4.10 Finishing the Upgrade . . . 107
5.4.11 Migrating Clustered Linux Volume Resource from clvmd to lvmlockd . . . 108
5.5 Using AutoYaST for OES Upgrade . . . 109
5.5.1 Prerequisites . . . 110
5.5.2 Creating an Answer File to Provide the eDirectory and DSfW Passwords . . . 110
5.5.3 Upgrading OES . . . 111
5.5.4 Upgrading OES on a XEN Host Server . . . 111
5.5.5 Troubleshooting an AutoYaST Upgrade . . . 112
5.6 Channel Upgrade from OES 24.3 to OES 24.4 . . . 112
5.6.1 Channel Upgrade from OES 24.3 to OES 24.4 via Wagon . . . 113
5.6.2 Channel Upgrade from OES 24.3 to OES 24.4 using Zypper . . . 116
5.6.3 Upgrading OES 24.3 to OES 24.4 using Subscription Management Tool (MFSMT) . . . 117
5.6.4 Rolling back the Server in the Middle of a Wagon-based Channel Upgrade . . . 118
5.7 Upgrading Open Enterprise Server Using SUSE Manager . . . 119
5.8 Using ZENworks to Upgrade from OES 23.4 to OES 24.4 or later . . . 120
5.9 Verifying that the Upgrade was Successful . . . 120
5.10 What's Next . . . 121

6 Completing OES Installation Tasks 123

6.1 Determining Which Services Need Additional Configuration . . . 123
6.2 Rebooting the Server after Installing NSS . . . 124
6.3 Restarting Tomcat . . . 124
6.4 Implementing Digital Certificates in an OES Environment . . . 124
6.4.1 Configuring the Digital Certificate . . . 125
6.4.2 Reconfiguring Services after Importing the Certificate . . . 125

7 Installing and Configuring NSS Active Directory Support 127

7.1 Understanding the NSS AD Support . . . 127

7.1.1 NSS Resource Access Until OES 11 SP2 . . . 127
7.1.2 NSS Resource Access with OES 2015 or Later . . . 129
7.2 NSS AD Support Matrix . . . 130
7.3 Prerequisites for Installing and Configuring NSS AD . . . 131
7.4 Installing OES 24.4 with NSS AD Support . . . 132
7.4.1 Resolving the AD DNS Name from OES 24.4 . . . 134
7.4.2 Installing and Configuring NSS AD Support . . . 134
7.4.3 Validating the NSS AD Configuration . . . 135
7.5 About Novell Identity Translator (NIT) . . . 136

8 Updating (Patching) an OES Server 139

8.1 Overview of Updating (Patching) . . . 139
8.1.1 The Patch Process Briefly Explained . . . 139
8.1.2 Update Options . . . 140
8.2 Supported OES Update Paths . . . 140
8.3 Preparing the Server for Updating . . . 141
8.4 Registering the Server in the Customer Center . . . 142
8.4.1 Prerequisites . . . 142
8.4.2 Registering the Server in the Customer Center Using the Command Line . . . 142
8.4.3 Registering the Server in the Customer Center Using the GUI . . . 143
8.5 Updating the Server . . . 144
8.5.1 Updating the Server Using the Command Line . . . 145
8.6 GUI Based Patching . . . 148
8.7 Frequently Asked Questions about Updating . . . 149
8.7.1 Do I apply all the patches in the catalogs? How do I know which patches to apply? . . . 149
8.8 Patching From Behind a Proxy Server . . . 149
8.9 Using SUSE Manager to Patch an OES Server . . . 149
8.9.1 Setting Up SUSE Manager . . . 149
8.9.2 Patching an OES 2018 or Later Server Using SUSE Manager . . . 151
8.10 Using ZENworks Server to Patch an OES Server . . . 151
8.11 Installing the Latest iManager NPMs After Applying OES Patches . . . 151
8.12 Restarting the OES Instance of Tomcat After Applying a Tomcat Update . . . 152

9 Using AutoYaST to Install and Configure Multiple OES Servers 153

9.1 Prerequisites . . . 153
9.2 Setting Up a Control File with OES Components . . . 154
9.2.1 Using the AutoInstallation Module to Create the Control File . . . 154
9.3 Setting Up an Installation Source . . . 159
9.4 Cloning an OES Server Post OES Installation and Configuration . . . 159
9.4.1 Generating the autoinst.xml File . . . 159
9.4.2 Using the autoinst.xml to Install or Reinstall an OES Server . . . 160

10 Installing OES on a VM 163

10.1 System Requirements . . . 164
10.1.1 VM Host Considerations . . . 164
10.1.2 OES Storage Services Considerations . . . 164
10.1.3 Setup Instructions . . . 164
10.2 Prerequisites . . . 165
10.3 Preparing the Installation Software . . . 165

10.3.1 Downloading the Installation Software 165
10.3.2 Preparing the Installation Source Files 165
10.4 Installing an OES 24.4 VM Guest 165
10.4.1 Specifying Options for Creating an OES 24.4 VM Guest 165
10.5 Setting Up an OES VM Guest to Use Novell Storage Services (NSS) 167

11 Deploying OES in a UEFI Secure Boot Environment 169

12 Switching to SHA-2 SSL Certificates 173

12.1 Configuring SHA-2 Certificate 173
12.1.1 Prerequisites 173
12.1.2 CA Server 173
12.1.3 Other Servers 174
12.1.4 Servers Running on eDirectory 8.8.7 or OES 11 SP1 or Earlier 174
12.2 Verifying the Certificates with SHA-2 Signature 174

13 Disabling OES Services 175

14 Reconfiguring eDirectory and OES Services 177

14.1 Cleaning Up the eDirectory Server 177
14.1.1 Before You Clean Up 177
14.1.2 Reconfiguring the Replica Server 178
14.1.3 Reconfiguring the CA Server 178
14.1.4 Cleaning Up eDirectory 178
14.2 Reconfiguring the eDirectory Server through YaST 179
14.3 Reconfiguring OES Services 179
14.3.1 Re-creating eDirectory Objects 180
14.3.2 Services Requiring Reconfiguration 181
14.3.3 Manually Starting Services 182

15 Centralized Certificate Management 185

15.1 Installing Centralized Certificate Management Binaries 186
15.2 Upgrading OES Server 186
15.3 Path to Important Certificate Management Files 187
15.4 Usage of Commands 187
15.4.1 Listing of Certificates Used by OES Services 187
15.4.2 Configuration file 189
15.4.3 Reconfiguring Certificates 190
15.5 Examples 191
15.5.1 Example - Replacing Expired or Corrupted Certificate 191
15.5.2 Example - Replacing Expired or Corrupted Certificate of CIS Server 192
15.5.3 Example - Reconfiguring Services to Use 3rd party CA Signed Certificate 193
15.5.4 Example - Replacing Expired or Corrupted eDirectory Server Certificate 193
15.5.5 Example - Moving from Self-Signed Certificates to eDirectory Server Certificate On Upgrade 194

16 OES Multifactor Authentication Service 195

16.1 Overview 195

16.1.1 Quick Start - OES MFA Configuration . . . 195
16.2 MFA Server Architecture . . . 196
16.2.1 MFA Control Flow Diagram . . . 197
16.3 Preparing to Deploy an MFA Server . . . 197
16.4 Deployment Recommendation . . . 198
16.4.1 Number of MFA Servers . . . 198
16.4.2 MFA Agents . . . 198
16.5 Setting-Up an MFA Server . . . 198
16.6 Setting-Up Subsequent MFA Servers . . . 199
16.7 Configuring MFA Agent . . . 200
16.8 Configuring OES Services to Use MFA Service . . . 200
16.8.1 Configuring OES CIFS to Use MFA Service . . . 200
16.9 Allowlist to Exempt from MFA . . . 200
16.10 Command Line Utility of MFA Server . . . 200
16.10.1 Syntax . . . 201
16.10.2 MFA Server Commands and Options . . . 201
16.10.3 Examples . . . 204
16.11 Command Line Utility of MFA Agent . . . 204
16.11.1 Syntax . . . 205
16.11.2 MFA Agent Commands and Options . . . 205
16.12 Important Files and Folders . . . 206
16.13 Security Configurations . . . 206
16.13.1 mTLS between MFA Server and MFA Agent . . . 206
16.13.2 HTTPS Communication between Advanced Authentication Server, MFA Server, and Smartphone . . . 207
16.14 Troubleshooting . . . 207
16.14.1 “Unable to verify the first certificate” message in MFA server log . . . 207
16.14.2 “Unable to verify the first certificate” message in MFA agent log . . . 207
16.14.3 Unable to configure MFA server or MFA agents or unable to discover MFA servers . . . 207
16.14.4 Configuration changes done on one MFA server is not reflecting on the other MFA servers . . . 208
16.14.5 Unable to configure MFA server post Transfer ID migration of the UMC server . . . 208
16.14.6 Unable to configure MFA parameters with a value that begin with the character $ . . . 208

17 Security Considerations 209

17.1 SSRF through Host Header Injection . . . 209
17.2 Enforce Secure HTTPS Browser Connections with Apache . . . 210
17.3 Access to the Server During an Installation or Upgrade . . . 210
17.4 Remote Installations Through VNC . . . 210
17.5 Improperly Configured LDAP Servers . . . 211

18 Troubleshooting 213

18.1 Prompt for Untrusted GnuPG Key During Upgrade . . . 213
18.2 Upgrade Failure in SUSE Xen Hypervisor Environment . . . 213
18.3 PID File Unavailable Message . . . 214
18.4 `systemctl kill` Not Supported . . . 214
18.5 Executing kinit Command Fails in .LOCAL Domain . . . 214
18.6 The OES Service Pattern Icons are not Displayed and OES Patterns are not in the Proper Order . . . 214

18.7 Deleting the Existing eDirectory Objects when Reinstalling the OES Server or Reconfiguring the eDirectory . . . 215
18.8 Problem In Assigning IP Address For autoinst.xml-based Installations . . . 215
18.9 eDirectory Restart Results in an Error Message on a Non-DSfW Server . . . 215
18.10 The DEFAULT SLP Scope Gets added to the slp.conf File During an Upgrade to OES 2018 or later . . . 216
18.11 The change_proxy_pwd.sh Script Fails to Synchronize Password . . . 216
18.12 OES Installation Fails Due to Encrypted OES Media URL in the autoinst.xml File . . . 217
18.13 Installing or Upgrading to OES 24.4 using AutoYaST Creates the OES Repository Name Using Random Characters . . . 217
18.14 Verification of the Container Object Fails During the AD Domain Join Process . . . 218
18.15 Timing Issues for OES on Xen . . . 218

A OES File and Data Locations 219

A.1 General Rules . . . 219
A.2 Exceptions . . . 220

B AutoYaST XML Tags 221

B.1 edirectory . . . 221
B.2 imanager . . . 227
B.3 iprint . . . 228
B.4 ncpserver . . . 228
B.5 ncs . . . 228
B.6 novell-cifs . . . 230
B.7 novell-dhcp . . . 231
B.8 novell-dns . . . 232
B.9 novell-lum . . . 233
B.10 nss . . . 235
B.11 oes-ldap . . . 235
B.12 sms . . . 236
B.13 novell-nssad . . . 237
B.14 oes-umc . . . 238
B.15 oes-database . . . 238

About This Guide

This guide describes how to install Open Enterprise Server (OES) 24.4. Except where specifically stated, the content of this guide applies to installing OES on a computer's physical hardware rather than on a Xen virtual machine host server.

- Chapter 1, "What's New or Changed in OES Install," on page 13
- Chapter 2, "Preparing to Install OES," on page 17
- Chapter 3, "Installing OES as a New Installation," on page 39
- Chapter 4, "Installing or Configuring OES Services on an Existing OES Server," on page 87
- Chapter 5, "Upgrading OES," on page 91
- Chapter 6, "Completing OES Installation Tasks," on page 123
- Chapter 7, "Installing and Configuring NSS Active Directory Support," on page 127
- Chapter 8, "Updating (Patching) an OES Server," on page 139
- Chapter 9, "Using AutoYaST to Install and Configure Multiple OES Servers," on page 153
- Chapter 10, "Installing OES on a VM," on page 163
- Chapter 11, "Deploying OES in a UEFI Secure Boot Environment," on page 169
- Chapter 12, "Switching to SHA-2 SSL Certificates," on page 173
- Chapter 13, "Disabling OES Services," on page 175
- Chapter 14, "Reconfiguring eDirectory and OES Services," on page 177
- Chapter 15, "Centralized Certificate Management," on page 185
- Chapter 16, "OES Multifactor Authentication Service," on page 195
- Chapter 17, "Security Considerations," on page 209
- Chapter 18, "Troubleshooting," on page 213
- Appendix A, "OES File and Data Locations," on page 219
- Appendix B, "AutoYaST XML Tags," on page 221

Audience

This guide is intended for system administrators.

Feedback

We want to hear your comments and suggestions about this guide and the other documentation included with OES. Please use **comment on this topic** at the bottom of each the page of the online documentation.

Documentation Updates

The latest version of the *OES Installation Guide* is available at the Open Enterprise Server 24.4 documentation website (https://www.microfocus.com/documentation/open-enterprise-server/24.4/).

Additional Documentation

For more information about	See
Planning and implementing OES	*Planning and Implementation Guide*
Migration from and coexistence with other products	"Different Migration Tools" in the *Migration Tool Administration Guide*
SLES 15 SP4 Deployment details	*SUSE LINUX Enterprise Server 15 SP4 Deployment* Guide
SLES 15 SP4 Administration details	SUSE LINUX Enterprise Server 15 SP4 Administration Guide

1 What's New or Changed in OES Install

This section describes enhancements and changes in Open Enterprise Server (OES) Installation Guide.

- Section 1.1, "What's New or Changed in OES 25.3," on page 13
- Section 1.2, "What's New or Changed in OES 25.2," on page 13
- Section 1.3, "What's New or Changed in OES 25.1," on page 13
- Section 1.4, "What's New or Changed in OES 24.4.1," on page 14
- Section 1.5, "What's New or Changed in OES 24.4," on page 14

1.1 What's New or Changed in OES 25.3

OES 25.3 is an update that includes enhancements, improves usability, and defect fixes.

For support matrix changes, see Supported OES Upgrade Paths and Supported OES Update Paths.

1.2 What's New or Changed in OES 25.2

1.2.1 Identity Console

This release supports Identity Console version 1.9.

1.2.2 SUSE Manager

This release supports SUSE Manager version 5.0.

For support matrix changes, see Supported OES Upgrade Paths and Supported OES Update Paths.

1.3 What's New or Changed in OES 25.1

1.3.1 Allowlist to Exempt from MFA

Use allowlist to exempt eDirectory or Active Directory users, eDirectory or Active Directory groups, IP address of CIFS client workstation, IP address range of CIFS client workstations, or subnet of CIFS client workstations from multifactor authentication in OES MFA server.

For more information, see Allowlist to Exempt from MFA.

1.3.2 SSRF through Host Header Injection

Restrict unauthorized access that can manipulate server-side requests to redirect traffic, bypass access controls, or exploit server behavior.

For more information, see Security Considerations.

1.3.3 SUSE Manager Support

Open Enterprise Server supports upgrade and patching using SUSE manager version 4.3.15 or later. For more information, see Upgrading Open Enterprise Server Using SUSE Manager and Using SUSE Manager to Patch an OES Server.

1.3.4 ZENworks Support

Open Enterprise Server supports upgrade and patching using ZENworks 24.4 server. For more information, see Using ZENworks to Upgrade from OES 23.4 to OES 24.4 or later and Using ZENworks Server to Patch an OES Server.

1.4 What's New or Changed in OES 24.4.1

OES 24.4.1 is an update that includes enhancements, improves usability, and defect fixes.

1.5 What's New or Changed in OES 24.4

1.5.1 OES MFA on CIFS Service

OES CIFS can be configured to use an OES Multifactor Authentication (MFA) service to enforce multifactor authentication when users access the CIFS share. MFA service is supported on OES version 24.4 or later.

For more information, see OES Multifactor Authentication Service.

1.5.2 iPrint Advanced

OES iPrint Advanced and OES iPrint patterns are merged in this release. Thus, OES iPrint Advanced is available with OES iPrint capabilities.

1.5.3 OES Database

The database configuration of the OES services are separated as a new OES database pattern.

1.5.4 OES FTP 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.

1.5.5 Unified Management Console

Identity Console

Identity Console is bundled with UMC for identity management in OES. The packages are installed automatically during the UMC installation and no separate installation is required.

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

2 Preparing to Install OES

In preparation for the installation, perform the tasks and understand the information in the following sections:

- Section 2.1, “Before You Install,” on page 17
- Section 2.2, “Meeting All Server Software and Hardware Requirements,” on page 17
- Section 2.3, “OES eDirectory Rights Needed for Installing OES,” on page 19
- Section 2.4, “Installing and Configuring OES as a Subcontainer Administrator,” on page 19
- Section 2.5, “Preparing eDirectory for OES,” on page 23
- Section 2.6, “Deciding What Patterns to Install,” on page 25
- Section 2.7, “Obtaining OES Software,” on page 33
- Section 2.8, “Preparing Physical Media for a New Server Installation,” on page 33
- Section 2.9, “Setting Up a Network Installation Source,” on page 34
- Section 2.10, “Install Only One Server at a Time,” on page 37
- Section 2.11, “What's Next,” on page 37

2.1 Before You Install

Before you install Open Enterprise Server (OES), review the following information:

- ❒ “Planning Your OES Implementation” in the *Planning and Implementation Guide*
- ❒ *Release Notes*

2.2 Meeting All Server Software and Hardware Requirements

Before installing OES, ensure that your system meets the following requirements:

- Section 2.2.1, “Server Software,” on page 17
- Section 2.2.2, “Server Hardware,” on page 18

2.2.1 Server Software

As you install OES, do not change any of the Base Technologies package selections, such as Java support. Doing so can cause various problems, such as the installation failing or one or more OES services not working properly.

2.2.2 Server Hardware

Table 2-1 *Server Hardware Requirements*

System Component	Minimum Requirements	Recommended Requirements
Computer	Any server-class computer that runs with AMD64 or Intel* EM64T processors.	**IMPORTANT:** OES only runs on x86_64. Other processors that are supported by SLES 12 SP2 or later, such as Itanium (IA64) and Intel x86(IA32), are not supported for running OES services.
Memory	4 GB of RAM	4 GB of RAM for the base system. Additional RAM might be required depending on which OES components are selected and how they are used.
Free Disk Space	40 GB of available, unpartitioned disk space	40 GB of available, unpartitioned disk space. Additional disk space might be required, depending on which OES components are selected and how they are used.
DVD Drive	DVD drive if installing from physical media	DVD drive if installing from physical media
Network Board	Ethernet 100 Mbps	
IP address	One static IP address Subnet mask Default gateway	
Mouse	N/A	USB or PS/2
Server computer BIOS	Using a DVD installation source, prepare the BIOS on your server computer so that it boots from the DVD drive first.	
Video Card and Monitor	1024 X 768 resolution or higher with a minimum color depth of 8 bits (256 colors)	Although it is technically possible to run the ncurses installation at a lower resolution, some informational messages aren't displayed because text strings don't wrap to the constraints of the window.

NOTE: The RAM and disk space amounts shown here are for system components only. The OES service components that you install might require additional RAM and disk space. Refer to the SLES 15 SP4 Administration Guide (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-administration.html) for SUSE® Linux Enterprise Server operating system.

Be sure to complete the planning instructions in the *Planning and Implementation Guide* for each component that you install.

2.3 OES eDirectory Rights Needed for Installing OES

- Section 2.3.1, “Rights to Install the First OES Server in a Tree,” on page 19
- Section 2.3.2, “Rights to Install the First Three Servers in an eDirectory Tree,” on page 19
- Section 2.3.3, “Rights to Install the First Three Servers in any eDirectory Partition,” on page 19

2.3.1 Rights to Install the First OES Server in a Tree

To install an OES server in a tree, you must have rights to extend the schema, meaning that you need Supervisor rights to the root of the tree.

You can extend the schema by using the OES Schema Tool in YaST or by having a user with Supervisor rights to the root of the eDirectory tree install the first OES server and the first instance of each OES service that will be used into the tree. For more information, see Section 2.5.1, “Extending the Schema,” on page 23.

2.3.2 Rights to Install the First Three Servers in an eDirectory Tree

If you are installing the server into a new tree, the Admin user that is created during the OES installation has full rights to the root of the tree. Using the account for user Admin allows the installer to extend the eDirectory schema for OES as necessary. To install the first OES server in an eDirectory tree, you must have the Supervisor right at the root of the eDirectory tree.

2.3.3 Rights to Install the First Three Servers in any eDirectory Partition

By default, the first three servers installed in an eDirectory partition automatically receive a replica of that partition. To install a server into a partition that does not already contain three replica servers, the user must have either the Supervisor right at the root of the tree or the Supervisor right to the container in which the server holding the partition resides.

2.4 Installing and Configuring OES as a Subcontainer Administrator

---

IMPORTANT: The information explained in Section 2.3, “OES eDirectory Rights Needed for Installing OES,” on page 19 is prerequisite to the information contained in this section.

This section outlines the required eDirectory rights and explains how a subcontainer administrator approaches various installation tasks.

- Section 2.4.1, “Rights Required for Subcontainer Administrators,” on page 20
- Section 2.4.2, “Starting a New Installation as a Subcontainer Administrator,” on page 22
- Section 2.4.3, “Adding/Configuring OES Services as a Different Administrator,” on page 23

2.4.1 Rights Required for Subcontainer Administrators

For security reasons, you might want to create one or more subcontainer administrators (administrators that are in a container that is subordinate to the container that user Admin is in) with sufficient rights to install additional OES servers, without granting them full rights to the entire tree.

A subcontainer administrator needs the rights listed in Table 2-2 to install an OES server into the tree. These rights are typically granted by placing all administrative users in a Group or Role in eDirectory, and then assigning the rights to the Group or Role. Sample steps for assigning the rights to a single subcontainer administrator are provided as a general guide.

Table 2-2 *Subcontainer Administrator Rights Needed to Install*

Rights Needed	Sample Steps to Follow
Supervisor right to itself	1. In iManager, click **View Objects** > the **Browse** tab, then browse to and select the subcontainer administrator. 2. Click the administrator object, then select **Modify Trustees**. 3. Click the **Assigned Rights** link for the administrator object. 4. For the [All Attributes Rights] property, select **Supervisor**, then click **Done > OK**.
Supervisor right to the container where the server will be installed	1. Browse to the container where the subcontainer administrator will install the server. 2. Click the container object and select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] and [Entry rights] properties, select **Supervisor**, then click **Done > OK > OK**.
Supervisor right to the W0 object located inside the KAP object in the Security container	1. Browse to **Security > KAP**. 2. In KAP, click **W0** and select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] and [Entry rights] properties, select **Supervisor**, then click **Done > OK > OK**.
Supervisor right to the W1 object located inside the KAP object in the Security container	1. Browse to **Security > KAP**. 2. In KAP, click **W1** and select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. To know more about AES 256-bit tree key, refer to the Creating an AES 256-Bit Tree Key.

Rights Needed	Sample Steps to Follow
Supervisor right to the Security container when installing the NMAS login methods	If the subcontainer administrator will install the NMAS login methods: 1. Browse to and select **Security**. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] and [Entry rights] properties, select **Supervisor**, then click **Done > OK > OK**.
Create right to its own container (context)	1. Browse to and select the container where you created the subcontainer administrator. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [Entry Rights] property, select **Create**, then click **Done > OK > OK**.
Create right to the container where the UNIX Config object is located	1. Browse to and select the container where the UNIX Config object is located. By default, this is the Organization object. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [Entry Rights] property, select **Create**, then click **Done > OK > OK**.
Read right to the Security container object for the eDirectory tree	This is not needed if the Supervisor right was assigned because of NMAS. If the subcontainer administrator won't install the NMAS login methods, do the following: 1. Browse to and select **Security**. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] property, select **Read**, then click **Done > OK > OK**.

Rights Needed	Sample Steps to Follow
Read right to the NDSPKI:Private Key attribute on the Organizational CA object (located in the Security container)	1. Browse to **Security** and select the Organizational CA object. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. Click the **Add Property** button. 6. Select **NDSPKI:Private Key**, then click **OK**. The Read right should be automatically assigned. 7. Click **Done > OK > OK**.
Read and Write rights to the UNIX Config object	1. Browse to and select the UNIX Config object. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] property, select **Write** (**Read** is already selected), then click **Done > OK > OK**.
Write right to the [All Attribute Rights] property for the admingroup object	1. Browse to and select the admingroup object. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] property, select **Write** (**Compare and Read** are already selected), then click **Done > OK > OK**.

When you install DNS/DHCP into an existing tree with DNS/DHCP, see the following additional guidelines:

- For DNS, see "eDirectory Permissions " in the *DNS/DHCP Services for Linux Administration Guide*.
- For DHCP, see "eDirectory Permissions " in the *DNS/DHCP Services for Linux Administration Guide*.

2.4.2 Starting a New Installation as a Subcontainer Administrator

You can install a new OES server into an existing tree as a subcontainer administrator if you have the following:

- The rights described in "Rights Required for Subcontainer Administrators" on page 20
- (If applicable) The rights described for the server installations in "OES eDirectory Rights Needed for Installing OES" on page 19

When you reach the eDirectory Configuration - Existing Tree page, enter your fully distinguished name (FDN) and password. After verifying your credentials, the installation proceeds normally.

2.4.3 Adding/Configuring OES Services as a Different Administrator

To add or configure OES services on an OES server that another administrator installed, see "Adding/Configuring OES Services on a Server That Another Administrator Installed" on page 89.

2.5 Preparing eDirectory for OES

- Section 2.5.1, "Extending the Schema," on page 23

2.5.1 Extending the Schema

An eDirectory tree must have its schema extended to accommodate OES servers and services as explained in the following sections:

- "Who Can Extend the Schema?" on page 23
- "Which OES Services Require a Schema Extension?" on page 23
- "Extending the Schema While Installing OES" on page 24
- "Using the YaST Plug-In to Extend the Schema" on page 24
- "Extending the Schema for OES Cluster Services" on page 24

Who Can Extend the Schema?

Only an administrator with the Supervisor right at the root of an eDirectory tree can extend the tree's schema.

Which OES Services Require a Schema Extension?

The following service schema extensions are included with OES.

A single asterisk (*) indicates a service that is either required for OES servers or for the default services that are installed on every OES server.

Unmarked extensions are implemented the first time their respective services are installed, unless the schema was previously extended using another method, such as the YaST plug-in (see "Using the YaST Plug-In to Extend the Schema" on page 24).

- NetIQ Directory Services*
- OES Linux User Management (LUM)*
- OES iPrint Services
- OES DHCP Services
- OES DNS Services
- OES NCP Server
- OES Storage Services (NSS)
- OES SMS*
- OES Domain Services for Windows
- NetIQ NMAS*

- OES CIFS
- OES Clustering
- OES Remote Manager
- Cloud Integrated Storage (CIS)

Extending the Schema While Installing OES

The simplest way to extend the schema for OES servers is to have a tree admin install the first OES server and the first instance of each OES service that you plan to run on your network.

After this initial installation, you can assign subcontainer admins with the required rights to install additional servers and services. For more information on the required rights for the various OES services, see "Rights Required for Subcontainer Administrators" on page 20.

Using the YaST Plug-In to Extend the Schema

If you want a subcontainer admin to install the first OES server or the first instance of an OES service in an existing tree, and you don't want to grant that admin the Supervisor right to the root of the tree, someone with the Supervisor right to root can extend the schema by using YaST from any of the following locations:

- An OES server running in another tree
- Install a fully patched OES without installing any of the services, followed by the `yast novell-schematool` installation.

To run the OES Schema Tool:

1. On the server's desktop, click **Computer** and open the **YaST Control Center**.
2. Click **Open Enterprise Server > OES Schema Tool**.
3. Depending on the installation method you used, you might be required to insert your OES installation media.
4. On the OES eDirectory Extension Utility page, specify the information for an eDirectory server with a Read/Write replica of the Root partition.

   Be sure to provide the correct information to authenticate as an admin user with the Supervisor right at the root of the target tree. Otherwise, the schema extension fails.
5. Select all of the other services you plan to run on any of the OES servers in the tree.
6. Click **Next**.

   The schema is extended.

   The YaST2 novell-schematool utility writes the schema event messages to the `/var/opt/novell/eDirectory/log/oes_schema.log` file on the server where the utility is running.

Extending the Schema for OES Cluster Services

If you want a subcontainer administrator to install the first instance of OES Cluster Services in a tree, you can extend the schema by following the instructions in "Installing, Configuring, and Repairing OES Cluster Services" in the *OES Cluster Services for Linux Administration Guide*.

2.6 Deciding What Patterns to Install

A default OES installation has the following base technology, graphical environment, and primary function patterns selected for installation.

Table 2-3 *Standard OES Installation Patterns*

Pattern	Description
Minimal Base System	The minimal base system is the base runtime system. Additional packages and patterns need to be added to make this pattern useful for running physical hardware that contains only a minimal multiuser boosting system.
Enhanced Base System	Enhanced base system is the enhanced base runtime system with lots of convenience packages.
AppArmor	AppArmor is an open source Linux application security framework that provides mandatory access control for programs, protecting against the exploitation of software flaws and compromised systems. AppArmor includes everything you need to provide effective containment for programs (including those that run as `root`) to thwart attempted exploits and even zero-day attacks. AppArmor offers an advanced tool set that largely automates the development of per-program application security so that no new expertise is required. This pattern is selected for installation by default.
GNOME Desktop Environment	The GNOME desktop environment is an intuitive and attractive desktop for users. The GNOME development platform is an extensive framework for building applications that integrate into the rest of the desktop. This pattern is selected for installation by default.
X Window System	In continuous use for over 20 years, the X Window System provides the only standard platform-independent networked graphical window system bridging the heterogeneous platforms in today's enterprise: from network servers to desktops, thin clients, laptops, and handhelds, independent of operating system and hardware. This pattern is selected for installation by default.

Table 2-4 *OES Services Pattern Descriptions*

Pattern	Description
OES Backup/Storage Management Services (SMS)	The OES backup infrastructure (called Storage Management Services or SMS) provides backup applications with the framework to develop a complete backup and restore solution. SMS helps back up file systems (such as NSS) or application data (such as data from GroupWise) on NetWare and SUSE Linux Enterprise Server (SLES) to removable tape media or other media for off-site storage. It provides a single consistent interface for all file systems and applications across NetWare and SLES. This pattern selects and installs these services: ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
OES Business Continuity Cluster (BCC)	OES Business Continuity Cluster protects your key business systems against downtime and disaster. Built on OES Cluster Services and Open Enterprise Server, Business Continuity Cluster is the only product on the market that automates the configuration and management of a high-availability clustered-server solution. This pattern selects and installs these services: ◆ OES Backup / Storage Management Services (SMS) ◆ OES Cluster Services (NCS) ◆ OES eDirectory ◆ OES Remote Manager (NRM) ◆ OES Linux User Management (LUM)
OES CIFS	CIFS (Common Internet File System) is a network sharing protocol. OES CIFS enables Windows, Linux, and UNIX client workstations to copy, delete, move, save, and open files on an OES server. CIFS allows read and write access from multiple client systems simultaneously. This pattern selects and installs these services: ◆ OES Backup / Storage Management Services (SMS) ◆ OES eDirectory ◆ OES Storage Services (NSS) ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM) ◆ OES NCP Server This pattern cannot be installed on the same server as these services: ◆ OES Domain Services for Windows

Pattern	Description
Cloud Integrated Storage (CIS)	Cloud Integrated Storage is a hybrid cloud solution that provides a secure gateway to store, manage, and access data across private or public cloud. This pattern selects and installs the following services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES eDirectory ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
OES Cluster Services (NCS)	OES Cluster Services is a server clustering system that ensures high availability and manageability of critical network resources including data, applications, and services. It is a multinode clustering product for Linux that is enabled for OES eDirectory and supports failover, failback, and migration (load balancing) of individually managed cluster resources. OES Cluster Services lets you add Linux nodes to an existing NetWare 6.5 cluster without bringing down the cluster, or it lets you create an all-Linux cluster. With a mixed cluster, you can migrate services between OS kernels, and if services are alike on both platforms (such as NSS), you can set the services to fail over across platforms. Using OES Cluster Services with iSCSI technologies included in OES, you can build inexpensive clustered SANs on commodity gigabit Ethernet hardware. You can leverage existing hardware into a high availability solution supporting Linux and NetWare clusters. This pattern selects and installs these services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM) This pattern cannot be installed on the same server with these services: ◆ High Availability
OES Database	OES Database enables you to configure PostgreSQL database on local or remote server for OES services such as Unified Management Console (UMC). This pattern allows you to select either one of the database: ◆ Local database ◆ Remote database

Pattern	Description
OES DHCP	OES DHCP (Dynamic Host Configuration Protocol) uses eDirectory to provide configuration parameters to client computers and integrate them into a network. The eDirectory integration lets you have centralized administration and management of DHCP servers across the enterprise and lets you set up DHCP subnet replication via OES eDirectory. This pattern selects and installs these services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES eDirectory ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
OES DNS	OES DNS uses OES eDirectory to deliver information associated with domain names, in particular the IP address. This eDirectory integration lets you have centralized administration and management of DNS servers across the enterprise and lets you set up a DNS zone via OES eDirectory. This pattern selects and installs these services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES eDirectory ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
OES Domain Services for Windows	OES Domain Services for Windows provides seamless cross-authentication capabilities between Windows/Active Directory and OES servers. It is a suite of integrated technologies that removes the need for the Client for Open Enterprise Server when logging on and accessing data from Windows workstations in eDirectory trees. This technology simplifies the management of users and workstations in mixed OES-Microsoft environments. This pattern selects and installs these services: ◆ OES Backup / Storage Management Services (SMS) ◆ OES eDirectory ◆ OES DNS ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ OES CIFS ◆ OES FTP ◆ OES Pre-Migration Server

Pattern	Description
OES eDirectory	OES eDirectory services are the foundation for the world's largest identity management, high-end directory service that allows businesses to manage identities and security access for employees, customers, and partners. More than just an LDAP data store, eDirectory is the identity foundation for managing the relationships that link your users and their access rights with corporate resources, devices, and security policies. This pattern selects and installs these services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ OpenLDAP
OES FTP	OES FTP (File Transfer Protocol) is integrated with OES eDirectory so that users can securely transfer files to and from OES volumes. This pattern selects and installs these services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES eDirectory ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ OES Domain Services for Windows
OES iManager	OES iManager is a Web-based administration console that provides secure, customized access to network administration utilities and content from virtually anywhere you have access to the Internet and a Web browser. iManager provides the following benefits: ◆ Single point of administration for OES eDirectory objects, schema, partitions, and replicas ◆ Single point of administration for many other network resources ◆ Management of many Novell products by using iManager plug-ins ◆ Role-Based Services (RBS) for delegated administration This pattern selects and installs these services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)

Pattern	Description
OES iPrint Advanced	OES iPrint Advanced edition offers a single, scalable solution for managing printing across multiple office locations. You can print from desktops, smartphones, Chromebooks, tablets, or email-enabled devices. Previously, two patterns were available: OES iPrint and OES iPrint Advanced. Both patterns are merged and OES iPrint Advanced is available along with OES iPrint capabilities. The CUPS service runs on port 3017. This service selects and installs these services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES eDirectory, OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
OES Linux User Management (LUM)	OES User Management (LUM) enables eDirectory users to function as local POSIX users on Linux servers. This functionality lets administrators use eDirectory to centrally manage remote users for access to one or more OES servers. This pattern selects and installs these services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES Remote Manager (NRM)
OES MFA Server (MFA)	OES MFA Server provides multi-factor authentication for OES services. It facilitates the OES services in performing multi-factor authentication for the users by configuring a centralized MFA server. This MFA server can run on any OES server within an eDirectory tree and utilize Advanced Authentication as an authentication server. For high availability, multiple OES MFA servers can be configured in an eDirectory tree.
OES NCP Server / Dynamic Storage Technology	OES 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 be seamlessly transitioned to file services on OES. NCP Server includes OES Dynamic Storage Technology, which allows seldom-accessed files on NSS volumes to be automatically moved, according to policies set by the administrator, from faster-access storage to lower-cost storage media where the files can be more easily managed and backed up. Services included with NCP (NetWare Core Protocol) are file access, file locking, security, tracking of resource allocation, event notification, synchronization with other servers, connection and communication, print services and queue management, and network management. This pattern selects and installs these services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES eDirectory ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)

Pattern	Description
OES Pre-migration Server	A OES Pre-migration Server is not actually a service. Rather, it is a special-purpose server—the target of a Server ID Transfer Migration. Selecting this option causes this server to be installed without an eDirectory replica, thus preparing it to assume the identity of another server that you plan to decommission. For more information, see the *Migration Tool Administration Guide*. You should also select and install all the services that you plan to migrate from the other server. Services that are not installed on this server prior to the migration cannot be migrated. This pattern selects and installs these services: ◆ OES Backup / Storage Management Services (SMS) ◆ OES eDirectory (without a replica) ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ OES Domain Services for Windows
OES Remote Manager (NRM)	OES Remote Manager lets you securely access and manage one or more servers from any location through a standard Web browser. You can use OES Remote Manager to monitor your server's health, change the configuration of your server, or perform diagnostic and debugging tasks. This pattern selects and installs these services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES Linux User Management (LUM)

Pattern	Description
OES Storage Services (NSS)	The OES Storage Services (NSS) file system provides many unique and powerful file system capabilities. It is especially suited for managing file services for thousands of users in an organization. It also includes OES Distributed File Services for NSS volumes. Unique features include visibility, trustee access control model, multiple simultaneous namespace support, native Unicode, user and directory quotas, rich file attributes, multiple data stream support, event file lists, and a file salvage subsystem. NSS volumes are cross-compatible between kernels. You can mount a non-encrypted NSS data volume on either the Linux or NetWare kernel and move it between them. In a clustered SAN, volumes can fail over between kernels, allowing for full data and file system feature preservation when migrating data to Linux. This pattern selects and installs these services: ◆ OES Backup/Storage Management Services (SMS) ◆ OES eDirectory ◆ OES NCP Server ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ Xen Virtual Machine Host Server
OES Storage Service AD Support	Beginning with OES 2015, you can join the OES server to an Active Directory domain to provide seamless access to the Active Directory identities on the NSS resources. Thereby, the Active Directory users can natively access the NSS resources, administer them, and provision rights and quotas for Active Directory trustees. This solution is termed as OES Storage Services Active Directory (NSS AD) Support. This pattern selects and installs the following services: ◆ OES CIFS ◆ OES Storage Services (NSS) ◆ OES Backup/Storage Management Services (SMS) ◆ OES eDirectory ◆ OES NCP Server ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ OES Domain Services for Windows

Pattern	Description
OES Unified Management Console (UMC)	UMC is a highly responsive, simple, and secure web-based management console for managing small and large deployments for all OES services. Administrators can access utilities and content from anywhere using the Internet and a Web browser. For more information, see Unified Management Console Administration Guide. Identity Console is bundled with UMC for identity management in OES. The packages are installed automatically during the UMC installation. For more information, see Identity Console documentation. This pattern selects and installs the following services: ◆ OES eDirectory ◆ OES Database

If you want to install these services, you can select them to install with most other patterns during the initial server installation by customizing the installation or you can install them after installing your initial Open Enterprise Server. For more information, see "Customizing the Software Selections" on page 49 and "Installing or Configuring OES Services on an Existing OES Server" on page 87.

2.7 Obtaining OES Software

For information on obtaining OES software, see "Getting and Preparing OES Software" in the *Planning and Implementation Guide*.

2.8 Preparing Physical Media for a New Server Installation

To prepare physical media for an installation you must first download ISO image files and then write the ISO data to the bootable media that you need for your server. Detailed download instructions are available in "Getting and Preparing OES Software" in the *Planning and Implementation Guide*.

NOTE: The size of the ISO image file exceeds the maximum capacity of a dual-layer DVD. Therefore, you can boot it from a USB device.

Table 2-5 *Files to Download*

Platform	File needed
64-bit server with USB port	◆ OES ISO (`OES24.4-DVD-x86_64-DVD1.iso`)

1. Download the ISO file from Software Licenses and Downloads (SLD).
2. Ensure that the checksum of the file you have downloaded is the same as specified on the download page. To get the checksum, use the `md5sum <file name>` command.
3. Insert the USB device into the system.

4 Launch the terminal and go to the logged-in user's Downloads directory (or default download location).

```
hostname:~ # cd ~/Downloads
```

5 Ensure that the USB device is attached and is recognized by the system. The SIZE column in the `lsbk` output is the best indicator.

```
hostname:~/Downloads # lsblk
```

6 Run the following dd command to write the ISO data to the USB device. For example, if `sdb` is the USB device identified with `lsblk` then the command is:

```
hostname:~/Downloads # dd if=OES24.4-DVD-x86_64-DVD1.iso of=/dev/sdb
bs=4k
```

(Use `sudo` with `dd` if you are not logged-in as the root user)

This process takes several minutes as `dd` reads the data from an input file and writes it to an output file block by block.

7 Before removing the device from the USB port, ensure that all cached writes to the device are flushed out to the disk using the `sync` command.

```
hostname:~/Downloads # sync
```

8 When the sync is complete, the data from the ISO image is fully copied to the USB device and the device is bootable. The new installation device can be safely unplugged from the system.

2.9 Setting Up a Network Installation Source

The YaST install lets you use installation sources files that are hosted on the network to install a new server or upgrade an existing server. The following sections describe how to set up a network installation source server on the following platforms:

- Section 2.9.1, “SUSE Linux as a Network Installation Source Server,” on page 34
- Section 2.9.2, “Windows as a Network Installation Source Server,” on page 37

2.9.1 SUSE Linux as a Network Installation Source Server

To prepare a network installation source on a SUSE Linux server, see:

- “Setting Up the Server Holding the Installation Sources” (https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-deployment-instserver.html) in the *SLES 15 SP4 Deployment Guide* (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-deployment.html)
- The instructions in the following sections:
  - “Requirements” on page 35
  - “Procedure” on page 35
  - “NFS Protocol Configuration” on page 35
  - “FTP Protocol Configuration” on page 36
  - “HTTP Protocol Configuration” on page 36

Requirements

To set up a network installation source, you need the following:

- ❒ A YaST Network Installation source server.

  This source server can be SLES 9 or later, OES 2 or later, or Windows.

- ❒ An active network connection between the installation source server and the OES server you are installing or upgrading.

Procedure

1. Download or copy the ISO image files to a directory of your choice. See "Getting and Preparing OES Software" in the *Planning and Implementation Guide*.
2. Configure your Linux server to be a YaST installation server and select the location for the root of the network installation.

   The three protocol options to choose from for configuring the YaST installation server are NFS, FTP, and HTTP. For the protocol configuration procedures, see the following:

   - "NFS Protocol Configuration" on page 35
   - "FTP Protocol Configuration" on page 36
   - "HTTP Protocol Configuration" on page 36

   FTP and HTTP do not allow you to serve the files without possible modifications to `.conf` files. NFS is the simplest protocol to configure and is recommended.
3. Create a boot DVD using the `.iso` image file for *Open Enterprise Server 24.4 DVD* and label it with that name.

   For information on creating this DVD, see "Preparing Physical Media for a New Server Installation" on page 33.

   This DVD will be the network installation boot DVD.

With these steps completed, you are ready to perform a new installation or upgrade using a network installation source. See "Starting the OES Installation" on page 40.

NFS Protocol Configuration

An NFS share can be shared easily from almost any location on your file system. Use the following procedure if you choose to use this protocol:

1. At your network installation server, launch YaST.
2. Select **Network Services**, then click **NFS Server**.

   You might be prompted to install the NFS server.
3. On the NFS Server configuration screen, select **Start** in the NFS Server section, select **Open Port in Firewall** in the Firewall section, then click **Next**.
4. In the Directories section, click **Add Directory** and specify or browse to the directory where you have created the install root (source directory), then click **OK**.
5. Accept the defaults in the pop-up window for adding a Host.

If you are experienced with NFS configurations, you can customize the configuration.

6 Click **Finish**.

FTP Protocol Configuration

These instructions use Pure-FTPd and can be implemented through YaST. Depending on the FTP server you use, the configuration might be different.

If you have created your install root (source directory) within your FTP root, you can forego the following procedure and simply start Pure-FTPd.

The default configuration of Pure-FTPd runs in chroot jail, so symlinks cannot be followed. In order to allow FTP access to the install root created outside of the FTP root, you must mount the install root directory inside of the FTP root.

Complete the following if you have not created your install root within your FTP root and you choose to use this protocol:

1 Create a directory inside of your FTP root.

2 Run the following command:

```
mount --bind /path_to_install_root /path_to_directory_in_ftp_root
```

For example,

```
mount --bind /tmp/OES /srv/ftp/OES
```

3 (Optional) If you want to make this install root permanent, add this command to the `/etc/fstab` file.

4 Start Pure-FTPd.

HTTP Protocol Configuration

These instructions use Apache2 as provided by SLES 15 SP4.

If you choose to use this protocol:

1 Modify the `default-server.conf` file of your HTTP server to allow it to follow symlinks and create directory indexes.

The `default-server.conf` file is located in the `/etc/apache2` directory. In the `Directory` tag of the `default-server.conf` file, remove `None` if it is there, add `FollowSymLinks` and `Indexes` to the `Options` directive, then save the changes.

2 (Conditional) If the install root is outside of the HTTP root, create a symbolic link to the install root with the following command:

```
ln -s /path_to_install_root /path_to_link
```

For example,

```
ln -s /tmp/OES /srv/www/htdocs/OES
```

3 Restart Apache.

2.9.2 Windows as a Network Installation Source Server

To prepare a network installation source on a Windows server, see "Using a Microsoft Windows Workstation" in the *SLES 15 SP4 Deployment Guide*.

2.10 Install Only One Server at a Time

You should install one server at a time into a tree. Then wait for the installation program to complete before installing an additional server into the same tree.

2.11 What's Next

Proceed to one of the following sections, depending on the task that you want to perform:

- "Installing OES as a New Installation" on page 39
- "Using AutoYaST to Install and Configure Multiple OES Servers" on page 153
- "Installing OES on a VM" on page 163
- "Installing or Configuring OES Services on an Existing OES Server" on page 87

3 Installing OES as a New Installation

The Open Enterprise Server (OES) is installed using the OES Install Media iso (`OES24.4-DVD-x86_64-DVD1.iso`). This ISO has both OES and SLES. When you use this ISO, you are not required to select OES as an add-on product in the Installation Mode screen. This section provides information on the installation of OES.

For detailed information on performing a SLES installation, see the *SLES 15 SP4 Deployment Guide (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-deployment.html)*.

This section does not provide step-by-step installation instructions because the installation interface is mostly self-explanatory. It does, however, provide information about important steps in the process that might require additional explanation.

- Section 3.1, “Linux Software RAIDs Are Not Cluster Aware,” on page 39
- Section 3.2, “Linux Software RAIDs,” on page 40
- Section 3.3, “Starting the OES Installation,” on page 40
- Section 3.4, “Specifying Network Settings,” on page 42
- Section 3.5, “Specifying Customer Center Configuration Settings,” on page 42
- Section 3.6, “Specifying the Add-On Product Installation Information,” on page 43
- Section 3.7, “System Role in OES 24.4,” on page 44
- Section 3.8, “Setting Up Disk Partitions,” on page 45
- Section 3.9, “Setting Up the Clock and Time Zone,” on page 48
- Section 3.10, “Creating Local User,” on page 48
- Section 3.11, “Authentication for the System Administrator “root”,” on page 49
- Section 3.12, “Specifying the Installation Settings,” on page 49
- Section 3.13, “Configuring Open Enterprise Server,” on page 54
- Section 3.14, “Product Improvement,” on page 83
- Section 3.15, “Finishing the Installation,” on page 84
- Section 3.16, “Verifying that the Installation was Successful,” on page 84
- Section 3.17, “What's Next,” on page 86

3.1 Linux Software RAIDs Are Not Cluster Aware

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

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

3.2 Linux Software RAIDs

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

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

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

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

3.3 Starting the OES Installation

1. Insert the OES Install Media that you created into the DVD drive of the computer that you want to be your OES server.
2. Boot the machine.
3. Continue with one of the following procedures:

- Section 3.3.1, “Installing from Physical Media,” on page 40
- Section 3.3.2, “Installing from a Network Source,” on page 41

3.3.1 Installing from Physical Media

1. From the DVD boot menu, select **Installation**, then press Enter.

   For installation in text mode, from the DVD boot menu, select **Installation**, press F3, select **Text Mode**, then press Enter.

   NOTE: If you install in text mode, ensure to set the systemd target to Text mode on the Installation Settings page later in the installation procedure.

   ---

2. Select the language that you want to use, read and accept the license agreement, then click **Next**.
3. Follow the prompts, using the information contained in the following sections:
   - **3a** “Specifying Network Settings” on page 42.
   - **3b** “Specifying Customer Center Configuration Settings” on page 42
   - **3c** “Specifying the Add-On Product Installation Information” on page 43.
   - **3d** “System Role in OES 24.4” on page 44
   - **3e** “Setting Up Disk Partitions” on page 45
   - **3f** “Setting Up the Clock and Time Zone” on page 48.

3g "Creating Local User" on page 48

3h "Authentication for the System Administrator "root"" on page 49

3i "Specifying the Installation Settings" on page 49.

3j "Configuring Open Enterprise Server" on page 54

3k "Finishing the Installation" on page 84.

4 Complete the server setup by following the procedures in "Completing OES Installation Tasks" on page 123.

3.3.2 Installing from a Network Source

1 From the DVD boot menu, select **Installation**, press F4, select **Network Config** > **Manual**.

2 In the Manual Network Config dialog box, provide the network details and click **OK**.

NOTE: If you are performing network configuration in boot parameters, ensure to set an additional parameter `sethostname=0` to avoid unnecessary prompts in YaST modules.

---

3 Press F4 again, then select the network installation type (SLP, FTP, HTTP, NFS, SMB/CIFS) that you set up on your network installation server.

See Step 2 on page 35 of the SUSE Linux as a Network Installation Source Server procedure.

4 Specify the required information (server name and installation path), then select **OK**.

5 Press Enter to begin the installation.

6 Select the language that you want to use, read and accept the license agreement, then click **Next**

7 Follow the screen prompts, referring to the information in the following sections as needed (remember that not all required selections are documented):

NOTE: Ensure that the network settings are correct before continuing with the installation.

If you want to specify the network settings, click **Network Configuration** on the Registration page.

7a "Specifying Customer Center Configuration Settings" on page 42

7b "Specifying the Add-On Product Installation Information" on page 43.

7c "System Role in OES 24.4" on page 44

7d "Setting Up Disk Partitions" on page 45

7e "Setting Up the Clock and Time Zone" on page 48.

7f "Creating Local User" on page 48

7g "Authentication for the System Administrator "root"" on page 49

7h "Specifying the Installation Settings" on page 49.

7i "Configuring Open Enterprise Server" on page 54

7j "Finishing the Installation" on page 84.

8 Complete the server setup by following the procedures in "Completing OES Installation Tasks" on page 123.

3.4 Specifying Network Settings

Configuration success is directly tied to specific networking configuration requirements. Ensure that the settings covered in the steps that follow are configured exactly as specified.

NOTE: If DHCP is configured in your network, Network Settings page is not displayed. In such case, to configure the Static IP, click **Network Configuration...** button on the top right corner of the Customer Center Configuration page.

Specify the setting for each network board on the server:

1. On the **Overview** tab of Network Settings page, select the network card you want to configure, then click **Edit**.
2. Select **Statically Assigned IP Address**, then specify the **IP Address** and the **Subnet Mask** for the interface. Specify the **Hostname** in the FQDN format associated with the static IP Address.

   OES requires a static IP address.
3. Click the **Hostname/DNS** tab.

   Specify the **Hostname** for this computer (example:) associated with the IP address you have or will assign to the server. The name is stored in `/etc/hostname`.
4. In the **Name Servers and Domain Search List**, specify from one to three DNS server IP addresses.
5. Click the **Routing** tab.
6. Click **Add**, and specify the IP address of the default gateway on the subnet where you are installing the OES server.
7. Click **Next**.
8. Continue with Section 3.5, “Specifying Customer Center Configuration Settings,” on page 42.

3.5 Specifying Customer Center Configuration Settings

Registering to Customer Center enables you to receive updates on OES, which includes defect fixes.

When you are entering the Customer Center configuration information, it is critical that you enter either your purchased OES code or the 60-day evaluation code available with your OES download.

1. Select **Configure Now** to download any updates that are available for the server, then click **Next**.
2. On the Customer Center Configuration page, select all of the following options:

Option	What it Does
Configure Now	Proceeds with registering this server and OES product in the Customer center.
Hardware Profile	Sends the information to the Customer Center about the hardware that you are installing OES on.
Optional Information	Sends optional information to the Customer Center for your registration. For this release, this option doesn’t send any additional information.
Registration Code	Makes the registration with activation codes mandatory.

Option	What it Does
Regularly Synchronize with the Customer Center	Keeps the installation sources for this server valid. It does not remove any installation sources that were manually added.

3 Click **Advanced** > **Local Registration Server**, specify the name of the SMT server plus the path to the registration internals (`/center/regsvc/`).

The URL needs to be in the following format: `https://FQDN/center/regsvc/` with FQDN being the fully qualified hostname of the SMT server. It must be identical to the FQDN of the server certificate used on the SMT server.

4 Click **OK** to continue on the Customer Center Configuration page.

5 After you click **Next**, the Contacting server message is displayed.

Wait until this message disappears and the Manual Interaction Required page displays.

6 On the Manual Interaction Required page, note the information that you will be required to specify, then click **Continue**.

7 On the Customer Center Registration page, specify the required information in the following fields, then click **Submit**:

Field	Information to Specify
Email Address	The email address for your Login account.
Confirm Email Address	The same email address for your Login account
Open Enterprise Server 24.4 (optional)	Specify your purchased or 60-day evaluation registration code for the OES 24.4 product. If you don't specify a code, the server cannot receive any updates or patches.
System Name or Description (optional):	Specify a description to identify this server.

8 When the message to complete the registration displays, click **Continue**.

9 After you click **Continue**, the `Contacting server..` message is displayed with the Manual Interaction Required screen.

Wait until this message disappears and the Customer Center Configuration page displays.

10 Continue with Section 3.6, "Specifying the Add-On Product Installation Information," on page 43.

3.6 Specifying the Add-On Product Installation Information

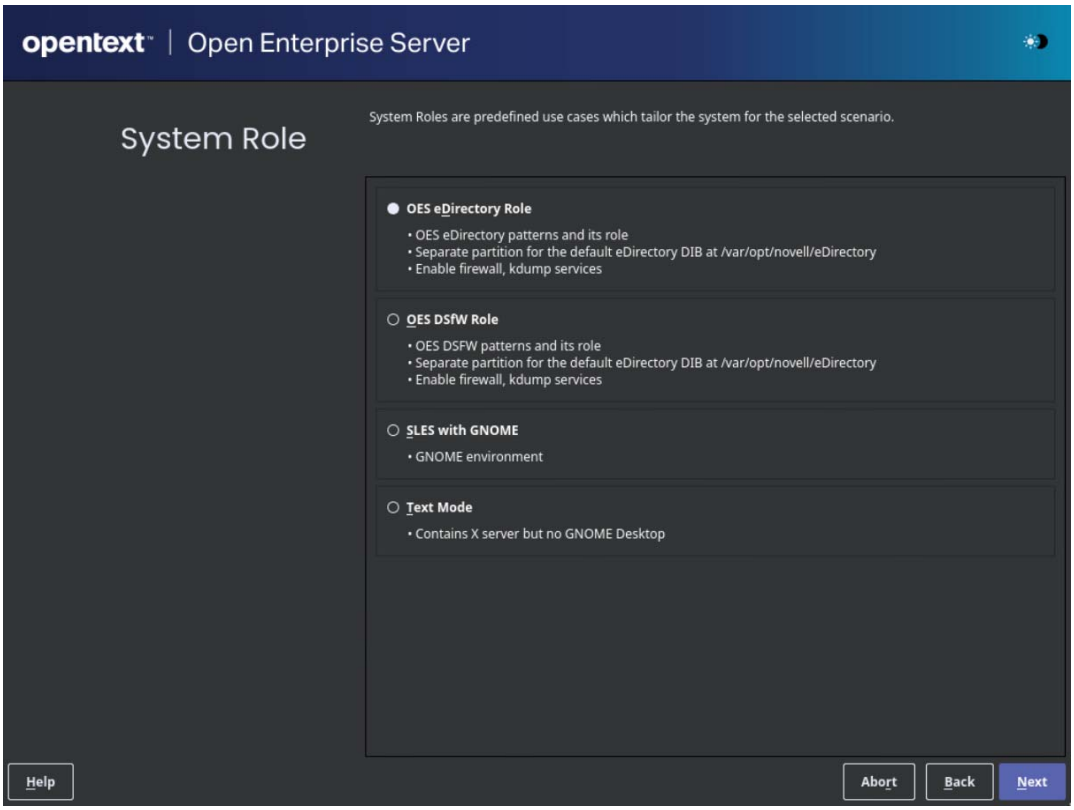
On the Add-On Product Installation page, you can add the add-on products you want that are supported on OES 24.4.

If you do not want to add any add-on products with OES, click **Next** to continue with Section 3.7, "System Role in OES 24.4," on page 44

3.7 System Role in OES 24.4

The OES installer offers predefined use cases which allow installation as per your requirements.

3.7.1 OES System Roles



In OES, the following system roles are available:

OES eDirectory Role

Select this role to install all the basic packages, eDirectory pattern along with the minimal OES specific patterns. Additionally, LUM, NRM, and SMS with eDirectory will be installed.

OES DSfW Role

Select this role to install basic packages, OES Domain Services for Windows along with OES specific patterns. Additionally, LUM, NRM, SMS, eDirectory along with DSfW will be installed.

SLES with GNOME

Select this role to install all the basic packages in the GNOME Desktop Environment. Any OES specific patterns will not be installed.

Text Mode

Select this role to install a basic SLES without a desktop environment. It contains a rich set of command-line tools.

NOTE: Select any OES pattern from the Installation Settings page, or run yast2 oes-install and select the required pattern after the installation.

3.8 Setting Up Disk Partitions

In most cases, YaST proposes a reasonable partitioning scheme that can be accepted without change. You can also use YaST to customize the partitioning.

OES 24.4 supports both btrfs and xfs file systems by default.

Volume / or root with btrfs file system.

Volume /var/opt/novell/eDirectory with xfs file system.

By selecting Expert Partitioner, customers can use any file system or partitioning scheme they like. The important thing is to create a separate volume for /var/opt/novell/eDirectory with the xfs file system with a minimum hard disk space of 1GB.

- Section 3.8.1, “Guidelines,” on page 45
- Section 3.8.2, “NSS on the System Disk,” on page 46
- Section 3.8.3, “Security Flag Recommendations,” on page 47
- Section 3.8.4, “Partitioning X86 Machines,” on page 47
- Section 3.8.5, “Disk Partition Statistics,” on page 48
- Section 3.8.6, “Combining Hard Disk Partitions,” on page 48

3.8.1 Guidelines

Table 3-1 presents guidelines for setting up disk partitions on your OES server. For more information, see “Installation Settings” in the *SLES 15 SP4 Deployment Guide* (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-deployment.html).

Table 3-1 *Partition Guidelines*

Partition to Create	Other Considerations
/boot	Depending on the hardware, it might be useful to create a boot partition (/boot) to hold the boot mechanism and the Linux kernel. You should create this partition at the start of the disk and make it at least 8 MB or 1 cylinder. As a rule of thumb, always create such a partition if it was included in the YaST original proposal. If you are unsure about this, create a boot partition to be on the safe side.
swap	This should normally be twice the size of the RAM installed on your server. If you create a / boot partition, create the swap partition second. Otherwise, create the swap partition first.

Partition to Create	Other Considerations
/	Define this partition as 3 GB or more. In all cases, create this partition after you create the swap partition. Keep in mind that this root (/) partition contains all of the partitions listed below that you don't specifically create.
/var	This contains system logs and should therefore be a separate partition to avoid impacting system and service stability because of a disk-full condition. Define this partition as 4 GB or more.
/opt	Some (mostly commercial) programs install their data in /opt. Define this partition as 4 GB or more.
/usr	Creating this as a separate partition makes updating the server easier if you need to reinstall the system from the beginning because you can keep the partition intact. Define this partition as 4 GB or more.
/srv	This contains the web and FTP servers. Consider making this a separate partition to avoid having someone flood the disk by accident or on purpose, which impacts system and service stability.
/home	User Home directories go here. Consider making this a separate partition to avoid having someone flood the disk by accident or on purpose, which impacts system and service stability. You can allocate the rest of the disk space to this partition.
/tmp	Creating this as a separate partition is optional. However, because it is writable by everyone, best practices suggest creating a separate partition to avoid having someone flood the disk by accident or on purpose, which impacts system and service stability.
	Place application-specific files on a separate partition.
	If you are building a mail server, note where the mail spools reside because they can grow quite large, and you need to anticipate this when you are defining partition sizes.

3.8.2 NSS on the System Disk

For OES, Novell Storage Services (NSS) volumes can be used only as data volumes, not as system volumes.

Additionally, they cannot be created as part of the install process.

However, you must consider whether you will be creating them in the future *on the storage device where you are installing Linux*. (Creating NSS volumes on storage devices that don't contain Linux system partitions requires no special handling.)

The default volume manager for Linux POSIX volumes on SUSE Linux is LVM (Linux Volume Manager).

3.8.3 Security Flag Recommendations

The following table indicates the recommended security flags for each partition. A question mark indicates that some software might not work if this flag is set.

Mount Point	Mount Options
/	
/var	nosuid
/tmp	nosuid
/home	nosuid, nodev, noexec?
/srv	nosuid?, nodev?, noexec?, ro? (after installation)
/usr/local	nosuid?, nodev?, ro? (after installation)
	IMPORTANT: Proprietary software installations might fail if executables in /tmp cannot run as the file owner (suid), and devices might not work in /usr/local, etc. In such cases, remount those partitions temporarily with security deactivated.

3.8.4 Partitioning X86 Machines

- There can be a maximum of four primary partitions or three primary partitions and one extended partition. An extended partition can hold 15 (SCSI) or 63 (IDE) logical partitions.
- Each partition is assigned a partition type, depending on the file system planned for the partition.
- Each partition holds its own file system.
- Partitions are mounted into the file system tree at mount points. The content of the partition is visible to users with sufficient access privileges below the mount point.
- One of the partitions must hold the root (/) file system. Other partitions can be integrated into the root file system by using the mount command.
- The /etc/fstab file holds partition and mount point information to allow automatic mounting at boot time.
- Device files in the “device” (/dev) partition are used to represent and address partitions; for example:

/dev/hda	Master disk on the first IDE channel
/dev/hda1	First primary partition on the IDE channel disk
/dev/hda5	First logical partition within the extended partition on that disk
/dev/sdb	Second SCSI disk
/dev/sdb3	Third primary partition on the second SCSI disk

3.8.5 Disk Partition Statistics

Use the following commands to get information about system storage usage:

`df`	Displays information about partitions
`df -h`	Displays information in megabytes or gigabytes as applicable (human readable format)
`du`	Displays disk usage
`du /dirA`	Displays the size of each file and directory in dirA
`du -sh`	Prints a summary of information in megabytes or gigabytes

3.8.6 Combining Hard Disk Partitions

- Partitions from two or more hard disks can be combined by using the logical volume manager (LVM).
- Partitions (physical volumes) can be combined into a volume group, which in turn can be divided into logical volumes that contain their own file systems.

Doing this increases flexibility because physical volumes can be easily added to the volume group if more storage space is needed. Logical volumes can be added while the machine is up and running.

3.9 Setting Up the Clock and Time Zone

1. Select the **Region** and **Timezone** either by using the map or the drop-down lists, then click **Next**.

   You can configure this information after the installation is complete, but it is easier to do it during the installation.
2. Continue with Section 3.10, “Creating Local User,” on page 48.

3.10 Creating Local User

You can create a local user and configure the user credentials, which is used for network authentication during log in.

1. Specify the **User’s Full Name**, which includes the first and last name of the user.
2. Specify the **Username** that will be used to log in.

   Only use lowercase letters (a-z), digits (0-9) and the characters . (dot), - (hyphen) and _ (underscore). Special characters, umlauts, and accented characters are not allowed
3. Specify the **Password** for the user.

   For security reasons, the password should be at least six characters long and consist of uppercase and lowercase letters, digits, and special characters (7-bit ASCII). Umlauts or accented characters are not allowed.
4. Re-enter the password specified in **Confirm Password**.

5 (Optional) To use the same password for both the user and the system administrator root log in, select **Use this password for system administrator**.

6 (Optional) To enable the user to log in to the system automatically when it starts, select **Automatic Login**.

7 Click **Next**.

If you do not want to configure any local users, select **Skip User Creation** to skip this step and confirm the warning.

3.11 Authentication for the System Administrator "root"

If you did not select **Use this password for system administrator** in the previous page Local User, you are prompted to specify a password for the System Administrator root. In the Password for the System Administrator root page:

1 Specify the password for the `root` administrator.

For security reasons, the `root` user's password should be at least five characters long and should contain a mixture of both uppercase and lowercase letters and numbers. Passwords are case sensitive.

The default password length limit is 8 characters. The maximum possible length for passwords is 72 characters.

2 Confirm the password.

3 Click **Next**.

3.12 Specifying the Installation Settings

The Installation Settings page lets you specify which software and services are installed on your server.

- Section 3.12.1, "Customizing the Software Selections," on page 49
- Section 3.12.2, "Configuring the Firewall Settings," on page 51
- Section 3.12.3, "Setting Systemd Target," on page 53
- Section 3.12.4, "Accepting the Installation Settings," on page 53

3.12.1 Customizing the Software Selections

IMPORTANT: To install any of the OES patterns, you must customize the software selections. If you don't make any selections, only the base OES packages are installed. However, you can install any of the patterns after the base OES installation is complete. See "Installing or Configuring OES Services on an Existing OES Server" on page 87.

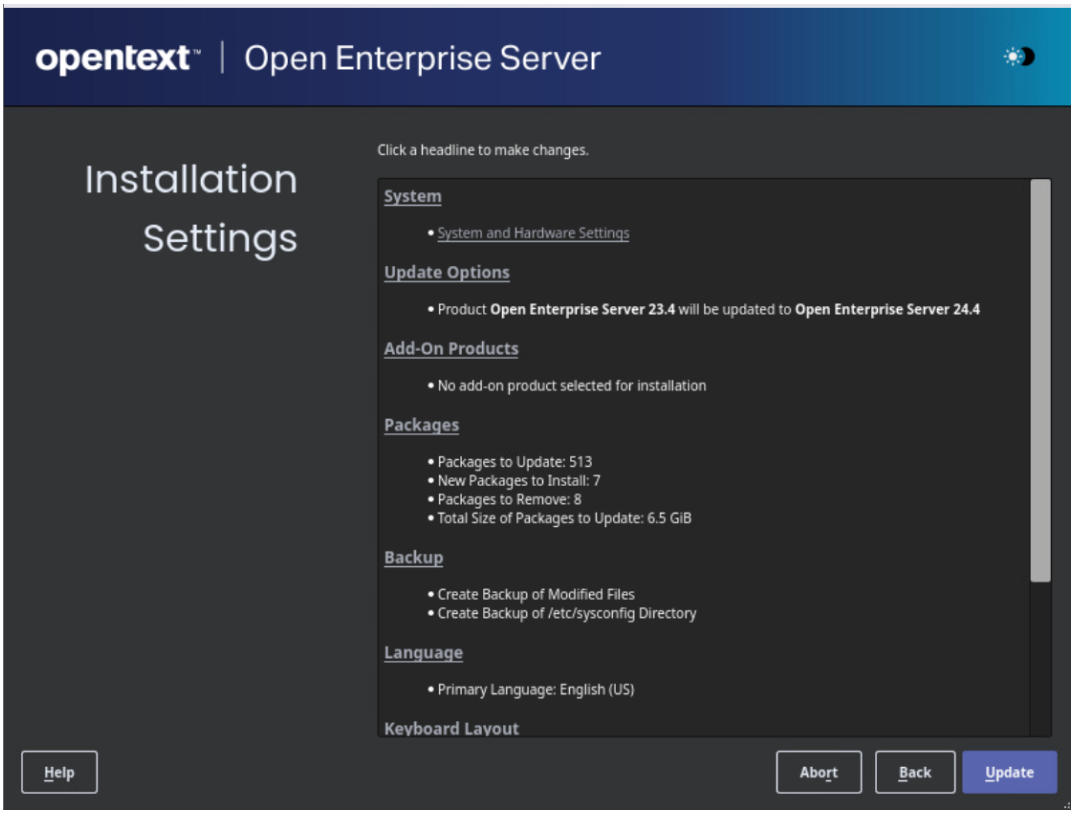
To customize which software packages are installed on the server:

1 On the Installation Settings page, click **Software**.

None of the OES Services is selected by default. This lets you fully customize your OES server.

2 You can do the following to customize your software selections:

- **Select OES Services:** You can select any number of the OES Services patterns as long as you avoid unsupported service combinations.



A description of each pattern displays to the right of the pattern when it is selected. For a description of OES Services patterns and the components selected with each pattern, see Table 2-4 on page 26.

IMPORTANT: If you deselect a pattern after selecting it, you are instructing the installation program to not install that pattern and all of it dependent patterns. Rather than deselecting a pattern, click **Cancel** to cancel your software selections, then click the **Software** heading again to choose your selections again.

Selecting only the patterns that you want to install ensures that the patterns and their dependent patterns and packages are installed.

If you click **Accept** and then return to software pattern selection page, the selections that you made become your base selections and must be deselected if you want to remove them from the installation proposal.

Selecting a pattern automatically selects the other patterns that it depends on to complete the installation.

- **Customize Your Selections:** You can view the details of your selection and add or remove specific packages for the installation by clicking **Details**.

3 When you have selected the software components that you want to install, click **Accept**.

4 (Conditional) If the prompt for **Automatic Changes** displays, click **Continue**.

5 (Conditional) If prompted, resolve any dependency conflicts.

3.12.2 Configuring the Firewall Settings

For security reasons, a firewall is started automatically on each configured interface. The configuration proposal for the firewall is updated automatically every time the configuration of the interfaces or services is modified.

Many of the OES services require an open port in the firewall. Table 3-2 shows the ports that are automatically opened when each listed OES service is configured.

Table 3-2 *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)
OES 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)
eDir API Port (Identity Console)	◆ 9010
iManager	◆ 80 (HTTP) ◆ 443 (secure HTTP)
iPrint	◆ 80 (HTTP) ◆ 443 (secure HTTP) ◆ 631 (IPP)

Service	Default Ports
Novell Identity Translator	◆ 3268 ◆ 389
OES CIFS	◆ 139 (Netbios) ◆ 445 (Microsoft-ds)
Cloud Integrated Storage (CIS)	**Infrastructure services:** ◆ 2181 (ZooKeeper) ◆ 2282 (secure ZooKeeper) ◆ 9092 (Kafka) ◆ 9094 (secure Kafka) ◆ 9400 (OpenSearch) ◆ 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

Service	Default Ports
SFCB	• 5988 (HTTP) • 5989 (secure HTTP)
Secure Shell	• 22
Storage Management Services (Backup)	• 40193 (smdr daemon)
Time Synchronization	• 323 (Network Time Protocol UDP)
OES Database Port	• 5432
NSS AD	• 389 • 636 • 88 • 749 • 464

To adapt the automatic settings to your own preferences:

1. On the Installation and Settings page, click **Security**.
2. On the Security Configuration page, select the required option and click **OK**.

To disable the firewall:

1. On the Installation Settings page, under **Security**, click **disable** on the **Firewall will be enabled** status line.

   or

   On the Installation Settings page, click **Security**; deselect **Enable Firewall** on the Security Configuration page and click **OK**.

   When the firewall is disabled, the status for Firewall should read **Firewall will be disabled**.
2. Verify that the settings on the Installation Settings page are set as desired, then click **Install**. Continue with Section 3.12.4, “Accepting the Installation Settings,” on page 53.

3.12.3 Setting Systemd Target

If you are installing OES in text mode, you must set the systemd target before continuing with the installation.

1. On the Installation Settings page, click **Default Systemd Target**.
2. On the Set Default Systemd Target page, select **Text mode** and click **OK**.
3. Continue with Section 3.12.4, “Accepting the Installation Settings,” on page 53.

3.12.4 Accepting the Installation Settings

1. Review the final Installation Summary page to ensure that you have all the Installation settings you desire.
2. After you have changed all the Installation Settings as desired, click **Install**.

3 On the Confirm Installation page, click **Install**.

The base installation settings are applied and the packages are installed.

4 After the server reboot, proceed with "Configuring Open Enterprise Server" on page 54.

3.13 Configuring Open Enterprise Server

You can configure OES in two methods: Typical Configuration and Custom Configuration. The Typical Configuration is also called as Express Install. It helps to install OES with minimal user intervention and the Custom Configuration is the detailed usual method to configure OES.

3.13.1 Typical Configuration

In the OES Configuration screen, if you have chosen to configure OES using Typical Configuration, you only need to provide the following minimum configuration details:

- **SLP Server and SLP Scopes:** In these fields, specify the host name or the IP address of the server where the SLP agent is running and the SLP scopes. If you don't enter any SLP details, multicast SLP mode is chosen by default.

  NOTE: If you would like to use the current server as the DA server, click **Back** and choose the custom configuration instead of typical configuration.

- **NTP Time Server:** Specify the IP address or the host name of the Network Time Protocol (NTP) server.
- **New or Existing Tree:** If you would like to configure OES using an existing eDirectory tree, choose **Existing Tree** else **New Tree**.
- **eDirectory Tree Name:** Provide the eDirectory tree name.
- **IP Address of an existing eDirectory Server with a replica:** If you have chosen to configure OES using an existing tree, this field is enabled to provide the IP address of an existing eDirectory server.

  IMPORTANT: Ensure that you verify the status of the eDirectory tree using the **Validate** button. If the validation is unsuccessful, do not proceed further with the OES configuration until the eDirectory server is up and running.

- **FDN of the tree administrator:** Specify the fully distinguished name of the administrative user.
- **Admin Password and Verify Admin Password:** In these two fields, specify the eDirectory administrative passwords.
- **Enter Server Context:** Specify the location of the server context in the eDirectory tree.
- **Directory Information Base (DIB) Location:** Specify the location of the eDirectory DIB.
- After providing all these details, click **Next**. OES will be installed and configured without any user intervention.

3.13.2 Custom Configuration

This is the normal method of installing and configuring OES by providing every configuration detail that OES requires instead of using the default configuration details. Custom configuration is explained in detailed in Section 3.13.3, “Specifying eDirectory Configuration Settings,” on page 55, Section 3.13.4, “Specifying LDAP Configuration Settings,” on page 61, Section 3.13.5, “Configuring OES Services,” on page 61, and Section 3.13.6, “Configuration Guidelines for OES Services,” on page 63.

3.13.3 Specifying eDirectory Configuration Settings

When you specify the eDirectory configuration settings, you can specify information to create a new tree and install the server in that new tree, or you can install the server into an existing tree by specifying the information for it. Use the following instructions as applicable:

- “Specifying SLP Configuration Options” on page 55
- “Specifying Synchronizing Server Time Options” on page 56
- “Creating a New eDirectory Tree and Installing the Server in It” on page 56
- “Installing the Server into an Existing eDirectory Tree” on page 57
- “Selecting the NetIQ Modular Authentication Services (NMAS) Login Method” on page 59
- “Specifying OES Common Proxy User Information” on page 60

Specifying SLP Configuration Options

1 On the eDirectory Configuration - SLP page, specify the SLP options as desired.

You have the following options for configuring SLP:

- **Use Multicast to Access SLP:** This option allows the server to request SLP information by using multicast packets. Use this in environments that have not established SLP DAs (Directory Agents).

  IMPORTANT: If you select this option, you must disable the firewall for SLP to work correctly. Multicast creates a significant amount of network traffic and can reduce network throughput.

- **Configure SLP to use an existing Directory Agent:** This option configures SLP to use an existing Directory Agent (DA) in your network. Use this in environments that have established SLP DAs. When you select this option, you configure the servers to use by adding or removing them from the SLP Directory Agent list.
- **Configure as Directory Agent:** This option configures this server as a Directory Agent (DA). This is useful if you plan to have more than three servers in the tree and want to set up SLP during the installation.
  - **Synchronize Service Registrations with other Directory Agents:** This option causes SLP, when it starts, to query the Directory Agents listed under Configured SLP Directory Agents for their current lists of registered services. It also causes the DA to share service registrations that it receives with the other DAs in the SLP Directory Agent list.

- **Backup SLP Registrations:** This option causes SLP to back up the list of services that are registered with this Directory Agent on the local disk.
- **Backup Interval in Seconds:** This specifies how often the list of registered services is backed up.

- **Service Location Protocols and Scopes:** This option configures the scopes that a user agent (UA) or service agent (SA) is allowed when making requests or when registering services, or specifies the scopes a directory agent (DA) must support. The default value is DEFAULT. Use commas to separate each scope. For example, net.slp.useScopes = myScope1,myScope2,myScope3.
- **Configured SLP Directory Agents:** This option lets you manage the list of hostname or IP addresses of one or more external servers on which an SLP Directory Agent is running.

2 Click **Next** and confirm your selection if necessary.

Specifying Synchronizing Server Time Options

eDirectory requires that all OES servers are time-synchronized.

1 On the eDirectory Configuration - NTP page, click **Add**.

2 In the **Time Servers** text box, specify the IP address or DNS hostname of an NTP server, then click **Add**.

For the first server in a tree, we recommend specifying a reliable external time source.

When you install multiple servers into the same eDirectory tree, ensure that all servers point to the same time source and not to the server holding the master replica.

For servers joining a tree, specify the same external NTP time source that the tree is using, or specify the IP address of a configured time source in the tree. A time source in the tree should be running time services for 15 minutes or more before connecting to it; otherwise, the time synchronization request for the installation fails.

3 If you want to use the server's hardware clock, select **Use Local Clock**.

For servers joining a tree, the installation does not let you proceed if you select this option. You must specify the same external NTP time source that the tree is using, or specify the IP address of a configured time source in the tree that has been running time services for 15 minutes or more.

For more information on time synchronization, see "Implementing Time Synchronization" in the *Planning and Implementation Guide*.

Creating a New eDirectory Tree and Installing the Server in It

1 On the eDirectory Configuration - New or Existing Tree page, select **New Tree**.

2 In the **eDirectory Tree Name** field, specify a name for the eDirectory tree that you want to create.

On OES servers, services that provide HTTPS connectivity are configured to use one of the following certificates:

- An eDirectory certificate issued by the Novell International Cryptographic Infrastructure (NICI)
- A third-party server certificate

By default, the **Use eDirectory Certificates for HTTPS Services** check box is selected. This means that the server certificate and key files will be created.

The eDirectory server certificate and key files are:

- Key file: `/etc/ssl/servercerts/serverkey.pem`
- Certificate file: `/etc/ssl/servercerts/servercert.pem`

For more information, see "Certificate Management" in the *Planning and Implementation Guide*.

3 On the eDirectory Configuration - New Tree Information page, specify the required information:

- The fully distinguished name and context for the user Admin
- The password for user Admin

4 Click **Next**.

5 On the eDirectory Configuration - Local Server Configuration page, specify the following information:

- The context for the server object in the eDirectory tree
- A location for the eDirectory database

  The default path is `/var/opt/novell/eDirectory/data/dib`, but you can use this option to change the location if you expect to have a large number of objects in your tree and if the current file system does not have sufficient space.
- The ports to use for servicing LDAP requests

  The default ports are 389 (non-secure) and 636 (secure).

  IMPORTANT: The scripts that manage the common proxy user require port 636 for secure LDAP communications.

- The ports to use for providing access to the iMonitor application

  The default ports are 8028 (non-secure) and 8030 (secure).

  NOTE: If there are non-default ports that are not added to the firewall, you can open the ports using the **yast2 firewall** after the installation is complete.

  ---

6 Click **Next**.

Installing the Server into an Existing eDirectory Tree

1 On the eDirectory Configuration - New or Existing Tree page, select **Existing Tree**.

2 In the **eDirectory Tree Name** field, specify a name for the eDirectory tree you want to join.

On OES servers, services that provide HTTPS connectivity are configured to use either of the following:

- An eDirectory certificate issued by the Novell International Cryptographic Infrastructure (NICI)

By default, the **Use eDirectory Certificates for HTTPS Services** check box is selected. This means that the existing YaST server certificate and key files will be replaced with eDirectory server certificate and key files.

The eDirectory server certificate and key files are:

- Key file: `/etc/ssl/servercerts/serverkey.pem`
- Certificate file: `/etc/ssl/servercerts/servercert.pem`

For more information on certificate management, see "Certificate Management" in the *Planning and Implementation Guide*.

- By default, **Enable NMAS-based login for LDAP authentication** is selected to enforce the use of a single-secure password for all partner products. The Secure Password Manager of the NMAS module manages this universal password implementation.

3 On the eDirectory Configuration - Existing Tree Information page, specify the required information:

- The IP address or the host name of an existing eDirectory server with a replica.

  IMPORTANT: Ensure that you verify the status of the eDirectory tree using the **Validate** button. If the validation is unsuccessful, do not proceed further with the OES configuration until the eDirectory server is up and running.

- The NCP port on the existing server
- The LDAP and secure LDAP port on the existing server
- The fully distinguished name and context for the user Admin on the existing server
- The password for user Admin on the existing server

4 Click **Next**.

5 On the eDirectory Configuration - Local Server Configuration page, specify the following information:

- The context for the server object in the eDirectory tree
- A location for the eDirectory database

  The default path is `/var/opt/novell/eDirectory/data/dib`, but you can use this option to change the location if you expect to have a large number of objects in your tree and if the current file system does not have sufficient space.

- The ports to use for servicing LDAP requests

  The default ports are 389 (non-secure) and 636 (secure).

  IMPORTANT: The scripts that manage the common proxy user require port 636 for secure LDAP communications.

- The ports to use for providing access to the iMonitor application

  The default ports are 8028 (non-secure) and 8030 (secure).

  NOTE: If there are non-default ports that are not added to the firewall, you can open the ports using the **yast2 firewall** after the installation is complete.

6 Click **Next**.

Selecting the NetIQ Modular Authentication Services (NMAS) Login Method

1 On the **NetIQ Modular Authentication Services** page, select all of the login methods you want to install.

IMPORTANT: The NMAS client software must be installed on each client workstation where you want to use the NMAS login methods. The NMAS client software is included with the Client for Open Enterprise Server software.

The following methods are available:

- **CertMutual:** The Certificate Mutual login method implements the Simple Authentication and Security Layer (SASL) EXTERNAL mechanism, which uses SSL certificates to provide client authentication to eDirectory through LDAP.
- **Challenge Response:** The Challenge Response login method works with the Identity Manager password self-service process. This method allows either an administrator or a user to define a password challenge question and a response, which are saved in the password policy. Then, when users forget their passwords, they can reset their own passwords by providing the correct response to the challenge question.
- **DIGEST-MD5:** The Digest-MD5 login method implements the Simple Authentication and Security Layer (SASL) DIGEST-MD5 mechanism as a means of authenticating the user to eDirectory through LDAP.
- **NDS:** The NDS login method provides secure password challenge-response user authentication to eDirectory. This method is installed by default and supports the traditional NDS password when the NMAS client is in use. Reinstallation is necessary only if the NDS login method object has been removed from the directory.
- **Simple Password:** The Simple Password NMAS login method provides password authentication to eDirectory. The Simple Password is a more flexible but less secure alternative to the NDS password. Simple Passwords are stored in a secret store on the user object.
- **SASL GSSAPI:** The SASL GSSAPI login method implements the Generic Security Services Application Program Interface (GSSAPI) authentication. It uses the Simple Authentication and Security Layer (SASL), which enables users to authenticate to eDirectory through LDAP by using a Kerberos ticket.

For more information about installing and configuring eDirectory, see "Installing or Upgrading NetIQ eDirectory on Linux in the *NetIQ eDirectory Installation Guide*.

For more information on these login methods, see the online help and "Managing Login and Post-Login Methods and Sequences" in the *Novell Modular Authentication Services 3.3.4 Administration Guide*.

2 Click **Next**.

Specifying OES Common Proxy User Information

For an OES service to run successfully, you need to use a separate proxy account to configure and manage each service. However, using multiple proxy user accounts means more overhead for the administrator. To avoid this overhead, the common proxy user has been introduced. Each node in a tree can have a common proxy user for all of its services. This enables administrators to configure and manage multiple services with just one proxy user.

NOTE: Two nodes in a tree cannot have the same common proxy user.

For information about this option, see "Common Proxy User" in the *Planning and Implementation Guide*.

1 On the OES Common Proxy User Information page, specify the configuration settings for this user.

- **Use Common Proxy User as Default for OES Products:** This option is disabled for the user and configures the common proxy user for the following services: CIFS, DNS, DHCP, and NCS. Optionally, you can specify that LUM uses it.
- **OES Common Proxy User Name:** For a host, the common proxy user's name is `OESCommonProxy_hostname`. You cannot specify any other name than what is given by the system. This restriction prevents possible use of the same common proxy user name across two or more nodes in a tree. For more information, see "Can I Change the Common Proxy User Name and Context?" in the *Planning and Implementation Guide*.
- **OES Common Proxy User Context:** Provide the FDN name of the container where the common proxy needs to be created. By default, this field is populated with the NCP server context. For example, `ou=acap,o=mf`. Where `ou` is the organization unit, `acap` is the organization unit name, `o` is the organization, and `mf` is the new organization name. For an existing tree, click **Browse** and select the container where the Common Proxy User must be created.
- **OES Common Proxy User Password:** You can accept the default system-generated password or specify a new password for the common proxy user.

  NOTE: If you choose to provide your own password, it should conform to the policy that is in effect for the common proxy user. If the password contains single (') or double (") quotes, OES Configuration will fail. These characters have to be escaped by prefixing \. For example, to add a single quote, escape it as nove\'ll. The system-generated password will always be in conformance with the policy rules.

- **Verify OES Common Proxy User Password:** If you specified a different password, type the same password in this field. Otherwise, the system-generated password is automatically included.
- **Assign Common Proxy Password Policy to Proxy User:** The initial common proxy password policy is a simple password policy created with default rules. If desired, you can modify this policy after the installation to enforce stricter rules regarding password length, characters supported, expiration intervals, and so forth.

IMPORTANT: We recommended against deselecting the **Assign Common Proxy Password Policy to Proxy User** option. If deselected, the common proxy user inherits the password policies of the container, which could lead to service failures.

2 Click **Next**.

3.13.4 Specifying LDAP Configuration Settings

Many of the OES services require eDirectory. If eDirectory was not selected as a product to install on this server but other OES services that do require LDAP services were installed, the LDAP Configuration service displays, so that you can complete the required information.

To specify the required information on the Configured LDAP Server page:

1 In the **eDirectory Tree Name** field, specify the name for the existing eDirectory tree that you are installing this server into.

2 In the **Admin Name and Context** field, specify the name and context for user Admin in the existing tree.

3 In the **Admin Password** field, specify a password for the Admin user in the existing tree.

4 Add the LDAP servers that you want the services on this server to use. The servers that you add should hold the master or a read/write replica of eDirectory. Do the following for each server you want to add:

4a Click **Add**.

4b On the next page, specify the following information for the server to add, then click **Add**.

- IP address
- LDAP port and secure LDAP port

5 When all of the LDAP servers that you want to specify are listed, click **Next**.

6 Verify that the Open Enterprise Server Configuration page displays the settings that you expected, then click **Next**.

3.13.5 Configuring OES Services

After you complete the LDAP configuration or the eDirectory configuration, the Open Enterprise Server Configuration summary page is displayed, showing all of the OES components that you installed and their configuration settings.

1 Review the setting for each component. Click the component heading to change any settings.

For help with specifying the configuration information for OES services, see the information in "Configuration Guidelines for OES Services" on page 63.

2 When you are finished reviewing the settings for each component, click **Next**.

3 When you confirm the OES component configurations, you might receive the following error:

```
The proposal contains an error that must be resolved before continuing.
```

If this error is displayed, check the summary list of configured products for any messages immediately below each product heading. These messages indicate products or services that need to be configured. If you are running the YaST graphical interface, the messages are red text. If you are using the YaST text-based interface, they are not red.

For example, if you selected Linux User Management in connection with other OES products or services, you might see a message similar to the following:

```
Linux User Management needs to be configured before you can continue or
disable the configuration.
```

If you see a message like this, do the following:

3a On the summary page, click the heading for the component.

3b Supply the missing information in each configuration page.

When you specify the configuration information for OES services, see the information in "Configuration Guidelines for OES Services" on page 63, or if you are reading online, click a link below:

- Backup/Storage Management Services (SMS)
- OES Business Continuity Cluster (BCC)
- CIFS
- Cloud Integrated Storage (CIS)
- Clustering (NCS)
- DHCP
- DNS
- Domain Services for Windows (DSfW)
- eDirectory
- FTP
- iManager
- iPrint
- Linux User Management (LUM)
- NCP Server/Dynamic Storage Technology
- Pre-Migration Server
- Novell Remote Manager (NRM)
- Novell Storage Services
- NSS Active Directory Support
- Unified Management Console (UMC)

When you have finished the configuration of a component, you are returned to the Open Enterprise Server Configuration summary page.

3c If you want to skip the configuration of a specific component and configure it later, click **Enable**d in the **Configure is enabled** status to change the status to **Reconfigure is disabled**.

If you change the status to **Reconfigure is disabled**, you need to configure the OES components after the installation is complete. See "Installing or Configuring OES Services on an Existing OES Server" on page 87.

4 After resolving all product configuration issues, click **Next** to proceed with the configuration of all components.

5 When the configuration is complete, continue with Section 3.15, "Finishing the Installation," on page 84.

3.13.6 Configuration Guidelines for OES Services

- "Service Configuration Caveats" on page 63
- "LDAP Configuration for Open Enterprise Services" on page 65
- "OES Backup/Storage Management Services (SMS)" on page 65
- "OES Business Continuity Cluster (BCC)" on page 65
- "OES CIFS Services" on page 66
- "Cloud Integrated Storage (CIS)" on page 66
- "OES Cluster Services" on page 66
- "OES DHCP Services" on page 68
- "OES DNS Services" on page 71
- "OES Domain Services for Windows" on page 72
- "OES eDirectory Services" on page 72
- "OES FTP Services" on page 77
- "OES iManager" on page 77
- "OES iPrint Advanced" on page 78
- "OES Linux User Management" on page 78
- "NetWare Core Protocol (NCP) Server" on page 80
- "OES Pre-Migration Server" on page 80
- "OES Remote Manager" on page 80
- "OES Storage Services (NSS)" on page 81
- "NSS Active Directory Support" on page 81
- "OES Database" on page 82
- "Unified Management Console (UMC)" on page 82

Service Configuration Caveats

Keep the following items in mind as you configure OES:

Table 3-3 *Caveats for Configuring OES Services*

Issue	Guideline
Software Selections When Using Text-Based YaST	Some older machines, such as a Dell 1300, use the text mode install by default when the video card does not meet SLES specifications. When you go to the **Software Selection**, and then to the details of the OES software selections, YaST doesn't bring up the OES selections like it does when you use the graphical YaST (YaST2). To view the Software Selection and System Task screen, select **Filter** > **Pattern** (or press Alt+F > Alt+I).

Issue	Guideline

Specifying a State identifier for a Locality Class object	If you to specify a state identifier, such as California, Utah, or Karnataka, as a Locality Class object in your eDirectory tree hierarchy, ensure to use the correct abbreviation in your LDAP (comma-delimited) or NDAP (period-delimited) syntax.
	
	When using LDAP syntax, use “st” to specify a state. For example:
	
	`ou=example_organization,o=example_company,st=utah,c=us`
	
	When using NDAP syntax, use “s” to specify a state. For example:
	
	`ou=example_organization.o=example_company.s=utah.c=us`

Specifying Typeful Admin Names	When you install OES, you must specify a fully distinguished admin name by using the typeful, LDAP syntax that includes object type abbreviations (cn=, ou=, o=, etc.). For example, you might specify the following: `cn=admin,ou=example_organization,o=example_company`

Using Dot-Delimited or Comma-Delimited Input for All Products	For all parameters requiring full contexts, you can separate the names by using comma-delimited syntax. Ensure that you are consistent in your usage within the field.
	
	The OES installation routine displays all input in the comma-delimited (LDAP) format. However, it converts the name separators to dots when this is required by individual product components.
	
	IMPORTANT: After the OES components are installed, be sure to follow the conventions specified in the documentation for each product. Some contexts must be specified using periods (.) and others using commas (,). However, eDirectory supports names like cn=juan\.garcia.ou=users.o=novell. The period (.) inside a name component must be escaped.
	
	When using NDAP format (dot), you must escape all embedded dots. For example: `cn=admin.o=mf\.provo`
	
	When using LDAP format (commas), you must escape all embedded commas. For example: `cn=admin,o=mf\,provo`
	
	The installation disallows a backslash and period (\.) in the CN portion of the admin name.
	
	For example, these names are supported:
	
	`cn=admin.o=mf`
	`cn=admin.o=mf\.provo`
	`cn=admin.ou=deployment\.linux.o=mf\.provo`
	
	These names are not supported:
	
	`cn=admin\.first.o=mf`
	`cn=admin\.root.o=mf`
	
	Before LUM-enabling users whose cn contains a period (.), you must remove the backslash (\) from the unique_id field of the User object container.
	
	For example, cn=juan.garcia has a unique_id attribute = juan\.garcia. Before such a user can be LUM-enabled, the backslash (\) must be removed from the unique_id attribute.

LDAP Configuration for Open Enterprise Services

Table 3-4 *LDAP Configuration for Open Enterprise Services Values*

Page and Parameters
Configured LDAP Servers
◆ **eDirectory Tree Name:** The eDirectory tree name that you specified when configuring eDirectory. The tree that you are installing this server into.
◆ **Admin Name and Context:** The eDirectory Admin name you specified when configuring eDirectory.
◆ **Admin Password:** The password of the eDirectory Admin user.
◆ **Configured LDAP Servers:** You can specify a list of servers that can be used to configure other OES services on this server. Each added server must have either the master or a read/write replica of the eDirectory tree. The first server added to the list becomes the default server for the installed and configured OES services to use. For each server you must specify an IP Address, LDAP Port, Secure LDAP Port, and Server Type. For information about specifying multiple LDAP servers for Linux User Management (LUM), see "Configuring a Failover Mechanism" in the *Linux User Management Administration Guide*. **Default:** The eDirectory server you specified when configuring eDirectory.

OES Backup/Storage Management Services (SMS)

Table 3-5 *OES Backup/Storage Management Services Parameters and Values*

Page and Parameters
SMS Configuration
◆ **Directory Server Address:** If you do not want to use the default shown, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add another LDAP server to the list, add it by using the LDAP Configuration for Open Enterprise Services dialog box. **Default:** The first server selected in the **LDAP Configuration** list of servers.

For additional configuration instructions, see "Installing and Configuring SMS" in the *Installing and Configuring SMS* guide.

OES Business Continuity Cluster (BCC)

For BCC configuration instructions, see Configuring BCC for Peer Clusters, Configuring BCC for Cluster Resources in the BCC Administration Guide for OES 2018 SP2.

OES CIFS Services

Table 3-6 *OES CIFS Parameters and Values*

Page and Parameters
OES CIFS Service Configuration
◆ **eDirectory server address or host name:** Leave the default or select from the drop-down list to change to a different server.
◆ **LDAP port for CIFS Server:** Displays the port value.
◆ **Local NCP Server context:** Displays the NCP Server context.
◆ **CIFS Proxy User** ◆ **Proxy User for CIFS Management:** Proxy user is used for CIFS. This is disabled for the user and a common proxy user is assigned by the system. **NOTE:** This user is granted rights to read the passwords of any users, including non-CIFS users, that are governed by any of the password policies you select in the Novell CIFS Service Configuration page. ◆ For more information on proxy user, see "Planning Your Proxy Users" in the *Planning and Implementation Guide*.
◆ **Credential Storage Location:** Accept OCS or specify the **Local File** option. The CIFS proxy user password is encrypted and encoded in the credential storage location. **Default:** OCS
Novell CIFS Service Configuration (2)
◆ **eDirectory Contexts:** Provide a list of contexts that are searched when the CIFS User enters a user name. The server searches each context in the list until it finds the correct user object.

For additional configuration instructions, see "Installing and Setting Up CIFS" in the *OES CIFS for Linux Administration Guide*.

Cloud Integrated Storage (CIS)

For more information, see Configuring CIS in Cloud Integrated Storage Administration Guide.

OES Cluster Services

Table 3-7 *OES Cluster Services Parameters and Values*

Page and Parameters
Before you configure a node for a OES Cluster Services cluster, ensure that you have satisfied the prerequisites and have the necessary Administration rights described in "Planning for OES Cluster Services" in the *OES Cluster Services for Linux Administration Guide*.
OES Cluster Services (NCS) Configuration

Page and Parameters

Before you configure a node for a OES Cluster Services cluster, ensure that you have satisfied the prerequisites and have the necessary Administration rights described in "Planning for OES Cluster Services" in the *OES Cluster Services for Linux Administration Guide*.

- **New or Existing Cluster:** Specify whether the server is part of a new cluster or is joining an existing cluster.

  Default: Existing Cluster

- **Directory Server Address:** The IP addresses shown are the LDAP servers that are available for this service to use. The selected IP address is the default LDAP server for this service.

  Default: The local LDAP server.

  The LDAP servers that you select must have a master replica or a Read/Write replica of eDirectory. You can add, remove, or change the order of available LDAP servers for the node after the setup is complete by using the `/opt/novell/ncs/install/ncs_install.py` script. For more information, see "Changing the Administrator Credentials or LDAP Server IP Addresses for a Cluster" in the *OES Cluster Services for Linux Administration Guide*.

- **Cluster FDN:** Browse to select an existing eDirectory context where the Cluster objects will be created. The fully distinguished name (FDN) of the cluster is automatically added to the field with a suggested cluster name. You can specify a different cluster name.

  You can also specify the typeful FDN for the cluster. Use the comma format illustrated in the example. Do not use dots.You must specify an existing context. Specifying a new context does not create a new context.

  Cluster names must be unique. You cannot create two clusters with the same name in the same eDirectory tree. Cluster names are case-sensitive on Linux.

- **Cluster IP Address:** If you are creating a new cluster, specify a unique IP address for the cluster.

  The cluster IP address is separate from the server IP address and is required to be on the same IP subnet as the other servers in the cluster.

- **Select the Storage Device With Shared Media:** If you are creating a new cluster, select the device where the Split Brain Detector (SBD) partition will be created.

  An SBD is required if you plan to use shared disks in the cluster. The drop-down menu shows only devices that have been initialized and shared. If a device is not available, accept the default (none). You must create the SBD manually before adding a second server to the cluster.

  Default: none

- **Select the Device where the Mirror Partition will be Created (Optional)":** If you want to mirror the SBD partition for greater fault tolerance, select the device where you want the mirror to be. You can also mirror SBD partitions after installing OES Cluster Services.

  Default: none

Page and Parameters
Before you configure a node for a OES Cluster Services cluster, ensure that you have satisfied the prerequisites and have the necessary Administration rights described in "Planning for OES Cluster Services" in the *OES Cluster Services for Linux Administration Guide*.
◆ **Desired Partition Size of Shared Media (MB):** Specify the size in MB (megabytes) of the SBD partition, or select Use Maximum Size to use the entire shared device. We recommend at least 20 MB for the SBD partition. If you specified a device to mirror the partition, the setting is also applied to the mirror. **Default:** 8
OES Cluster Services (NCS) Proxy User Configuration (2)
Specify the following user as the NCS Proxy user. ◆ **Proxy User for NCS Management:** This is disabled for the user, and the system will choose a common proxy for the NCS service.
OES Cluster Services (NCS) Configuration (3)
◆ **Name of This Node:** This is the hostname of the server.
◆ **IP Address of this Node:** This field contains the IP address of this node. If this server has multiple IP addresses, you can change the default address to another value if desired.
◆ **Start Cluster Services Now:** Select this box if you want clustering to start now. If you want clustering to start after rebooting, or if you want to manually start it later, deselect this box. This option applies only to installing Novell Cluster Services after the OES installation because it starts automatically when the server initializes during the installation. If you choose to not start Novell Cluster Services software, you need to either manually start it after the installation, or reboot the cluster server to automatically start it. You can manually start Novell Cluster Services by entering `systemctl start novell-ncs.service` at the server console of the cluster server. **Default:** Selected

For additional instructions, see the *OES Cluster Services for Linux Administration Guide*.

OES DHCP Services

Table 3-8 *OES DHCP Services Parameters and Values*

Page and Parameters
Novell DHCP Services Configuration
◆ **DHCP Server Context:** Specify a context for the DHCP Server object. **Default:** o=example

Page and Parameters
◆ **DHCP Server Object Name:** Specify the name of the Server object that these DHCP services will be running on. This is the DHCP server object that contains a list of DHCP Services (configuration) served by the DHCP Server. **Default:** DHCP_example_server
◆ **Common DHCP Configuration Object Contexts** ◆ **Locator Object:** Specify the context for the DHCP Locator object. The DHCP Locator object has references to dhcpServer and dhcpService objects. ◆ **Group Context:** Specify the context for the DHCP Group object. This object is used to grant the necessary rights to the eDirectory user used by the DHCP server to access the DHCP objects. **Default:** o=example
◆ **Log File Location:** Specify the path and file name for the DHCP server to dump the configurations it reads from eDirectory. Specify the path manually or click **Browse** to locate the log. **Default:** Usually `/var/log/dhcp-ldap-startup.log`
◆ **LDAP Method** ◆ **Static:** Select this option if you do not want the DHCP server to query the LDAP server for host details. ◆ **Dynamic:** Select this option if you want the DHCP server to query for host details from the LDAP server for every request. Selecting the dynamic LDAP method ensures that the responses you receive to queries are accurate, but the server takes a longer time to respond. **Default:** Static
◆ **Referrals** A referral is a message that the LDAP server sends to the LDAP client informing it that the server cannot provide complete results and that more data might be on another LDAP server. ◆ **Chase Referral:** Select this option if you want the DHCP server to follow referrals. ◆ **Do Not Chase Referral:** Select this option to ignore LDAP referrals. **Default:** Chase referral
OES DHCP LDAP and Secure Channel Configuration
◆ **eDirectory Server Address or Host Name:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add another LDAP server to the list, add it by using the LDAP Configuration for Open Enterprise Services dialog box. **Default:** The first server is selected in the **LDAP Configuration** list of servers.

Page and Parameters
◆ **Use Secure Channel for Configuration:** This option is selected by default. When you are configuring DHCP services, it ensures that all configuration is transferred over a secure channel. Deselecting the option lets a user with fewer privileges configure LDAP services and allows configuration information to be transferred over a non-secure channel. **Default:** Selected
◆ **Proxy User for DHCP Management:** Common proxy user is assigned by the system and can access the DHCP server.
◆ **LDAP Port for DHCP Server:** Select a port for the LDAP operations to use. **IMPORTANT:** The scripts that manage the common proxy user require port 636 for secure LDAP communications. **Default:** 636
◆ **Use Secure channel for DHCP Server:** Selecting this option ensures that the data transferred between the DHCP server and the LDAP server is secure and private. If you deselect this option, the data transferred is in clear text format. **Default:** Selected
◆ **Certificates (optional)** ◆ **Request Certificate:** Specifies what checks to perform on a server certificate in a SSL/TLS session. Select one of the following options: ◆ **Never**: The server does not ask the client for a certificate. This is the default ◆ **Allow**: The server requests a client certificate, but if a certificate is not provided or a wrong certificate is provided, the session still proceeds normally. ◆ **Try:** The server requests the certificate. If none is provided, the session proceeds normally. If a certificate is provided and it cannot be verified, the session is immediately terminated ◆ **Hard:** The server requests a certificate. A valid certificate must be provided, or the session is immediately terminated. ◆ **Paths to Certificate Files:** Specify or browse the path for the certificate files. ◆ The LDAP CA file contains CA certificates. ◆ The LDAP client certificate contains the client certificate. ◆ The LDAP client key file contains the key file for the client certificate.
OES DHCP Services Interface Selection
◆ **Network Boards for the OES DHCP Server:** From the available interfaces, select the network interfaces that the Novell DHCP server should listen to.

For additional configuration instructions, see "Installing and Configuring DHCP " in the *DNS/DHCP Services for Linux Administration Guide*.

OES DNS Services

Table 3-9 *OES DNS Services Parameters and Values*

Page and Parameters
OES DNS Configuration
◆ **Directory server address:** If you have specified multiple LDAP servers by using the LDAP Configuration for Open Enterprise Services dialog box, you can select a different LDAP server than the first one in the list. If you are installing into an existing tree, ensure that the selected server has a master or read/write replica of eDirectory. **Default:** The first LDAP server in the **LDAP Server Configuration** dialog box. ◆ **Local NCP Server Context:** Specify a context for the local NCP Server object. **Default:** The eDirectory context specified for this OES server. ◆ **Use Secure LDAP Port:** Selecting this option ensures that the data transferred by this service is secure and private. If you deselect this option, the transferred data is in clear text format. **Default:** Selected ◆ **Proxy User for DNS Management:** By default, the common proxy user is assigned by the system and cannot be changed. An existing user must have eDirectory read, write, and browse rights under the specified context. If the user doesn't exist, it is created in the context specified. ◆ **Credential Storage Location:** Specify where the DNS proxy user's credentials are to be stored. **Default:** For security reasons, the default and recommended method of credential storage is OCS.

Page and Parameters

• **Common DNS Configuration Object and User Contexts:**
  • **Get Context and Proxy User Information from Existing DNS Server:** Select this option if you are configuring DNS in an existing tree where DNS is already configured, and you want to use the existing Locator, Root Server Info, Group and Proxy User contexts.
  • **Existing OES DNS Server Address:** If you have enabled the previous option, you can type the IP address of an NCP server (must be up and running) that is hosting the existing DNS server.
  To automatically retrieve the contexts of the objects that follow, click **Retrieve**.
  If you do not want to use the retrieved contexts, you can change them manually.
  • **OES DNS Services Locator Object Context:** Specify the context for the DNS Locator object.
  The Locator object contains global defaults, DHCP options, and a list of all DNS and DHCP servers, subnets, and zones in the tree.
  Default: The context you specified for the OES server you are installing.
  • **OES DNS Services Root Server Info Context:** Specify the context for the DNS Services root server.
  The RootSrvrInfo Zone is an eDirectory container object that contains resource records for the DNS root servers.
  Default: The context you specified for the OES server you are installing.
  • **OES DNS Services Group Object Context:** Specify the context for the DNS Group object.
  This object is used to grant DNS servers the necessary rights to other data within the eDirectory tree.
  Default: The context you specified for the OES server you are installing.

• **Create DNS Server Object:** Select this check box if you want to create the DNS server object in the eDirectory tree associated with the NCP server. • **Host Name:** Type the unique host name for the DNS server object. • **Domain Name for the DNS Server:** Type the domain name for the server object.

For additional configuration instructions, see "Installing and Configuring DNS " in the *DNS/DHCP Services for Linux Administration Guide*.

OES Domain Services for Windows

There are multiple configuration scenarios, depending on your deployment. For information, see "Installing Domain Services for Windows" in the *Domain Services for Windows Administration Guide*.

OES eDirectory Services

IMPORTANT: You specified the eDirectory configuration for this server in either "Specifying LDAP Configuration Settings" on page 61 or "Specifying eDirectory Configuration Settings" on page 55, and the settings you specified were extended to your OES service configurations by the OES install.

If you change the eDirectory configuration at this point in the install, your modifications might or might not extend to the other OES services. For example, if you change the server context from o=example to ou=servers.o=example, the other service configurations might or might not reflect the change.

Be sure to carefully check all of the service configuration summaries on the Open Enterprise Server Configuration summary screen. If any of the services don't show the eDirectory change you made, click the service link and modify the configuration manually. Otherwise, your installation will fail.

Table 3-10 *OES eDirectory Parameters and Values*

Page and Parameters
eDirectory Configuration - New or Existing Tree
◆ **New or Existing Tree** ◆ **New Tree:** Creates a new tree. Use this option if this is the first server to go into the tree or if this server requires a separate tree. Keep in mind that this server will have the master replica for the new tree, and that users must log in to this new tree to access its resources. ◆ **Existing Tree:** Incorporates this server into an existing eDirectory tree. This server might not have a replica copied to it, depending on the tree configuration. For details, see Guidelines for Replicating Your Tree in the NetIQ eDirectory Administration Guide . **Default:** New Tree
◆ **eDirectory Tree Name:** Specify a unique name for the eDirectory tree you want to create or the name of the tree you want to install this server into. ◆ **Use eDirectory Certificates for HTTPS Services:** Selecting this option causes eDirectory to automatically back up the currently installed certificate and key files and replace them with files created by the eDirectory Organizational CA (or Tree CA). Most OES services that provide HTTPS connectivity are configured by default to use the self-signed common server certificate created by YaST. Self-signed certificates provide minimal security and limited trust, so you should consider using eDirectory certificates instead. For all server installations, this option is enabled by default and is recommended for the increased security it provides. To prevent third-party CA certificates from being accidentally backed up and overwritten, deselect this option. For more information on certificate management and this option, see "Security" in the *Planning and Implementation Guide*. ◆ **Require TLS for Simple Binds with Password:** Select this option to make connections encrypted in the Session layer. ◆ **Install SecretStore:** Select this option to install Novell SecretStore (SS), an eDirectory-based security product.
eDirectory Configuration - New/Existing Tree Information

Page and Parameters
◆ **IP Address / Host Name of an Existing eDirectory Server with a Replica:** Specify the IP address of a server with an eDirectory replica. This option appears only if you are joining an existing tree.
◆ **NCP Port on the Existing Server:** Specify the NCP port used by the eDirectory server you specified. This option appears only if you are joining an existing tree. **Default:** 524
◆ **LDAP and Secure LDAP Ports on the Existing Server:** Specify the LDAP ports used by the eDirectory server you specified. This option appears only if you are joining an existing tree. **IMPORTANT:** The scripts that manage the common proxy user require port 636 for secure LDAP communications. **Default:** 389 (LDAP), 636 (Secure LDAP)
◆ **FDN Admin Name with Context:** Specify the name of the administrative user for the new tree. This is the fully distinguished name of a User object that will be created with full administrative rights in the new directory. **Default:** The eDirectory Admin name and context that you specified when initially configuring eDirectory.
◆ **Admin Password:** Specify the eDirectory administrator's password. This is the password of the user specified in the prior field.
◆ **Verify Admin Password:** Retype the password to verify it. This option only appears if you are creating a new tree.
eDirectory Configuration - Local Server Configuration
◆ **Enter Server Context:** Specify the location of the new server object in the eDirectory tree.
◆ **Directory Information Base (DIB) Location:** Specify a location for the eDirectory database. **Default:** The default path is `/var/opt/novell/eDirectory/data/dib`, but you can use this option to change the location if you expect the number of objects in your tree to be large and the current file system does not have sufficient space.
◆ **Enter LDAP Port:** Specify the LDAP port number this server will use to service LDAP requests. **Default:** 389
◆ **Enter Secure LDAP Port:** Specify secure LDAP port number this server will use to service LDAP requests. **IMPORTANT:** The scripts that manage the common proxy user require port 636 for secure LDAP communications. **Default:** 636

Page and Parameters
◆ **Enter iMonitor Port:** Specify the port this server will use to provide access to the iMonitor application. iMonitor lets you monitor and diagnose all servers in your eDirectory tree from any location on your network where a web browser is available. **Default:** 8028
◆ **Enter Secure iMonitor Port:** Specify the secure port this server will use to provide access to the iMonitor application. **Default:** 8030
eDirectory Configuration - NTP and SLP
◆ **Network Time Protocol (NTP) Server:** Specify the IP address or DNS hostname of an NTP server. ◆ For the first server in a tree, we recommend specifying a reliable external time source. ◆ For servers joining a tree, specify the same external NTP time source that the tree is using, or specify the IP address of a configured time source in the tree. A time source in the tree should be running time services for 15 minutes or more before connecting to it; otherwise, the time synchronization request for the installation fails. If the time source server is NetWare 5.0 or earlier, you must specify an alternate NTP time source, or the time synchronization request fails. For more information, see "Time Services" in the *Planning and Implementation Guide*. ◆ **Use Local Clock:** Alternatively, you can select **Use Local Clock** to designate the server's hardware clock as the time source for your eDirectory tree. This is not recommended if there is a reliable external time source available.
◆ **(SLP Options)** ◆ **Use Multicast to Access SLP:** Allows the server to request SLP information by using multicast packets. Use this in environments that have not established SLP DAs (Directory Agents). **IMPORTANT:** If you select this option, you must disable the firewall for SLP to work correctly. Multicast creates a significant amount of network traffic and can reduce network throughput. ◆ **Configure as Directory Agent:** Configures this server as a Directory Agent (DA). This is useful if you plan to have more than three servers in the tree and want to set up SLP during the installation. ◆ **Synchronize Service Registrations with other Directory Agents:** Causes SLP, when it starts, to query the Directory Agents listed under Configured SLP Directory Agents for their current lists of registered services. It also causes the DA to share service registrations that it receives with the other DAs in the SLP Directory Agent list. ◆ **Backup SLP Registrations:** Causes SLP to back up the list of services that are registered with this Directory Agent on the local disk. ◆ **Backup Interval in Seconds:** Specifies how often the list of registered services is backed up. ◆ **Configure SLP to use an existing Directory Agent:** Configures SLP to use an existing Directory Agent (DA) in your network. Use this in environments that have established SLP DAs. When you select this option, you configure the servers to use by adding or removing them from the SLP Directory Agent list.

Page and Parameters

- **Service Location Protocols and Scope:** Configures the scopes that a user agent (UA) or service agent (SA) is allowed when making requests or when registering services, or specifies the scopes that a directory agent (DA) must support. The default value is DEFAULT. Use commas to separate each scope. For example, net.slp.useScopes = myScope1,myScope2,myScope3.

  This information is required when selecting the **Use Multicast to Access SLP** or **Configure SLP to Use an Existing Directory Agent** option.

  Default: Default

- **Configured SLP Directory Agents:** Lets you manage the list of hostname or IP addresses of one or more external servers on which an SLP Directory Agent is running.

  It is enabled for input only when you configure SLP to use an existing Directory Agent.

NetIQ Modular Authentication Services

IMPORTANT: NMAS client software (included with Client for Open Enterprise Server software) must be installed on each client workstation where you want to use the NMAS login methods.

- **CertMutual:** The Certificate Mutual login method implements the Simple Authentication and Security Layer (SASL) EXTERNAL mechanism, which uses SSL certificates to provide client authentication to eDirectory through LDAP.
- **Challenge Response:** The Challenge-Response login method works with the Identity Manager password self-service process. This method allows either an administrator or a user to define a password challenge question and a response, which are saved in the password policy. Then, when users forget their passwords, they can reset their own passwords by providing the correct response to the challenge question.
- **DIGEST-MD5:** The Digest MD5 login method implements the Simple Authentication and Security Layer (SASL) DIGEST-MD5 mechanism as a means of authenticating the user to eDirectory through LDAP.
- **NDS:** The NDS login method provides secure password challenge-response user authentication to eDirectory. This method supports the traditional NDS password when the NMAS client is in use. Reinstallation is necessary only if the NDS login method object has been removed from the directory.
- **Simple Password:** The Simple Password NMAS login method provides password authentication to eDirectory. The Simple Password is a more flexible but less secure alternative to the NDS password. Simple Passwords are stored in a secret store on the user object.
- **SASL GSSAPI:** The SASL GSSAPI login method implements the Generic Security Services Application Program Interface (GSSAPI) authentication by using the Simple Authentication and Security Layer (SASL) that enables users to authenticate to eDirectory through LDAP by using a Kerberos ticket.

If you want to install all of the login methods into eDirectory, click **Select All**.

If you want to clear all selections, click **Deselect All**.

For more information on these login methods, see "Managing Login and Post-Login Methods and Sequences" in the *Novell Modular Authentication Services 3.3.4 Administration Guide*.

Defaults: Challenge Response and NDS

OES Common Proxy User Information

Page and Parameters
◆ **Use Common Proxy User as Default for OES Products:** This option is disabled for the user and configures the common proxy user for the following services: CIFS, DNS, DHCP, and NCS. Optionally, you can specify that LUM use it. ◆ **OES Common Proxy User Name:** By default, the common proxy user is created in the container that you specify for the server object. You can specify a different container, but it must meet one of the following qualifications: ◆ **New Tree Installation:** The container must be included in either the path specified for the eDirectory Admin user or the path for Server object. ◆ **Existing Tree Installation:** The container must already exist in eDirectory. **IMPORTANT:** You cannot create a new container by specifying a non-qualifying path. If you attempt this, the installation program will appear to proceed normally until the eDirectory Configuration (ndsconfig) runs. At that point the installation will fail with an `Error creating Common Proxy User: 32` error, and you will need to install the server again. ◆ **OES Common Proxy User Password:** This is disabled for the user, and password will be generated by system. ◆ **Verify OES Common Proxy User Password:** This is disabled for the user. ◆ **Assign Common Proxy Password Policy to Proxy User:** The initial common proxy password policy is a simple password policy created with default rules. You can modify this policy after the installation to enforce stricter rules regarding password length, characters supported, expiration intervals, and so forth.

For additional configuration instructions, see "Installing or Upgrading NetIQ eDirectory on Linux" in the *NetIQ eDirectory Installation Guide*.

OES FTP Services

No additional configuration is required.

OES iManager

Table 3-11 *NetIQ iManager Parameters and Values*

Page and Parameters
iManager Configuration
◆ **eDirectory Tree:** Shows the name of a valid eDirectory tree that you specified when configuring eDirectory. To change this configuration, you must change the eDirectory configuration.
◆ **FDN Admin Name with Context** Shows the eDirectory Admin name and context that you specified when configuring eDirectory. This is the user that has full administrative rights to perform operations in iManager. To change this configuration, you must change the eDirectory configuration.

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.

For additional configuration instructions, see "Installing iManager Server and Workstation" in the *NetIQ iManager Installation Guide*.

OES iPrint Advanced

Table 3-12 *OES iPrint Advanced Parameters and Values*

Page and Parameters
iPrint Advanced Configuration
◆ **Directory server address:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add another LDAP server to the list, add it by using the LDAP Configuration for Open Enterprise Services dialog box.
◆ **eDirectory Search Context:** iPrint Advanced uses LDAP to verify rights to perform various iPrint operations, including authenticating users for printing and performing management tasks such as uploading drivers. During the installation of the iPrint Advanced software attempts to identify the topmost container of the eDirectory tree and sets the base dn to this container for the AuthLDAPURL entry in `/etc/opt/novell/iprint/httpd/conf/iprint_ssl.conf`. For most installations, this is adequate because users are often distributed across containers. **IMPORTANT:** If you have multiple peer containers at the top of your eDirectory tree, leave this field blank so that the LDAP search begins at the root of the tree.

For more information, see " OES iPrint Advanced Administration Guide".

OES Linux User Management

Table 3-13 *OES Linux User Management Parameters and Values*

Page and Parameters
Linux User Management Configuration

Page and Parameters
◆ **Directory Server Address:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add another LDAP server to the list, add it by using the LDAP Configuration for Open Enterprise Services dialog box. For information about specifying multiple LDAP servers for Linux User Management (LUM), see "Configuring a Failover Mechanism" in the *Linux User Management Administration Guide*. **Default:** The first server selected in the **LDAP Configuration** list of servers
◆ **Unix Config Context:** The UNIX Config object holds a list of the locations (contexts) of UNIX Workstation objects in eDirectory. It also controls the range of numbers to be assigned as UIDs and GIDs when User objects and Group objects are created. Specify the eDirectory context (existing or created here) where the UNIX Config object will be created. An LDAP search for a LUM User, a LUM Group, or a LUM Workstation object begins here, so the context must be at the same level or higher than the LUM objects searched for. If the UNIX Config Object is placed below the location of the User objects, the `/etc/nam.conf` file on the target computer must include the support-outside-base-context=yes parameter. Geographically dispersed networks might require multiple UNIX Config objects in a single tree, but most networks need only one UNIX Config object in eDirectory. **Default:** The server context specified in the eDirectory configuration
◆ **Unix Workstation Context:** Computers running Linux User Management (LUM) are represented by UNIX Workstation objects in eDirectory. The object holds the set of properties and information associated with the target computer, such as the target workstation name or a list of eDirectory groups that have access to the target workstation. Specify the eDirectory context (existing or created here) for the UNIX Workstation object created by the install for this server. The context should be the same as or below the UNIX Config Context specified above. **Default:** The context you specified for this OES server in the eDirectory configuration
◆ **Proxy User for LUM Management (Optional):** The system will assign a common proxy for the LUM service if the user selects the "**User OES Common Proxy User**" option. The user cannot modify this.
◆ **Use OES Common Proxy User:** Check this option if you specified a common proxy user and want to use it as the proxy user for LUM.
◆ **Restrict Access to the Home Directories of Other Users:** This option is selected by default to restrict read and write access for users other than the owner to home directories. Using the default selection changes the umask setting in `/etc/login.defs` from 022 to 077. **Default:** Selected
Linux User Management Configuration (2)

Page and Parameters
IMPORTANT: Before you change the PAM-enabled service settings, ensure that you understand the security implications explained in "User Restrictions: Some OES Limitations" in the *Planning and Implementation Guide*. ◆ **Click to LUM-Enable the Services:** Select the services to LUM-enable on this server. The services marked **yes** are available to authenticated LUM users. ◆ **login**: no ◆ **ftp**: no ◆ **sshd**: no ◆ **su**: no ◆ **sfcbd: yes** This is selected by default because it is used by many of the OES services such as NSS, SMS, and Novell Remote Manager. To access iManager and NRM, you must enable SFCB. ◆ **gdm**: no ◆ **gnome-screensaver**: no ◆ **gnomesu-pam**: no

For additional configuration instructions, see "Setting Up Linux User Management" in the *Linux User Management Administration Guide*.

NetWare Core Protocol (NCP) Server

Table 3-14 *OES NCP Server Parameters and Values*

Page and Parameters
NCP Server Configuration
◆ **Admin Name with Context:** The eDirectory Admin user you specified in the eDirectory configuration.

For additional configuration instructions, see "Installing and Configuring NCP Server for Linux" in the *NCP Server for Linux Administration Guide*.

OES Pre-Migration Server

No additional configuration is required. For information, see "Preparing the Source Server for Migration" the *Migration Tool Administration Guide*.

OES Remote Manager

No additional configuration for the installation is required. To change the configuration after the installation, see "Changing the HTTPSTKD Configuration" in the OES Remote Manager Administration Guide.

OES Storage Services (NSS)

Table 3-15 *OES Storage Services Parameters and Values*

Page and Parameters
NSS Unique Admin Object
◆ **Directory Server Address:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add another LDAP server to the list, add it by using the LDAP Configuration for Open Enterprise Services dialog box. **Default** The first server selected in the **LDAP Configuration** list of servers.
◆ **Unique object Name for NSS Admin of This:** Specify the NSS Admin name and context or accept the default. This is the fully distinguished name of a User object with administrative rights to NSS. You must have a unique NSS admin name for each server that uses NSS. For more information, see "Planning Your Proxy Users" in the *Planning and Implementation Guide*. **Default:** The server hostname concatenated with the LDAP Admin Name you entered for this server,. cn=*myserver*admin,o=*organization*.

For additional configuration instructions, see "Installing and Configuring OES Storage Services" in the *Storage Services File System (NSS) Administration Guide for Linux*.

NSS Active Directory Support

Table 3-16 *NSS Active Directory Support Parameters and Values*

Page and Parameters
◆ **AD Domain Name**: Specify the appropriate AD domain name. ◆ **AD Supervisor Group**: Is the AD supervisor group name. The AD users belonging to this group will have supervisory rights for all the volumes associated with that OES server. ◆ **AD User Name**: Specify the user name that can be used for the domain join operation. This user requires to have the following privileges: rights to reset password, create computer objects, delete computer objects, and read and write the `msDssupportedEncryptionTypes` attribute. ◆ **Password**: Specify the appropriate password of the user who is used for the domain join operation.

Page and Parameters
◆ **Container to Create Computer Object**: You can specify the container under which the OES computer object will be created. The default container is CN=Computers. If you have already created an OES computer object in Active Directory, select **Use pre-created computer object**, then specify the container name where the pre-created OES computer object exists. ◆ **Novell Identity Translator (NIT) Configuration**: NIT is used to manage the eDirectory and Active Directory user identities such as UID, GUID, SID, and user name. It maps those user identities and translates from one identity to another. For more information on NIT, see "About Novell Identity Translator (NIT) (page 136)". If you want NIT to generate UIDs for AD users, select **Generate UID for AD users**, then specify the UID range. The default range is from 100000 to 200000. If you want NIT to fetch UIDs, do not select the **Generate UID for AD users** option.

For additional configuration instructions, see Chapter 7, "Installing and Configuring NSS Active Directory Support," on page 127.

OES Database

Table 3-17 *OES Database*

Page and Parameters
◆ **Hostname:** Specify the host name of the database server. ◆ **Port:** Specify the port for the server. By default, the port number is 5432. ◆ **Username:** Specify the user name of the database server. ◆ **Password and Verify Password:** Specify the password for the database. ◆ **Name:** Specify the name of the database. ◆ **Open port in the firewall:** By default, it is selected to open the port for the database in firewall.

Unified Management Console (UMC)

Table 3-18 *Unified Management Console Parameters and Values*

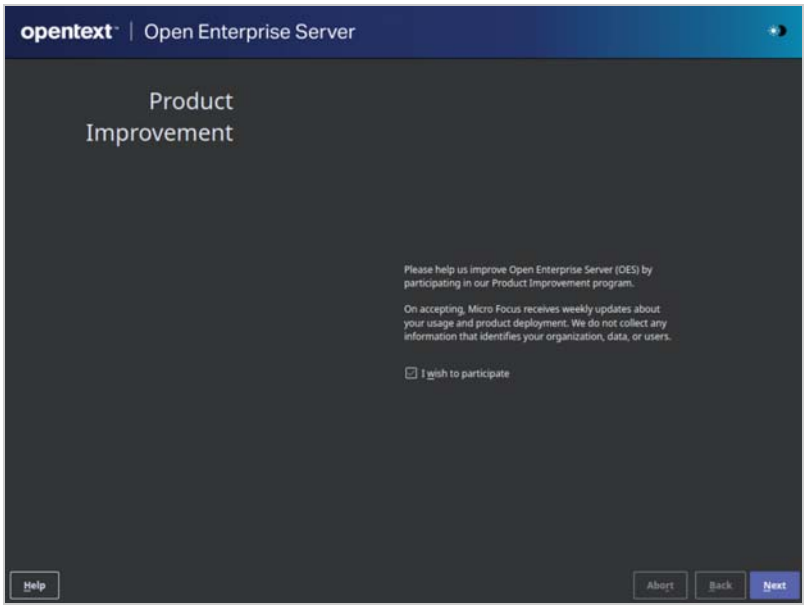
Page and Parameters
◆ **eDirectory API Port:** Specify the eDirectory API port for UMC. By default, the eDirectory API port is 9010.

3.14 Product Improvement

Participating in the Product Improvement program enables 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 microfocus server. For overview and the data collected from each component, see Product Improvement in the Planning and Implementation Guide.

Select the checkbox to participate in the program. All the servers in the same context as this server are automatically enabled and this screen is not displayed to other servers in that context.

Figure 3-1 *Product Improvement - Participate*



3.14.1 How is Data Sent to the Micro Focus Server

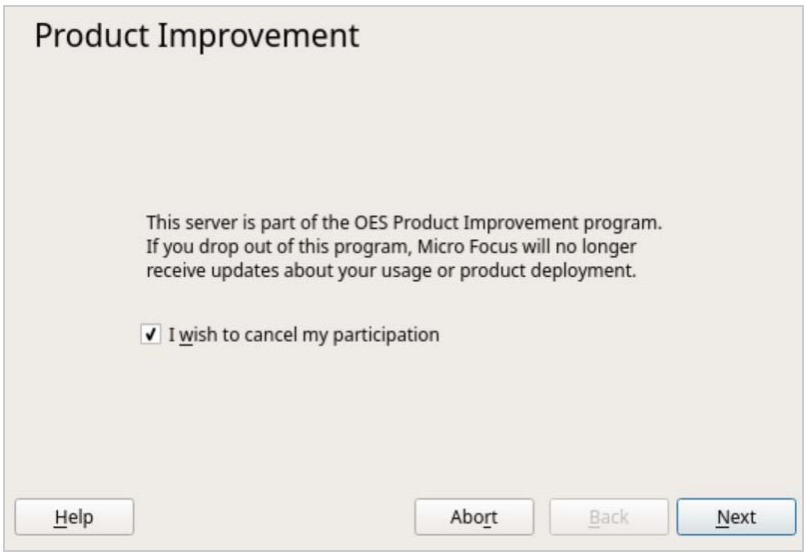
After the weekly collection, the data is stored at /var/opt/novell/telemetry/data/ on the OES server that was configured with this program. The OES server transfers the data to the Micro Focus server. If the transfer is unsuccessful, the system attempts to send it again during the next weekly cycle. 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.

3.14.2 Opt Out of Product Improvement

If you do not wish to continue participation, run `yast2 oes-improvement` on the same server that was configured with this program and select the checkbox. This server and all the other servers in this server's context will no longer contribute to product improvement.

Figure 3-2 *Product Improvement - Cancel*



3.15 Finishing the Installation

After a successful configuration, YaST shows the Installation Completed dialog box. Do the following:

1. (Optional) Select whether to clone your newly installed system for AutoYaST. To clone your system, select **Clone This System for AutoYaST**.

   The profile of the current system is stored in `/root/autoinst.xml`. Cloning is selected by default.

   AutoYaST is a system for automatically installing one or more SUSE Linux Enterprise systems without user intervention. AutoYaST installations are performed by using a control file with installation and configuration data. For detailed information, see Chapter 9, “Using AutoYaST to Install and Configure Multiple OES Servers,” on page 153.
2. Finish the installation by clicking **Finish** in the Installation Completed page.
3. Continue with Section 3.16, “Verifying that the Installation was Successful,” on page 84.

3.16 Verifying that the Installation was Successful

One way to verify that your OES server installation was successful and the components are loading properly is to watch the server console. As each component is loaded, the boot logger provides a status next to it indicating if the components are loading properly.

You can also quickly verify a successful installation by accessing the server from your web browser.

1. In the Address field of your web browser, specify the following URL:

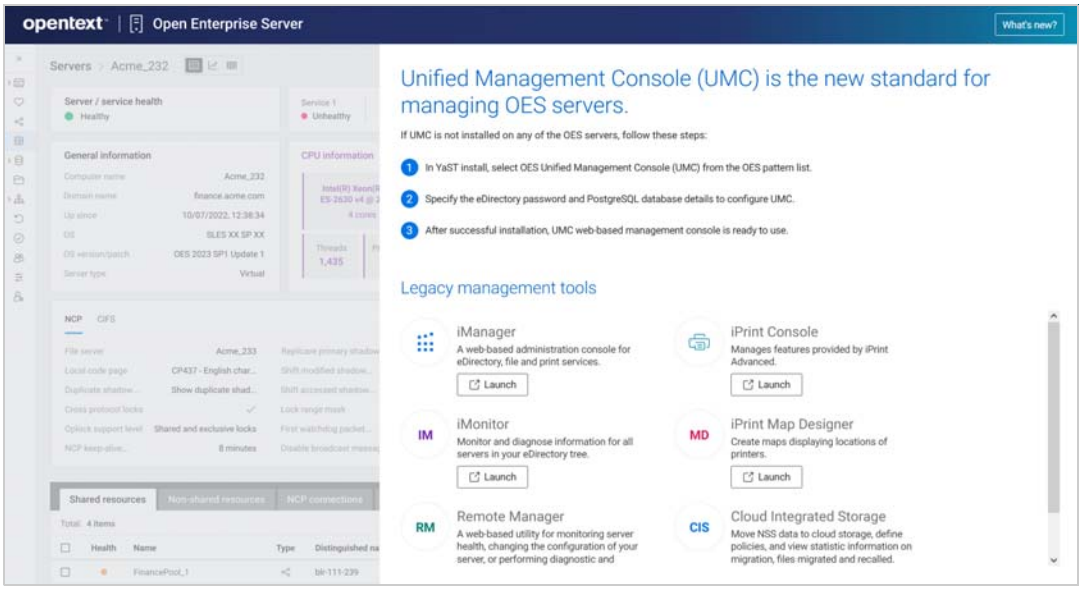
   `https://IP_or_DNS`

   Replace IP_or_DNS with the IP address or DNS name of your OES server and proceed.

The next page appears based on the following scenarios:

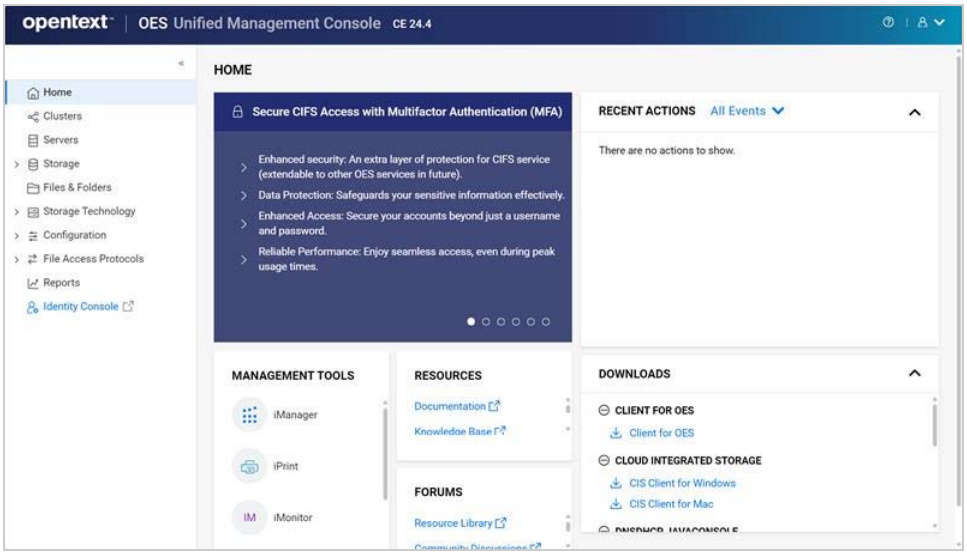
- **UMC pattern not installed**

  If UMC pattern is not installed, you are directed to the OES welcome page, which consists of the steps to install and configure UMC. Only **Legacy management tools** can be accessed from the OES welcome page. You can use the Application Delivery Marketplace (https://www.microfocus.com/marketplace/appdelivery) to download the client softwares.



- **UMC pattern installed**

  If UMC pattern is installed and configured, you are directed to the UMC login page. You can download the client softwares from the UMC home page or from the Application Delivery Marketplace.



  If you still want to access the OES welcome page after login to UMC, update the Address field as `https://<IP>/welcome`.

2. Continue with "What's Next (page 86)".

3.17 What's Next

After you complete the initial installation, complete any additional tasks you might need to perform. See “Completing OES Installation Tasks” on page 123.

4 Installing or Configuring OES Services on an Existing OES Server

After installing or upgrading to the latest OES version, you can also install additional services and configure them.

- Section 4.1, “Adding/Configuring OES Services on an Existing Server,” on page 87
- Section 4.2, “Adding/Configuring OES Services on a Server That Another Administrator Installed,” on page 89
- Section 4.3, “What's Next,” on page 90

IMPORTANT: If you have updated a server with a Support Pack, ensure that the installation source is pointing to the latest Support Pack media.

4.1 Adding/Configuring OES Services on an Existing Server

IMPORTANT: If you are not using the administrator account that originally installed the OES server you are adding services to, see Section 2.4, “Installing and Configuring OES as a Subcontainer Administrator,” on page 19 and then follow the instructions in Section 4.2, “Adding/Configuring OES Services on a Server That Another Administrator Installed,” on page 89.

To add/configure OES services on an existing OES server:

1. On the OES server, launch YaST, then click **Open Enterprise Server** > **OES Install and Configuration**.
2. On the Software Selection page, select the OES components that you want to install or configure.

   Services that you have already installed are indicated by a white tick mark on a black background in the status check box next to the service.

   IMPORTANT: You cannot uninstall an OES service by deselecting it. For more information about removing service functionality from the server, see Chapter 13, “Disabling OES Services,” on page 175.
3. If you are only configuring or reconfiguring services that are already installed, click **Accept**, then skip to Step 7.

   Not all OES components require eDirectory to be installed on the local server. Components that have a dependency on eDirectory being installed locally will prompt you to install eDirectory if it is not already installed.

IMPORTANT: If you need to reconfigure eDirectory, we recommend that you use tools provided by eDirectory, such as iMonitor or iManager, rather than using YaST to change the configuration. The configuration provided in YaST is only for the initial eDirectory installation and configuration.

If you need to reconfigure eDirectory and OES services due to database corruption, go to Chapter 14, "Reconfiguring eDirectory and OES Services," on page 177 and follow the instructions there.

4 After selecting the services to install, click **Accept**.

5 If package changes are required for your selections, select **Continue**.

6 Insert any media required to install the new packages.

7 Change the default configuration information as required.

In most cases, the default configuration is acceptable. You need to change the configuration at the following times:

- When the installation displays the following message to indicate that more information (often the administrator password) is required:

  service_name `service requires additional configuration information before continuing or disable the configuration.`

- When you want to change the default configuration settings, such as enabling services for LUM.
- When you want to reconfigure a service that has already been configured.

7a To change the configuration of a newly installed service or a service that has already been configured, change its configuration status to **Enabled**, then click the service heading link to access the configuration dialog box for that service.

Newly installed services that have not been configured have the status of `Configure is enabled`.

Services that have already been configured have a status of `Reconfigure is disabled`.

7b To enable the configuration status of any disabled service configuration, click the **Disabled** link to change the status to **Enabled**.

7c To delay the configuration of newly installed services to a later time, click the **Enabled** link to change the status to `Configure is disabled`.

For configuration guidelines, see Section 3.13.6, "Configuration Guidelines for OES Services," on page 63 or click a link below:

- Backup/Storage Management Services (SMS)
- Business Continuity Cluster (BCC)
- CIFS
- Cloud Integrated Storage (CIS)
- Clustering (NCS)
- DHCP
- DNS
- Domain Services for Windows (DSfW)
- eDirectory

- FTP
- iManager
- iPrint Advanced
- Linux User Management (LUM)
- NCP Server/Dynamic Storage Technology
- Pre-Migration Server
- Novell Remote Manager (NRM)
- Novell Storage Services
- Novell Storage Services AD Support
- Unified Management Console (UMC)

8 When all of the services have complete configuration information and the configuration or reconfiguration status is set to **Enabled** for the services that you want to configure, click **Next** to continue with the configuration process.

9 After the service configuration process has run and is finalized, click **Finish**.

4.2 Adding/Configuring OES Services on a Server That Another Administrator Installed

To add or configure OES services on an OES server that another administrator installed, you must have the rights described in "Rights Required for Subcontainer Administrators" on page 20.

1 On the OES server, launch YaST. Then click **Open Enterprise Server** > **OES Install and Configuration**.

2 On the Software Selection page, select the additional OES services you want to install, then click **Accept**.

The required packages are installed.

3 When the Open Enterprise Server Configuration summary screen appears, click the **disabled** link under **LDAP Configuration for Open Enterprise Services**.

The link changes to **enabled**.

4 Click **LDAP Configuration for Open Enterprise Services**.

5 Change the Admin Name and Context.

IMPORTANT: Ensure all field delimiters are consistent. For example, if you are adding to the context already displayed, either use comma-delimited syntax or change all other delimiters to periods.

---

6 Type the subcontainer admin password in the **Admin Password** field, then click **Next**.

7 Go to Step 7 on page 88 in Section 4.1, "Adding/Configuring OES Services on an Existing Server," on page 87 and continue from there.

4.3 What's Next

After you complete the configuration process, complete any additional tasks you might need to perform. See “Completing OES Installation Tasks” on page 123.

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 are kept intact. During the life cycle of the product, you can apply Service Packs to increase system security and correct software defects.

- Section 5.1, “Supported OES Upgrade Paths,” on page 91
- Section 5.2, “Planning for the Upgrade,” on page 92
- Section 5.3, “Meeting the Upgrade Requirements,” on page 93
- Section 5.4, “Upgrading OES,” on page 97
- Section 5.5, “Using AutoYaST for OES Upgrade,” on page 109
- Section 5.6, “Channel Upgrade from OES 24.3 to OES 24.4,” on page 112
- Section 5.7, “Upgrading Open Enterprise Server Using SUSE Manager,” on page 119
- Section 5.8, “Using ZENworks to Upgrade from OES 23.4 to OES 24.4 or later,” on page 120
- Section 5.9, “Verifying that the Upgrade was Successful,” on page 120
- Section 5.10, “What's Next,” on page 121

5.1 Supported OES 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 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.

5.2 Planning for the Upgrade

- Section 5.2.1, “Be Sure to Check the Release Notes,” on page 92
- Section 5.2.2, “Understanding the Implications for Other Products Currently Installed on the Server,” on page 92
- Section 5.2.3, “Upgrading the OES Cluster Nodes,” on page 92

5.2.1 Be Sure to Check the Release Notes

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

5.2.2 Understanding the Implications for Other Products Currently Installed on the Server

OES Server Upgrades: Non-OES Packages Are Retained but Might Not Work After Upgrading

During the upgrade process from supported upgrade paths to OES 24.4, packages that are not part of the OES distributions are automatically retained unless you select them for deletion.

This includes third-party products you have installed, as well as other products such as GroupWise, ZENworks, and Identity Manager.

There is no guarantee that these products will continue to work after you upgrade. Therefore, it is critical that you check the product documentation for compatibility information before you upgrade servers with any Micro Focus product installed.

Product	See This Documentation
GroupWise	GroupWise online documentation
ZENworks	ZENworks online documentation
Identity Manager	Identity Management online documentation
Other products	All Novell online documentation

If you have installed a third-party product, ensure that it is supported on OES and follow the upgrade instructions that should be included with it.

5.2.3 Upgrading the OES Cluster Nodes

If the autostart of OES Cluster Services or Business Continuity Clustering is enabled, you must disable autostart to prevent it from automatically loading the OES Cluster Services or Business Continuity Clustering during the upgrade.

To disable the service:

- Log in to the node as a root user, and open a terminal console.

- Perform `cluster leave` command to remove the node from the cluster.
- (Optional) Stop the Business Continuity Clustering by executing

  ```
  systemctl stop novell-bcc.service
  ```
- Stop the OES Cluster Services by executing

  ```
  systemctl stop novell-ncs.service
  ```
- (Optional) Disable the Business Continuity Clustering by executing

  ```
  systemctl disable novell-bcc.service
  ```
- Disable the OES Cluster Services by executing

  ```
  systemctl disable novell-ncs.service
  ```

NOTE: Post upgrade if the shared storage or SBD partition is unavailable on the machine, ensure they are available, and then restart NCS. SBD partition is not available as iscsi service is disabled post upgrade.

You can enable the iscsi service using `systemctl enable iscsi.service`.

- Enable the autostart of OES Cluster Services for the node by executing

  ```
  systemctl enable novell-ncs.service
  ```
- (Optional) Enable the autostart of Business Continuity Clustering for the node by executing

  ```
  systemctl enable novell-bcc.service
  ```
- Start OES Cluster Services by executing

  ```
  systemctl start novell-ncs.service
  ```
- (Optional) Start the Business Continuity Clustering by executing

  ```
  systemctl start novell-bcc.service
  ```

5.3 Meeting the Upgrade Requirements

Meet the following requirements before you upgrade and install any OES 24.4 components:

- Section 5.3.1, “Removing Identity Console,” on page 94
- Section 5.3.2, “Securing Current Data,” on page 94
- Section 5.3.3, “Ensuring That There Is Adequate Storage Space on the Root Partition,” on page 94
- Section 5.3.4, “Converting ReiserFS to Btrfs File System,” on page 95
- Section 5.3.5, “Preparing the Server You Are Upgrading,” on page 95
- Section 5.3.6, “Checking the Server’s DNS Name,” on page 95
- Section 5.3.7, “Ensuring That the Server Has a Server Certificate,” on page 95
- Section 5.3.8, “Changing the Mount Options Before an Upgrade,” on page 96
- Section 5.3.9, “Preparing an Installation Source,” on page 96
- Section 5.3.10, “Synchronizing the OES Configuration Information before Starting an Upgrade,” on page 96

5.3.1 Removing Identity Console

Beginning with OES 24.4, UMC Server pattern installs and configures the identity console. Ensure that you remove any existing identity console configuration from the OES Server prior to upgrade. For more information, see Deploying Identity Console as Docker Container.

5.3.2 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.

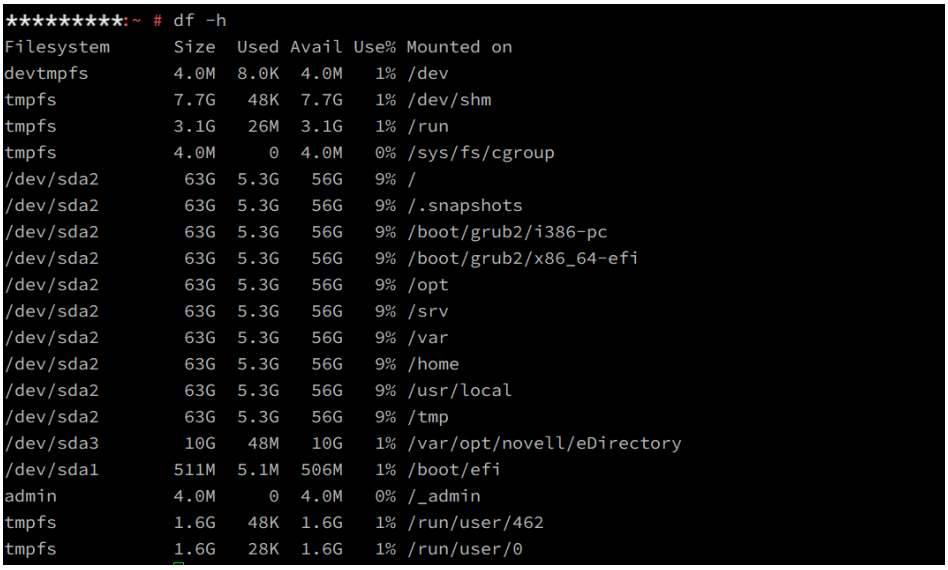
Save your configuration files. Copy all configuration files to a separate medium, such as a removable hard disk or USB stick, to secure the data. This primarily applies to files stored in `/etc` as well as some of the directories and files in `/var` and `/opt`. You might also want to write the user data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

5.3.3 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 56 GB available.



5.3.4 Converting ReiserFS to Btrfs File System

Beginning with SUSE Linux Enterprise 15, ReiserFS support is completely removed from YaST. The installer blocks the upgrade when it detects a ReiserFS file system. For more information, see SUSE Linux Enterprise Server 15 GA Release Notes.

Before migrating the system to OES 24.4, the existing data partitions formatted with ReiserFS must be converted to Btrfs.

5.3.5 Preparing the Server You Are Upgrading

Ensure that the server meets the hardware requirements for OES 24.4. See Section 2.2.2, “Server Hardware,” on page 18.

Itanium is not a supported platform for OES 24.4.

If the server is running supported source version, 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 23.4 using the instructions in this section, then apply all patches and verify services.

5.3.6 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
```

5.3.7 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**.

5.3.8 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 partitioner`.

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**.

6 Repeat Step 4 and Step 5 on page 96 for all the Linux partitions (not for NSS partitions).

7 After you have changed the mount options, click **Next**.

8 In the **Expert Partitioner: Summary** dialog box, click **Finish**.

The mount options are successfully changed.

5.3.9 Preparing an Installation Source

Review and complete the instructions for "Setting Up a Network Installation Source" on page 34. We recommend using the network installation option, especially if you are upgrading multiple servers.

5.3.10 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/sysconfig/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/sysconfig/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 or download the script from the OES documentation site. This script assumes that the respective OES service configuration 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/sysconfig/novell`, execute the `./oes_upgrade_check.pl all` command.
- To synchronize any particular OES service configuration information, for example LUM, with `/etc/sysconfig/novell/lum_oes2018`, execute the `./oes_upgrade_check.pl lum` command.

5.4 Upgrading OES

NOTE: If the OES Cluster Service (NCS) and Business Continuity Clustering (BCC) are configured on the node that is getting upgraded, stop the service before proceeding with Upgrade. See Upgrading the OES cluster node.

Use the following instructions to complete the upgrade applicable to the installation source you are using:

- Section 5.4.1, “Using Physical Media to Upgrade,” on page 98
- Section 5.4.2, “Specifying the Partition to Update,” on page 98
- Section 5.4.3, “Reviewing the Previously Used Repositories,” on page 99
- Section 5.4.4, “Specifying Customer Center Configuration Settings,” on page 99
- Section 5.4.5, “Specifying the Add-On Product Installation Information,” on page 101
- Section 5.4.6, “Verifying and Customizing the Update Options in Installation Settings,” on page 101
- Section 5.4.7, “Accepting the Installation Settings,” on page 103
- Section 5.4.8, “Specifying Configuration Information,” on page 103
- Section 5.4.9, “Participating in Product Improvement Consent Screen,” on page 107
- Section 5.4.10, “Finishing the Upgrade,” on page 107
- Section 5.4.11, “Migrating Clustered Linux Volume Resource from clvmd to lvmlockd,” on page 108

5.4.1 Using Physical Media to Upgrade

1. Ensure that the server meets the upgrade requirements. See “Meeting the Upgrade Requirements” on page 93.
2. Insert the OES 24.4 Install Media into the DVD drive of the server that you are upgrading to OES 24.4, then reboot the machine.
3. From the DVD boot menu, select **Upgrade**, then press Enter.

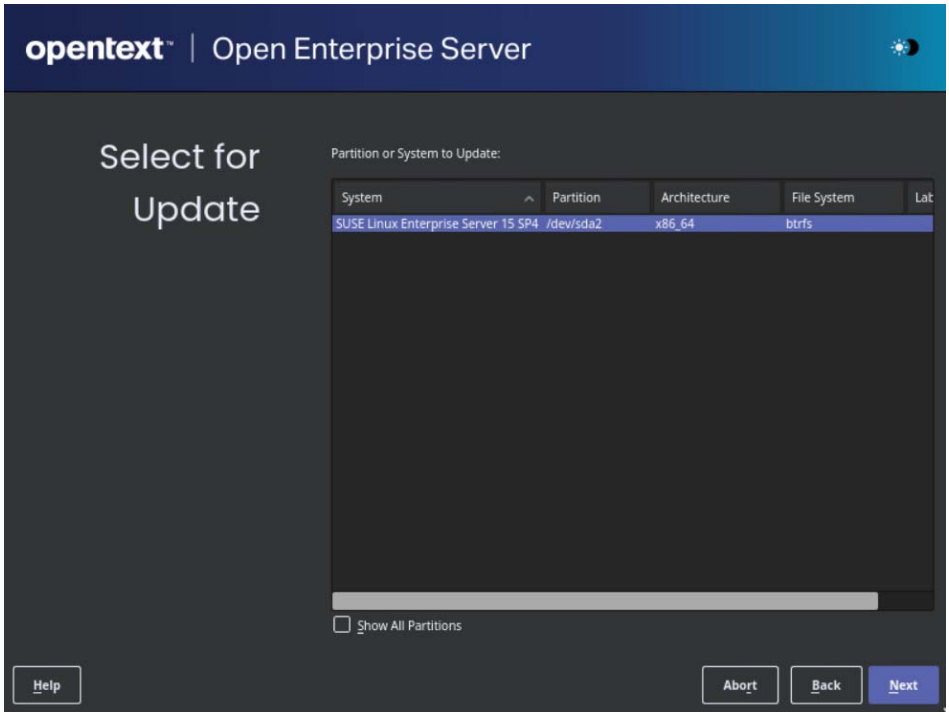
   For upgrading in text mode, from the DVD boot menu, select **Upgrade**, press F3, select **Text Mode**, then press Enter.
4. Select the language that you want to use, agree to the license terms, then click **Next**.
5. On the Network Settings page, click **Next**.
6. Follow the prompts, using the information contained in the following sections:
   - **6a** “Specifying the Partition to Update” on page 98.
   - **6b** “Reviewing the Previously Used Repositories” on page 99
   - **6c** “Specifying Customer Center Configuration Settings” on page 99
   - **6d** “Specifying the Add-On Product Installation Information” on page 101
   - **6e** “Verifying and Customizing the Update Options in Installation Settings” on page 101.
   - **6f** “Accepting the Installation Settings” on page 103.
   - **6g** “Specifying Configuration Information” on page 103.
   - **6h** “Finishing the Upgrade” on page 107.
7. Verify that the upgrade was successful. See the procedures in “Verifying that the Installation was Successful” on page 84.
8. Complete the server setup by following the procedures in “Completing OES Installation Tasks” on page 123.

5.4.2 Specifying the Partition to Update

YaST tries to determine the correct root (/) partition. If there are several possibilities, or if YaST can’t definitely determine the correct root partition, the Select for Update page displays.

1. If there is only one partition listed, click **Next**.
2. If there are several partitions, select the root partition you want to upgrade.
3. Click **Next**.

YaST mounts the selected partition and displays all repositories that have been found on the partition that you want to upgrade.



5.4.3 Reviewing the Previously Used Repositories

On the Previously Used Repositories page, all the previous OES and SLES repositories are marked for removal. Review and click **Next**.

5.4.4 Specifying Customer Center Configuration Settings

To receive support and updates for your OES server, you need to register it in the Customer Center. When the Customer Center Configuration page is displayed, you have two options:

- “Registering the Server Later” on page 99
- “Registering the Server During the Upgrade” on page 100

Ensure to configure the network settings using the **Network Configuration...** button on the top right corner of the Customer Center Configuration page before proceeding with registration.

Registering the Server Later

1. Click **Configure Later**.
2. Click **Next**.

Registering the Server During the Upgrade

NOTE: Registering an OES server updates it to the latest OES version.

1 On the Customer Center Configuration page, select all of the following options, then click **Next**.

Option	What it Does
Configure Now	Proceeds with registering this server and the OES product in the Customer Center.
Hardware Profile	Sends information to the Customer Center about the hardware that you are installing OES on.
Optional Information	Sends optional information to the Customer Center for your registration. For this release, this option doesn't send any additional information.
Registration Code	Makes the registration with activation codes mandatory.
Regularly Synchronize with the Customer Center	Keeps the installation sources for this server valid. It does not remove any installation sources that were manually added.

2 After you click **Next**, the Contacting server message is displayed. Wait until this message disappears and the Manual Interaction Required page displays.

3 On the Manual Interaction Required page, note the information that you will be required to specify, then click **Continue**.

4 On the Customer Center Registration page, specify the required information in the following fields, then click **Submit**:

- **Email Address:** The email address for your Login account.
- **Confirm Email Address:** The same email address for your Login account
- **Activation Code for OES Components (optional):** Specify your purchased or 60-day evaluation registration code for the OES product.

  If you don't specify a code, the server cannot receive any updates or patches.
- **System Name or Description (optional):** The hostname for the system is specified by default.

  If you want to change this to a description, for the Customer Center, specify a description to identify this server.

5 When the message to complete the registration displays, click **Continue**.

6 After you click **Continue**, the Contacting server.. message is displayed with the Manual Interaction Required page. Wait until this message disappears and the Customer Center Configuration page displays with the message: `Your configuration was successful`.

7 When you see the message `Your configuration was successful` on the dialog box, click **Ok**.

8 Click **Next**.

9 Continue with "Specifying the Add-On Product Installation Information" on page 101.

5.4.5 Specifying the Add-On Product Installation Information

On the Add-On Product Installation page, you can add the add-on products you want that are supported on OES 24.4.

If you do not want to add any add-on products with OES 24.4, click **Next** to continue with "Verifying and Customizing the Update Options in Installation Settings" on page 101.

5.4.6 Verifying and Customizing the Update Options in Installation Settings

---

IMPORTANT: To verify that previously installed services are selected for installation and to install any additional OES services during the upgrade, you must customize the Update Options on the Installation Settings page.

To verify or customize the software packages that are installed on the server:

1. On the Installation Settings page, click on **Packages**.
2. All of the OES Services patterns that were previously installed are selected by default.

   Ensure that the patterns for the services you are upgrading are selected, then select the patterns for any new OES Services that you might want to also install.

   A description displays to the right of a pattern when the pattern is selected. For a description of OES Services patterns and the components selected with each pattern, see Table 2-4 on page 26.

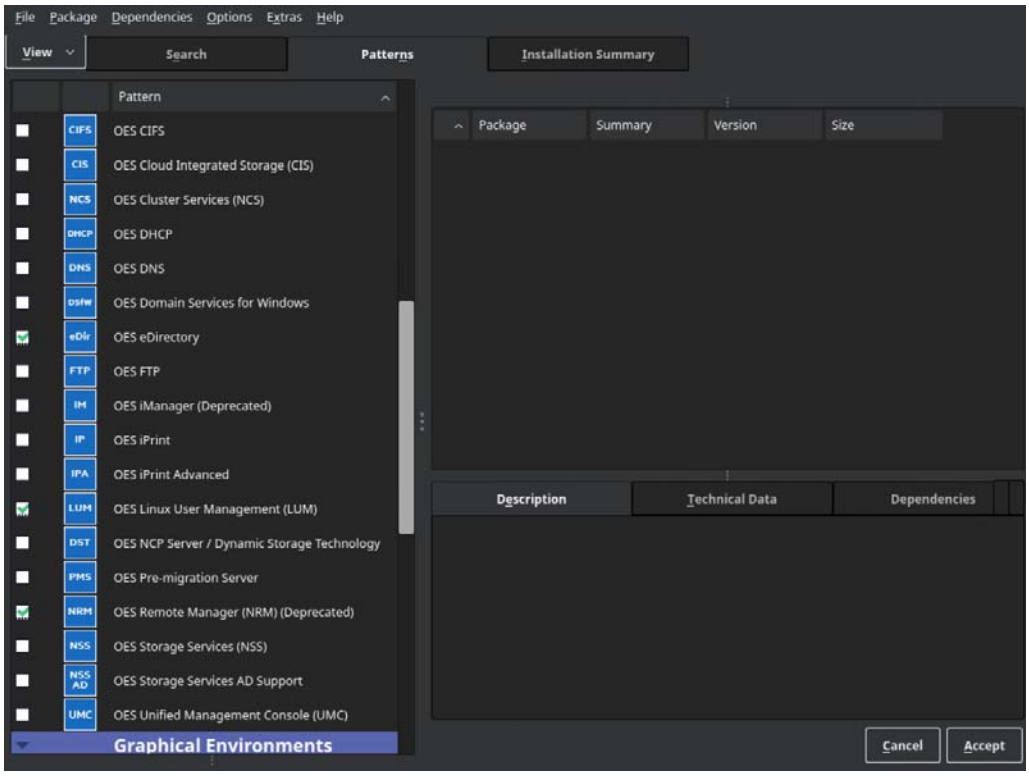
   IMPORTANT: If you deselect a pattern after selecting it, you are instructing the installation program to not install that pattern and all of its dependent patterns. Rather than deselecting a pattern, click **Cancel** to cancel your software selections, then click the **Select Patterns** heading again to choose your selections again.

   Selecting only the patterns that you want to install ensures that the patterns and their dependent patterns and packages are installed.

   If you click **Accept** and then return to software pattern selection page, the selections that you made become your base selections and must be deselected if you want to remove them from the installation proposal.

   Attempting to uninstall a service by deselecting its pattern is not recommended. For more information, see Chapter 13, "Disabling OES Services," on page 175.

   Selecting a pattern automatically selects the other patterns that it depends on to complete the installation.



3 If you want to see the details of your selections, click **Details...**.

4 When you have the software components selected that you want to install, click **Accept**.

5 When the notification about deleting unmaintained packages appears, click **OK**.

6 (Conditional) If the prompt for **Automatic Changes** displays, click **Continue**.

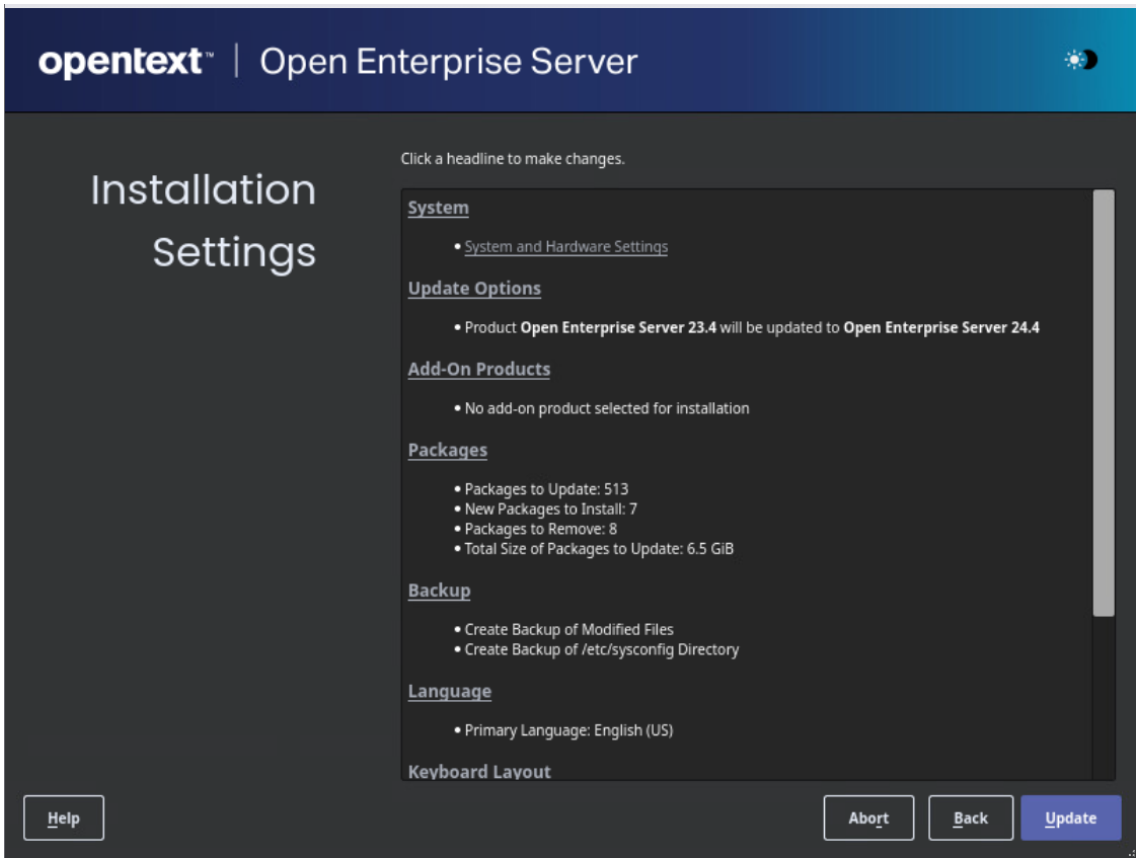
7 (Conditional) If you are prompted to resolve any dependency conflicts, resolve them.

8 If the Update Options page displays again, click **OK**.

9 On the Installation Settings page, ensure the following are listed under the **Update Options**:

Product **Open Enterprise Server *<earlier version number>*** will be updated to **Open Enterprise Server 24.4**

Proceed with Section 5.4.7, “Accepting the Installation Settings,” on page 103.



10 If you see package conflict errors (red text under the **Packages** link), refer to the *Release Notes* for resolution instructions.

11 Continue with "Accepting the Installation Settings" on page 103.

5.4.7 Accepting the Installation Settings

1 Review the final Installation Settings page to ensure that you have all the Installation settings you desire. Ensure that the page shows all the OES Services that you want to update and install.

2 After you have changed all the installation settings as desired, click **Update**.

3 In the Confirm Update dialog box, click **Start Update**.

The base installation settings are applied and the packages are installed.

4 After the server reboots, continue with "Specifying Configuration Information" on page 103.

5.4.8 Specifying Configuration Information

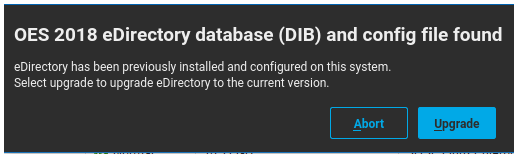
When the server reboots, you are required to complete the following configuration information:

- "Upgrading eDirectory" on page 104
- "Specifying LDAP Configuration Settings" on page 104
- "Configuring Open Enterprise Server Services" on page 105

Upgrading eDirectory

OES Version	eDirectory Version
OES 23.4, OES 24.1	9.2.8
OES 24.2, OES 24.3, OES 24.4	9.2.9

1 When the following dialog box appears, click **Upgrade**.



NOTE: If you are upgrading from OES 2018 SP3, this dialog will show that the OES 2018 eDirectory database (DIB) and config file were found.

2 On the eDirectory Upgrade - Existing Server Information page, type the **Admin password**, then click **Next**.

3 On the Novell Modular Authentication Service page, click **Next**.

4 Continue with "Specifying LDAP Configuration Settings" on page 104.

Specifying LDAP Configuration Settings

Many of the OES services require eDirectory. If eDirectory was not selected as a product to upgrade or install but other OES services that do require LDAP services were installed, the LDAP Configuration service displays so that you can complete the required information.

1 In the **eDirectory Tree Name** field, specify the name for the existing eDirectory tree that you are installing this server into.

2 In the **Admin Name and Context** field, specify the name and context for user Admin on the existing tree.

3 In the **Admin Password Name** field, specify a password for user Admin on the existing tree.

4 Add the LDAP servers that you want the services on this server to use. The servers that you add should hold the master or a read/write replica of eDirectory. Do the following for each server you want to add:

4a Click **Add**.

4b In the next dialog box, specify the following information for the server to add, then click **Add**:

- Server IP Address
- LDAP port
- Secure LDAP port

4c Click **Add**.

4d (Optional) Repeat Step 4a through Step 4c to add additional servers.

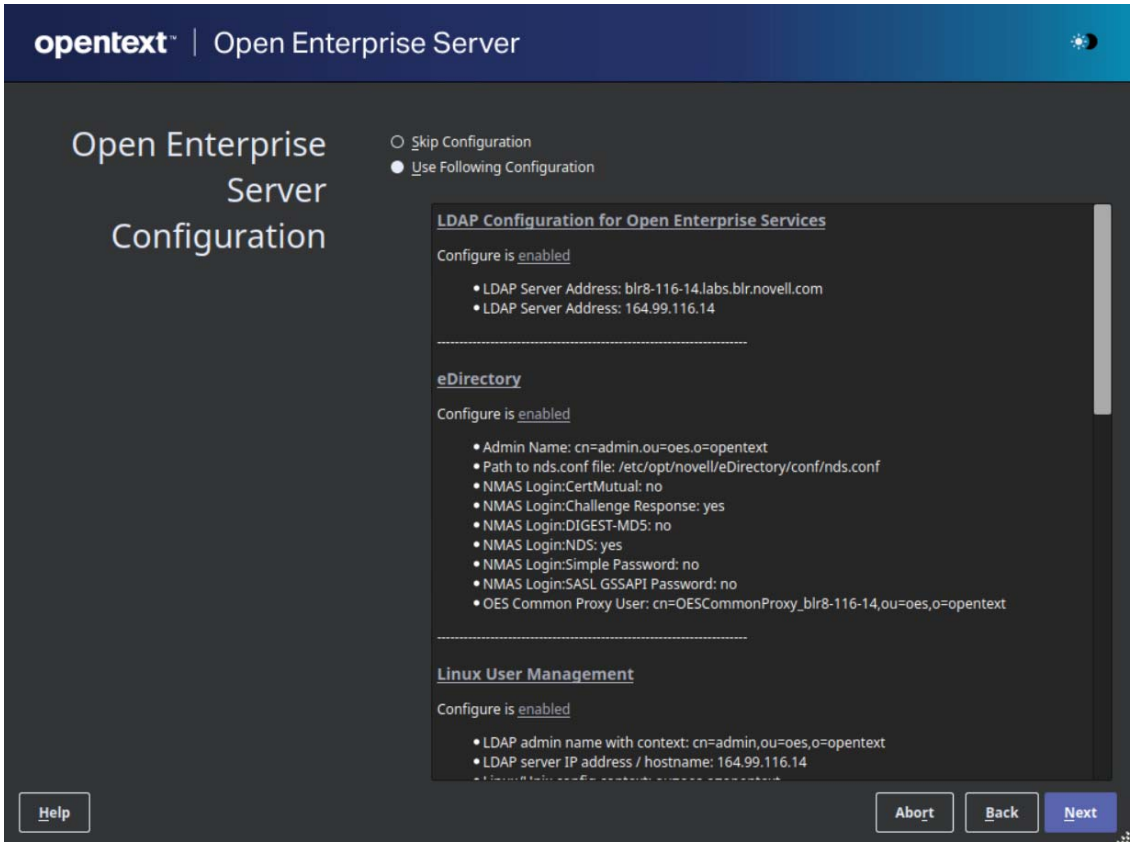
5 When all the LDAP servers that you want to specify are listed, click **Next**.

6 Continue with "Configuring Open Enterprise Server Services" on page 105.

Configuring Open Enterprise Server Services

After you complete the LDAP configuration or eDirectory configuration, the **Open Enterprise Server Configuration** summary page is displayed, showing all the OES components you updated and installed and their configuration settings.

1 Review the setting for each component and click the component heading to change any settings.



When you specify the configuration information for OES services, see the information in "Configuration Guidelines for OES Services" on page 63, or click a link below:

- Backup/Storage Management Services (SMS)
- Business Continuity Cluster (BCC)
- CIFS
- Cloud Integrated Storage (CIS)
- Clustering (NCS)
- DHCP
- DNS
- Domain Services for Windows (DSfW)

- eDirectory
- FTP
- iManager
- iPrint Advanced
- Linux User Management (LUM)
- NCP Server/Dynamic Storage Technology
- Pre-Migration Server
- Novell Remote Manager (NRM)
- Novell Storage Services
- NSS Active Directory Support
- Unified Management Console (UMC)

2 When you are satisfied with the settings for each component, click **Next**.

3 When you confirm the OES component configurations, you might receive the following error:

```
The proposal contains an error that must be resolved before continuing.
```

If this error is displayed, check the summary list of configured products for any messages immediately below each product heading. These messages indicate products or services that need to be configured. If you are running the YaST graphical interface, the messages are red text. If you are using the YaST text-based interface, they are not red.

For example, if you selected Linux User Management in connection with other OES products or services, you might see a message similar to the following:

```
Linux User Management needs to be configured before you can continue or
disable the configuration.
```

If you see a message like this, do the following:

3a On the summary page, click the heading for the component.

3b Supply the missing information in each configuration page.

When you specify the configuration information for OES services during the upgrade, see the information in "Configuration Guidelines for OES Services" on page 63.

When you have finished the configuration of that component, you are returned to the Novell Open Enterprise Server Configuration summary page.

3c If you want to skip the configuration of a specific component and configure it later, click **Enable**d in the **Configuration is enabled** status to change the status to **Configuration is disabled**.

If you change the status to **Configuration is disabled**, you must configure the OES components after the installation is complete. See "Installing or Configuring OES Services on an Existing OES Server" on page 87.

4 After resolving all product configuration problems, click **Next** to proceed with the configuration of all services and installation of iManager plug-ins.

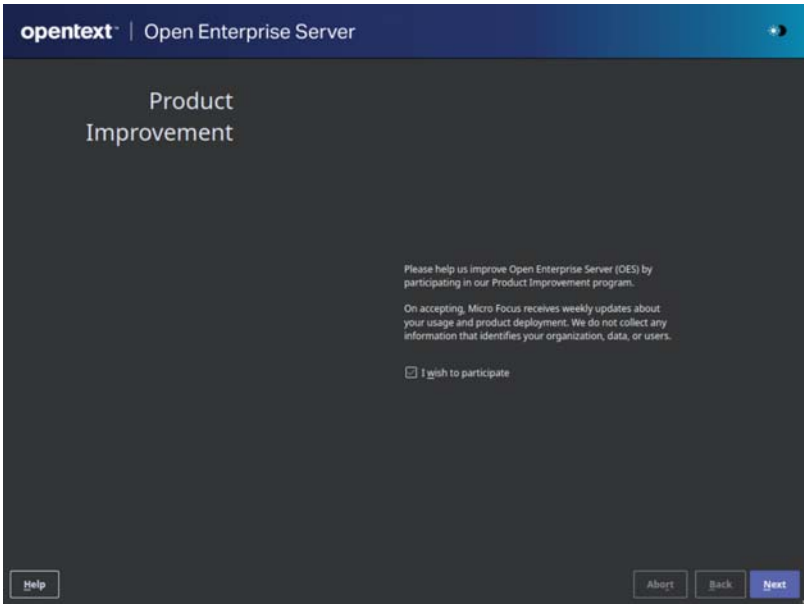
5 When the Readme page displays, click **Next** and continue with Section 5.4.10, "Finishing the Upgrade," on page 107.

5.4.9 Participating in Product Improvement Consent Screen

Telemetry enables 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 Micro Focus server.

Select the checkbox to participate in the program. All the servers in the same context as this server are automatically enabled for telemetry and this screen is not displayed to other servers in that context.

Figure 5-1 *Product Improvement*



How the Micro Focus Server Receives the Data

After the weekly collection, the data is stored at /var/opt/novell/telemetry/data/ on the OES server that was configured with this program. The OES server transfers the data to the Micro Focus 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.

5.4.10 Finishing the Upgrade

After a successful configuration, YaST shows the Installation Completed page.

1. Deselect **Clone This System for AutoYaST**. Cloning is selected by default.

   This increases the speed of finishing the installation update.

   AutoYaST is a system for automatically installing one or more SUSE Linux Enterprise systems without user intervention. Although you can create a profile from a system that has been upgraded, it does not work to upgrade a similar system.
2. Finish the upgrade by clicking **Finish** on the Installation Completed page.

5.4.11 Migrating Clustered Linux Volume Resource from clvmd to lvmlockd

Beginning with OES 24.4, clustered Linux volume (LV) uses the lvmlockd instead of clvmd as it is deprecated.

Without performing the following step, if the clustered linux volume is migrated to OES 24.4 the clustered Linux volume resources will go to comatose state.

Migrating clustered Linux volume resource from `clvmd` to `lvmlockd` consists of the following steps:

1. Changing the `clvmd` resource to local resource.
2. Changing the clustered Linux volume to use `lvmlockd` from `clvmd`.

NOTE: After performing the above steps, if the clustered Linux volume is migrated to previous OES version node, then the clustered Linux volume resources will go to comatose state.

Changing clvmd Resource to Local Resource

You must perform the following steps on a node where cluster resource is running:

1. Ensure the `clvmd` resource is not running on any node. For more information, see Onlining and Offlining (Loading and Unloading) Cluster Resources from a Cluster Node.
2. Change the clustered volume group (VG) to a local VG.

   ```
   vgchange -cn <vgname>
   ```

Changing Clustered Linux Volume to use lvmlockd from clvmd

1. Ensure the `clvmd` or clustered VG to a local VG.

   ```
   vgchange --lock-type none --lock-opt force <vgname>
   ```

   CAUTION: This command is only safe if all the nodes have stopped using the VG.

   ---

2. Deactivate the logical volume on OES 24.4 server.

   ```
   lvchange -an <lvname/vgname>
   ```

3. Change a local VG to a shared VG.

   ```
   vgchange --config "global/use_lvmlockd=1" --locktype sanlock --lockopt skipgl <vgname>
   ```

   If this command succeeds, go to Step 6.

4. If Step 3 fails with an error "`Volume group "VGNAME" has insufficient free space (0 extents): 64 required`" then complete the following:

   a. Activate the logical volume.

      ```
      lvchange -ay <lvname/vgname>
      ```

   b. Resize the volume using `lvreduce` command.

Example: `lvreduce --resizefs -L <new volume size> <vgname>`

c. Deactivate the logical volume.

```
lvchange -an <lvname/vgname>
```

5. Repeat Step 3 if you have executed Step 4.
6. Update the load and unload script for the clustered resource.
   a. Add the following command in cluster load script before activating the volume group:

```
ignore_error vgchange --lock-start $VOLGROUP_NAME
```

Example

```
# activate lvm-lock on volume
ignore_error vgchange --lock-start $VOLGROUP_NAME
# activate the volume group
exit_on_error vgchange -a ey $VOLGROUP_NAME
```

   b. Add the following command in cluster unload script after deactivating the volume group:

```
ignore_error vgchange --lock-stop $VOLGROUP_NAME
```

Example

```
# deactivate the volume group
exit_on_error vgchange -a en $VOLGROUP_NAME # deactivate lock on volumes
ignore_error vgchange --lock-stop $VOLGROUP_NAME
```

7. Make the cluster resource available on the OES 24.4 server.

```
cluster online <resource name>
```

5.5 Using AutoYaST for OES Upgrade

If you are a system administrator who needs to upgrade different versions of multiple OES servers, it can be time-consuming and inconvenient to repeat the process of swapping installation discs and providing necessary upgrade information. You can now use AutoYaST to upgrade an existing OES server to the latest OES version with no user intervention.

IMPORTANT: Information provided in this section is critical. Failing to meet the prerequisites and follow the procedures as outlined might result in loss of data or the OES server becoming unrecoverable. Before performing these procedures in a live environment, we strongly recommend that you try them in a test environment to become familiar with the unattended upgrade process.

- Section 5.5.1, “Prerequisites,” on page 110
- Section 5.5.2, “Creating an Answer File to Provide the eDirectory and DSfW Passwords,” on page 110
- Section 5.5.3, “Upgrading OES,” on page 111
- Section 5.5.4, “Upgrading OES on a XEN Host Server,” on page 111
- Section 5.5.5, “Troubleshooting an AutoYaST Upgrade,” on page 112

5.5.1 Prerequisites

- Identify the server that you want to upgrade, and ensure that the latest patches are applied before starting the upgrade. Ensure that you meet all the OES 24.4 upgrade requirements specified in Section 5.3, “Meeting the Upgrade Requirements,” on page 93.
- Ensure that you have the eDirectory replica server IP address and eDirectory credentials.
- Ensure that the replica server is reachable over the network.
- Ensure that the correct eDirectory replica server's IP address is present in the eDirectory install configuration file at `/etc/sysconfig/novell/` as shown below:

  `CONFIG_EDIR_REPLICA_SERVER="<specify the eDirectory Replica IP>"`
- Create an answer file that provides the eDirectory password. For more information, see Section 5.5.2, “Creating an Answer File to Provide the eDirectory and DSfW Passwords,” on page 110.

5.5.2 Creating an Answer File to Provide the eDirectory and DSfW Passwords

During an AutoYaST upgrade, the system requires user input only to provide the eDirectory and DSfW passwords. This intervention can be eliminated with the help of an answer file.

WARNING: During the answer file creation, no validation is performed on the passwords you enter. If the wrong password is entered, the upgrade will fail and the server that you are upgrading will become unrecoverable.

To create an answer file, use any one of the following methods:

Directly Generating the Answer Key File

1. Log in to your machine as a `root` user and execute the following command:

   OES 2018 or later:

   `yast2 /usr/share/YaST2/clients/create-answer-file.rb <eDirectory password> [<DSfW Administrator Password for a DSfW server upgrade>]`

   NOTE: This method is not recommended because the passwords are stored in the `y2log` file in clear text.

Exporting the Passwords to Variables

1. In the terminal window, type the following commands:
   - `export OES_EDIR_DATA=<specify eDirectory Administrator Password>`
   - `export OES_DSFW_DATA=<specify the DsfW Administrator Password for a DsfW server upgrade>`
   - `yast2 /usr/share/YaST2/clients/create-answer-file.rb`

Using the GUI

1 In the terminal window, type the following command:

```
yast2 /usr/share/YaST2/clients/create-answer-file.rb
```

2 In the YaST2 dialog, provide the eDirectory and DSfW passwords, then click **OK**.

NOTE: DSfW password should be specified only if you are upgrading a DSfW server.

Once you have successfully generated the answer key file using any of the above stated methods, copy it from the current working directory to `/opt/novell/oes-install/`. For example, `cp answer /opt/novell/oes-install/`.

TIP: To invoke help for creating the answer key file, in the terminal window, type `yast2 /usr/share/YaST2/clients/create-answer-file.rb --help`.

5.5.3 Upgrading OES

Ensure that you have met all the requirements listed in Section 5.5.1, “Prerequisites,” on page 110.

1 Use the integrated ISO (OES24.4-x86_64-DVD1.iso) to boot the supported machine that you want to upgrade.

2 In the installation screen, select **Install**, and specify the following information in the **Boot Options**:

```
autoupgrade=1 autoyast=file:///autoupgrade.xml
```

If your server is using a different keyboard or is installed in a different language or supports multiple languages, then you will need to adjust the keyboard and language sections of the control file. For more information, see Server Upgrade Using AutoYaST.

3 Press Enter.

The upgrade proceeds without any user intervention.

NOTE: No tags are available for Product Improvement (telemetry) through AutoYaST.

5.5.4 Upgrading OES on a XEN Host Server

Ensure that you have met all the requirements listed in Section 5.5.1, “Prerequisites,” on page 110.

1 Shut down the guest machine.

2 Open the guest machine's XML file at `/etc/xen/vm`, delete the boot loader entry, then save the file.

3 Use the following command to delete the guest machine:

```
xm delete <guest machine>
```

4 Use the following command to start the virtual manager GUI:

```
vm-install --vm-settings /etc/xen/vm/<guest>.xml --os-type sles15 --os-
settings http://<the web server IP>/download/autoupgrade.xml
```

5 In the Operating System Installation screen, select the appropriate SLES 15 options as shown in the following image.

By default, the `autoupgrade.xml` path is populated for the AutoYaST file.

NOTE: If you choose to upgrade using an ISO, in the **Virtual Disk**, select the path where the integrated ISO exists. If you choose to upgrade using a URL, specify the HTTP path where the integrated installation source exists in **Network URL**.

6 In the **Additional Arguments** text box, specify the parameter information for the host IP, gateway IP, and netmask.

For example:

```
autoupgrade=1 netsetup=hostip hostip=192.168.1.1 netmask=255.255.254.0
gateway=192.168.1.254
```

7 Click **Apply**.

The upgrade proceeds without any user intervention.

5.5.5 Troubleshooting an AutoYaST Upgrade

- "Providing the Correct eDirectory and DSfW Administrator Password" on page 112
- "Unattended Upgrade Scenarios That Require User Input" on page 112

Providing the Correct eDirectory and DSfW Administrator Password

There is no validation for the passwords that you enter while creating the `answer` file. If you do not specify the correct passwords, the upgrade will not be successful and the server that you are upgrading will become unrecoverable.

For a Domain Services for Windows (DSfW) server upgrade, specify the DSfW Administrator password after the eDirectory password. For more information, see Section 5.5.2, "Creating an Answer File to Provide the eDirectory and DSfW Passwords," on page 110

Unattended Upgrade Scenarios That Require User Input

If you have not created the `answer` file, you will be prompted for the eDirectory and DSfW administrator passwords.

If the eDirectory replica server's IP address is not present in the eDirectory install configuration file (for OES 2018 SP2, it is `edir_oes2018_sp2`) at `/etc/sysconfig/novell/`, you will be prompted for the same. For more information, see Section 5.5.1, "Prerequisites," on page 110.

5.6 Channel Upgrade from OES 24.3 to OES 24.4

- Section 5.6.1, "Channel Upgrade from OES 24.3 to OES 24.4 via Wagon," on page 113
- Section 5.6.2, "Channel Upgrade from OES 24.3 to OES 24.4 using Zypper," on page 116

- Section 5.6.3, “Upgrading OES 24.3 to OES 24.4 using Subscription Management Tool (MFSMT),” on page 117
- Section 5.6.4, “Rolling back the Server in the Middle of a Wagon-based Channel Upgrade,” on page 118

IMPORTANT: Stop OES Cluster service (NCS) on the node that is getting upgraded before proceeding with Channel Upgrade.

5.6.1 Channel Upgrade from OES 24.3 to OES 24.4 via Wagon

1. Register the OES 23.4 server with Micro Focus Customer Center using the following command:

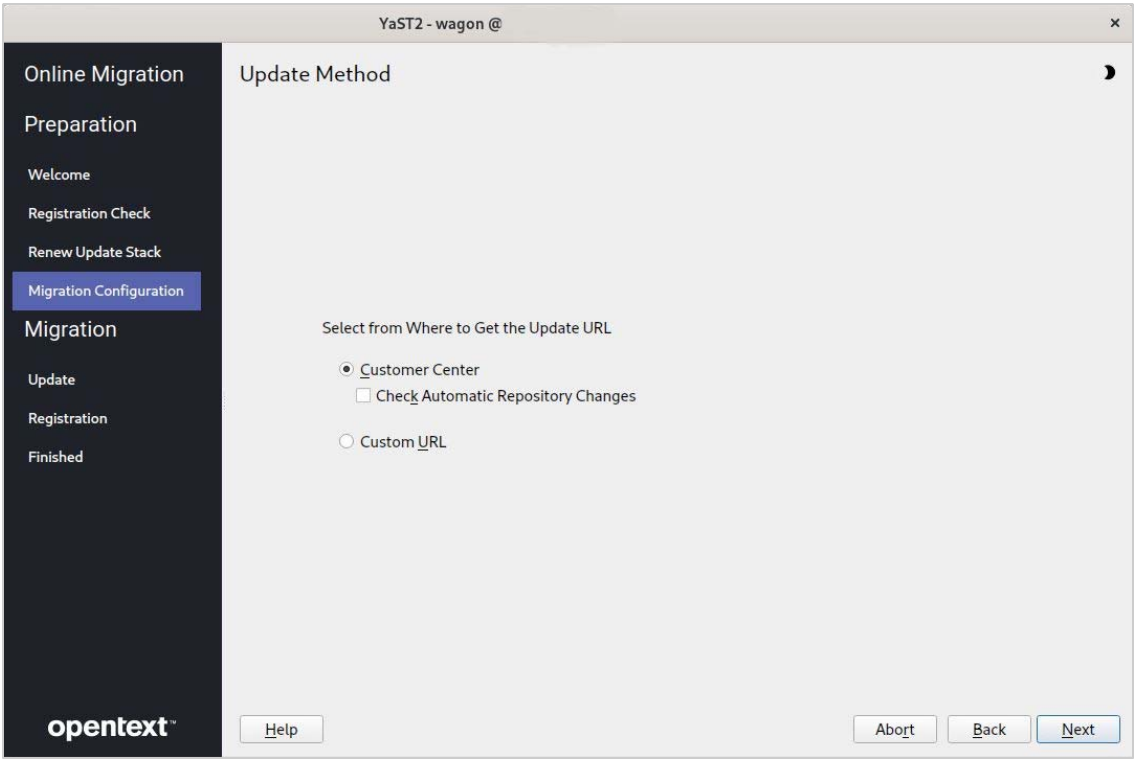
   ```
   suse_register -a email=<Email-Address> -a regcode-oes=<OES-activation-key> -L /root/.suse_register.log
   ```

2. Run the `zypper lr` command to ensure that OES23.4-Pool, OES23.4-SLE-Module-Basesystem15-SP4-Pool, OES23.4-SLE-Module-Basesystem15-SP4-Updates, OES23.4-SLE-Module-Containers15-SP4-Pool, OES23.4-SLE-Module-Containers15-SP4-Updates, OES23.4-SLE-Module-Desktop-Applications15-SP4-Pool, OES23.4-SLE-Module-Desktop-Applications15-SP4-Updates, OES23.4-SLE-Module-Server-Applications15-SP4-Pool, OES23.4-SLE-Module-Server-Applications15-SP4-Updates, OES23.4-SLE-Product-SLES15-SP4-Pool, OES23.4-SLE-Product-SLES15-SP4-Updates, and OES23.4-Updates catalogs are subscribed and enabled.

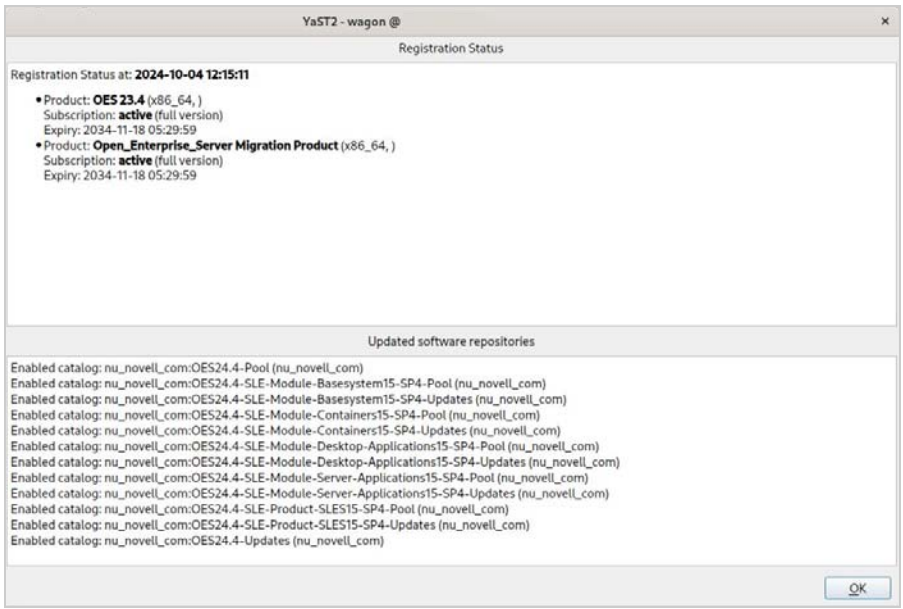
3. Apply all the available patches either using `zypper patch` or `yast2 online_update`. In the list of available patches, ensure that the `Enable update to OES 24.4` is selected. If this patch is not installed, you cannot proceed with the upgrade.

   NOTE: If the patching requires a server reboot, do so when notified by the system.

4. Start the wagon upgrade module using the `yast2 wagon` command.
5. On the welcome screen, click **Next**.
6. In Registration Check screen, click **Run Registration** if the “System not Registered” warning is displayed.
7. The Run Registration redirects to the Micro Focus Customer Center screen and click **Next.** Wagon does a sync and pops up a message stating that the software repositories need not be changed. This happens as there are no updates at this stage.
8. In the Registration Check screen, ensure that the registration summary displays “**Open Enterprise Server 23.4** has a valid registration”. If the valid registration message is displayed, click **Next,** and it resets the package manager.
9. In the Update Method screen, select **Customer Center > Next**.



10 The NCC screen is displayed again. Click **Next**, and it does a sync and pops up a message stating that the configuration is successful. Click **Details** and ensure that the following repositories are enabled as shown in the following figure.



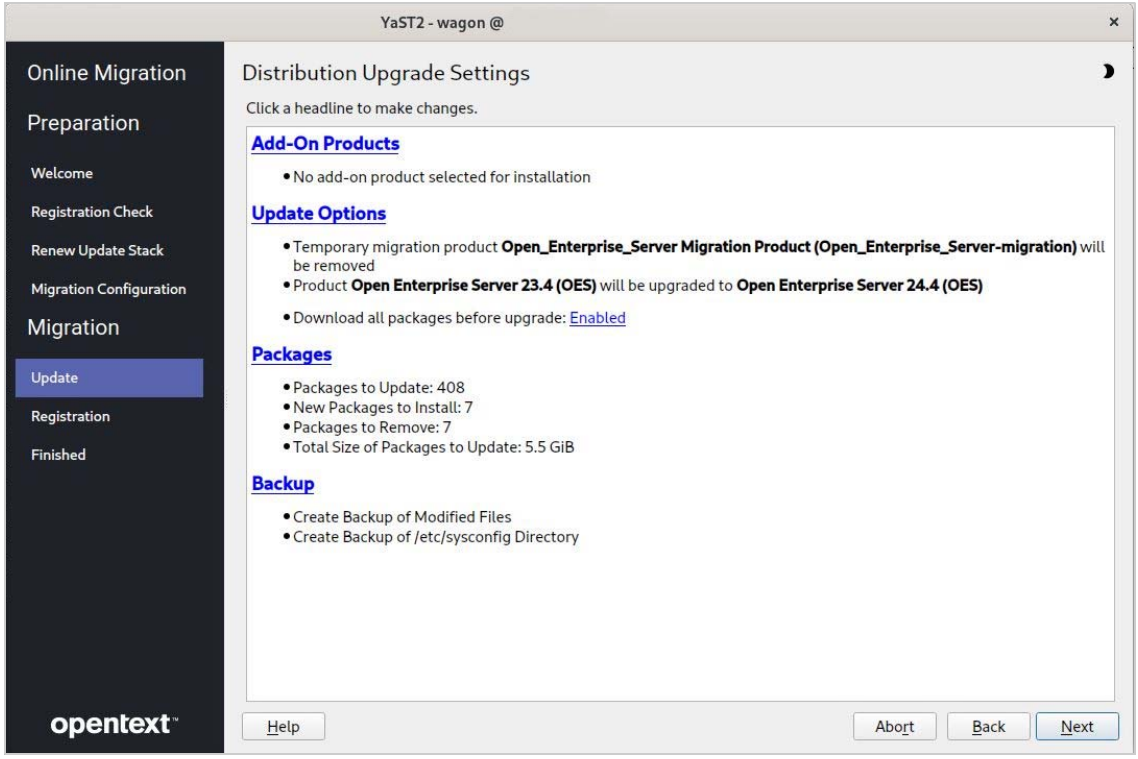
NOTE: If the repositories are not enabled, click **Back > Next** and redo the Micro Focus Customer Center registration until it is successful. If you are not able to do a successful Micro Focus Customer Center registration after multiple attempts, abort the process and roll back the server. For more information, see Section 5.6.4, “Rolling back the Server in the Middle of a Wagon-based Channel Upgrade,” on page 118.

11 In the Distribution Upgrade Settings screen, you must see the following content under the **Update Options** section.

- Temporary migration product Open_Enterprise_Server Migration Product (Open_Enterprise_Server-migration) will be removed.
- Product Open Enterprise Server 24.4 (Open_Enterprise_Server) will be upgraded to the latest OES version.

WARNING: If **Product Open Enterprise Server 23.4 (Open_Enterprise_Server) will be upgraded to Open Enterprise Server 24.4 (Open_Enterprise_Server)** is not displayed, click **Abort** and roll back the server.

NOTE: In the following screen shot, the number of packages to be updated may vary based on the patterns selected.



IMPORTANT: After clicking **Start Upgrade**, you cannot revert the server to its old state.

12 Click **Next > Start update** and continue with the upgrade. Once the upgrade is complete, a pop up is displayed informing about a server reboot; click **OK** and continue with the upgrade.

13 The Micro Focus Customer Center screen is displayed once again, wherein the registration of the final product is triggered. Click **Next**.

14 At the final **Migration Completed** dialog, click **Reboot** to reboot the server and proceed with OES service configuration.

15 After the reboot, system will prompt for eDirectory or DSFW password if the answer file is not created. Provide the password and continue. For more information on creating the answer file, see Section 5.5.2, “Creating an Answer File to Provide the eDirectory and DSfW Passwords,” on page 110.

16 A Program Improvement screen is displayed if this is the first server that is upgrading to OES 24.4. For more information, see Section 3.14, “Product Improvement,” on page 83.

5.6.2 Channel Upgrade from OES 24.3 to OES 24.4 using Zypper

1 Register the OES 23.4 server with Micro Focus Customer Center using the `suse_register -a email=<Email-Address> -a regcode-oes=<OES-activation-key> -L /root/.suse_register.log` command.

2 Run the `zypper lr` command to ensure that OES23.4-Pool, OES23.4-SLE-Module-Basesystem15-SP4-Pool, OES23.4-SLE-Module-Basesystem15-SP4-Updates, OES23.4-SLE-Module-Containers15-SP4-Pool, OES23.4-SLE-Module-Containers15-SP4-Updates, OES23.4-SLE-Module-Desktop-Applications15-SP4-Pool, OES23.4-SLE-Module-Desktop-Applications15-SP4-Updates, OES23.4-SLE-Module-Server-Applications15-SP4-Pool, OES23.4-SLE-Module-Server-Applications15-SP4-Updates, OES23.4-SLE-Product-SLES15-SP4-Pool, OES23.4-SLE-Product-SLES15-SP4-Updates, and OES23.4-Updates catalogs are subscribed and enabled.

3 Run the `zypper refresh` command.

4 Run the `zypper patch` command to install all the available updates for OES 23.4. Ensure that the **Enable update to OES 24.4** patch is installed. If this patch is not installed, you cannot proceed with the upgrade.

NOTE: If the patching requires a server reboot, do so when intimated by the system.

---

5 Run the `zypper pd` command to ensure that the Open_Enterprise_Server-migration is listed but not installed. To check the products installed, run `zypper pd -i` command.

6 The installed products contain information about the distribution upgrades and the migration products that should be installed to perform the migration. Use the `zypper se -t product | grep -h -- "-migration" | cut -d\| -f2` command.

A sample output is as follows:

```
Open_Enterprise_Server-migration
```

7 Install these migration products using the command `zypper in -t product Open_Enterprise_Server-migration`

8 Run the `suse_register -L /root/.suse_register.log` command to register the products and to get the corresponding repositories.

9 Run the `zypper ref -s` command to refresh services and repositories.

10 Check the repositories using the `zypper lr` command. It should list OES24.4-Pool, OES24.4-SLE-Module-Basesystem15-SP4-Pool, OES24.4-SLE-Module-Basesystem15-SP4-Updates, OES24.4-SLE-Module-Containers15-SP4-Pool, OES24.4-SLE-Module-Containers15-SP4-Updates, OES24.4-SLE-Module-Desktop-Applications15-SP4-Pool, OES24.4-SLE-Module-Desktop-Applications15-SP4-Updates, OES24.4-SLE-Module-Server-Applications15-SP4-Pool, OES24.4-

SLE-Module-Server-Applications15-SP4-Updates, OES24.4-SLE-Product-SLES15-SP4-Pool, OES24.4-SLE-Product-SLES15-SP4-Updates, and OES24.4-Updates repositories, and they should be enabled.

11 Perform a distribution upgrade using the `zypper dup --from OES24.4-Pool --from OES24.4-SLE-Module-Basesystem15-SP4-Pool --from OES24.4-SLE-Module-Basesystem15-SP4-Updates --from OES24.4-SLE-Module-Containers15-SP4-Pool --from OES24.4-SLE-Module-Containers15-SP4-Updates --from OES24.4-SLE-Module-Desktop-Applications15-SP4-Pool --from OES24.4-SLE-Module-Desktop-Applications15-SP4-Updates --from OES24.4-SLE-Module-Server-Applications15-SP4-Pool --from OES24.4-SLE-Module-Server-Applications15-SP4-Updates --from OES24.4-SLE-Product-SLES15-SP4-Pool --from OES24.4-SLE-Product-SLES15-SP4-Updates --from OES24.4-Updates` command.

- The following product is going to be upgraded:

  `Open Enterprise Server 23.4  23.4-150400.796.6 -> 24.4-0`

  It's safe to ignore the following messages as well. They have no impact on the channel upgrade.

  The following product is going to be REMOVED:

  `"Open_Enterprise_Server Migration Product"`

  REMARK: You can choose to ignore this message. The actual product that is being removed is OES 24.4 Migration Product.

- During channel upgrade using zypper, some of the packages are going to be downgraded.

  NOTE: The packages may vary based on the setup.

12 Once the upgrade is successfully completed, register the new products once again using the `suse_register -L /root/.suse_register.log` command.

13 Reboot the server.

14 **IMPORTANT:** After the reboot, log on to the server and run the following command to complete the OES services reconfiguration:

`yast2 channel-upgrade-oes`

This will prompt for eDirectory or DSfW password if the answer file is not created. Provide the password and continue. For more information on creating the answer file, see Section 5.5.2, "Creating an Answer File to Provide the eDirectory and DSfW Passwords," on page 110.

5.6.3 Upgrading OES 24.3 to OES 24.4 using Subscription Management Tool (MFSMT)

1 Install and set up the Subscription Management Tool (MFSMT) server. For more information on setting up MFSMT, see Micro Focus Subscription Management Tool.

NOTE: Ensure to use MFSMT server for upgrading to OES. Because MFSMT on SLES 15 cannot access and mirror the OES update channels hosted on Micro Focus Customer Center.

2 Mirror down the following channels on to the SMT server:

- **OES 24.4:** OES24.4-Pool, OES24.4-SLE-Module-Basesystem15-SP4-Pool, OES24.4-SLE-Module-Basesystem15-SP4-Updates, OES24.4-SLE-Module-Containers15-SP4-Pool, OES24.4-SLE-Module-Containers15-SP4-Updates, OES24.4-SLE-Module-Desktop-Applications15-SP4-Pool, OES24.4-SLE-Module-Desktop-Applications15-SP4-Updates, OES24.4-SLE-Module-Server-Applications15-SP4-Pool, OES24.4-SLE-Module-Server-Applications15-SP4-Updates, OES24.4-SLE-Product-SLES15-SP4-Pool, OES24.4-SLE-Product-SLES15-SP4-Updates, and OES24.4-Updates channels
- **OES 24.3:** OES23.4-Pool, OES23.4-SLE-Module-Basesystem15-SP4-Pool, OES23.4-SLE-Module-Basesystem15-SP4-Updates, OES23.4-SLE-Module-Containers15-SP4-Pool, OES23.4-SLE-Module-Containers15-SP4-Updates, OES23.4-SLE-Module-Desktop-Applications15-SP4-Pool, OES23.4-SLE-Module-Desktop-Applications15-SP4-Updates, OES23.4-SLE-Module-Server-Applications15-SP4-Pool, OES23.4-SLE-Module-Server-Applications15-SP4-Updates, OES23.4-SLE-Product-SLES15-SP4-Pool, OES23.4-SLE-Product-SLES15-SP4-Updates, and OES23.4-Updates channels

For more information on Mirroring and Managing the repositories, see Mirroring Repositories on the Micro Focus SMT Server and Managing Repositories with YaST Micro Focus SMT Server Management.

3 Register the OES server with the MFSMT server. For more information on registering, see Configuring Clients with the clientSetup4SMT.sh Script in the Micro Focus Subscription Management Tool Guide.

4 After registration, upgrading from OES 2023 to the latest OES version is the same as Micro Focus Customer Center upgrades as described from step 2 in Section 5.6, “Channel Upgrade from OES 24.3 to OES 24.4,” on page 112.

NOTE: If you use Wagon and MFSMT based upgrade, you will not go through the Step 6 to Step 8 on page 113 mentioned in Section 5.6.1, “Channel Upgrade from OES 24.3 to OES 24.4 via Wagon,” on page 113. After clicking on next in Step 5 continue from Step 9 on page 113.

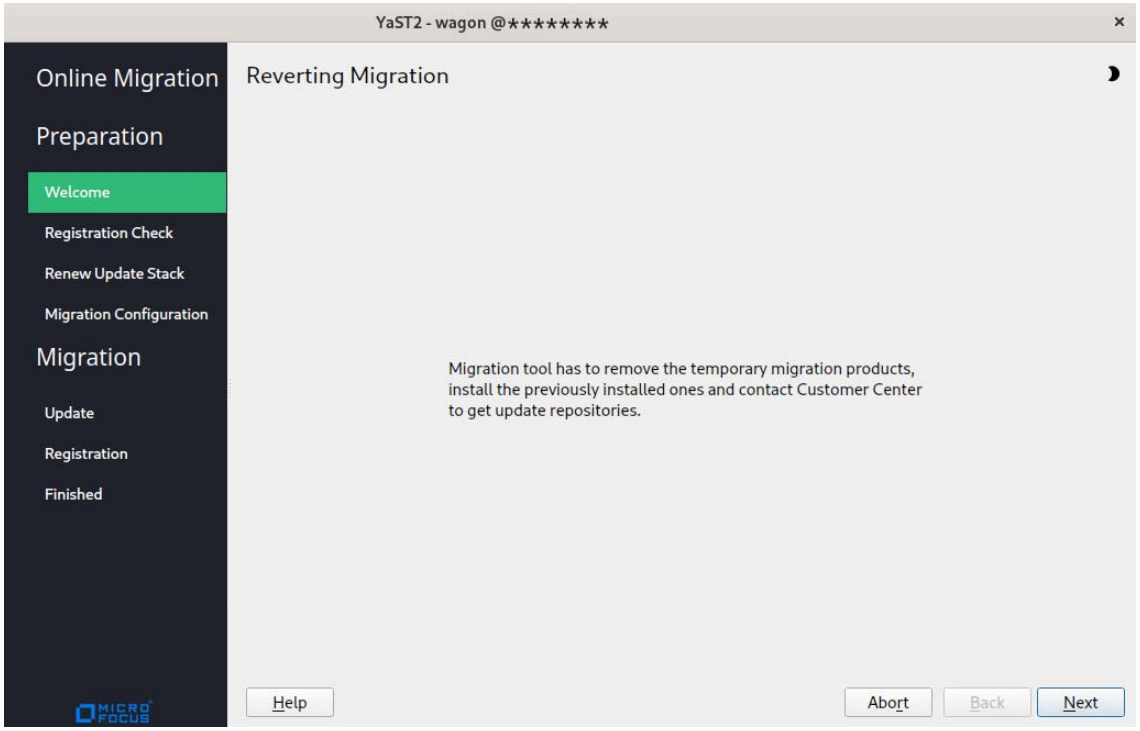
5.6.4 Rolling back the Server in the Middle of a Wagon-based Channel Upgrade

After multiple failed attempts to do an Micro Focus Customer Center registration, follow this procedure to roll back the server to its previous state safely.

1 Click **Abort** > **Abort Installation**.

2 In the Reverting Migration screen, click **Next**.

IMPORTANT: Do not click **Abort** in this screen as it will abort the revert process.



3 In Micro Focus Customer Center registration screen, click **Next**.

4 Follow the screen prompts and complete the revert process.

5.7 Upgrading Open Enterprise Server Using SUSE Manager

SUSE Manager version 4.3.15 or later supports product migration from OES 23.4 to OES 24.4 or OES 25.2.

To upgrade OES using SUSE manager, perform the following steps:

1 Ensure that you have completed the instructions in Section 8.9.1, Setting Up SUSE Manager, and patched the OES server with the latest patches.

2 Run the `zypper pd` command to ensure that the `Open_Enterprise_Server-migration` is listed but not installed.

To check the products installed, run `zypper pd -i` command.

The installed products contain information about the distribution upgrades and the migration products that should be installed to perform the migration.

3 Use the `zypper se -t product | grep -h -- "-migration" | cut -d\| -f2` command.

A sample output is as follows:

```
Open_Enterprise_Server-migration
```

4 Install migration products using the `zypper in -t product Open_Enterprise_Server-migration` command.

5 Perform the service pack migration:

5a Log in to the SUSE Manager Web console with administrative credentials.

5b Click **System**, then select the OES server to be migrated.

5c Click **Software** > **SP Migration** and verify the information of the installed product (OES 23.4) and target product (OES 24.4).

5d Click the **Select Channels to view the target channels**, and ensure that all mandatory channels are selected, if not, select manually.

5e Click **Schedule Migration** > **Confirm**.

6 Reboot the OES server after the support pack migration.

7 Log in to the OES server and run the `yast2` repositories command.

8 From the repositories, remove the OES 23.4 installation sources (if present), then add the OES 24.4 installation sources.

9 Run the following command to complete the OES services reconfiguration:

```
yast2 channel-upgrade-oes
```

10 Enter the eDirectory or DSfW password and continue. For more information on creating the answer file, see Section 5.5.2, Creating an Answer File to Provide the eDirectory and DSfW Passwords.

A Program Improvement screen is displayed if this is the first server that is upgrading to OES 24.4. For more information, see Section 3.14, Product Improvement.

5.8 Using ZENworks to Upgrade from OES 23.4 to OES 24.4 or later

Select one of the method listed below to perform an upgrade by using ZENworks 24.4:

- Managing Pool Bundles, Update Bundles and Update Bundle Groups in the Micro Focus Consulting Best Practices Guide.
- Upgrading to OES by using ZENworks 24.4 in the ZENworks Linux Package Management Reference.

5.9 Verifying that the Upgrade was Successful

One way to verify that your OES server upgrade was successful and that the components are loading properly is to watch as the server boots. As each component is loaded, the boot logger provides a status next to it indicating if the component is loading properly.

1 Verify the version of OES using the following command. It should be OES 24.4.

```
cat /etc/novell-release
```

2 Ensure that all the RPMs are up to date after an upgrade. You may use the following command to see the list of RPMs and compare them with a fresh installation of OES 24.4 or an installation source.

```
rpm -qa | sort >> <type the filename where the list of rpms will be
stored>
```

3 Continue with “What's Next” on page 121.

5.10 What's Next

After you complete the upgrade and verify that it was successful, see “Completing OES Installation Tasks” on page 123.

6 Completing OES Installation Tasks

This section provides information for completing the following tasks:

- Section 6.1, “Determining Which Services Need Additional Configuration,” on page 123
- Section 6.2, “Rebooting the Server after Installing NSS,” on page 124
- Section 6.3, “Restarting Tomcat,” on page 124
- Section 6.4, “Implementing Digital Certificates in an OES Environment,” on page 124

6.1 Determining Which Services Need Additional Configuration

NOTE: For information on configuring OES services as a different administrator than the one who originally installed the OES server, see Section 2.4.3, “Adding/Configuring OES Services as a Different Administrator,” on page 23.

Depending on the products you have installed, there might be some tasks that you must complete before you can use individual service components.

If a component requires additional configuration that is not part of the Open Enterprise Server (OES) installation, see the component's administration guide for more information. The following table include links to the installation and configuration information for most OES 24.4 services.

Table 6-1 *OES 24.4Services Additional Installation and Configuration Instructions*

OES Service	For Additional Installation and Configuration Information
Domain Services for Windows	See “Installing Domain Services for Windows” in the *Domain Services for Windows Administration Guide*.
OES Backup/Storage Management Services (SMS)	See “Installing and Configuring SMS” in the *Storage Management Services Administration Guide for Linux*.
OES Business Continuity Cluster (BCC)	See “Installing Business Continuity Clustering” in the *BCC Administration Guide for OES 2018 SP2*.
OES CIFS	See “Installing and Setting Up CIFS” in the*OES CIFS for Linux Administration Guide*.
OES Cluster Services	See “Installing, Configuring, and Repairing OES Cluster Services” in the *OES Cluster Services for Linux Administration Guide*.
OES DHCP	See “Installing and Configuring DHCP ” in the *DNS/DHCP Services for Linux Administration Guide*.
OES DNS	See “Installing and Configuring DNS ” in the *DNS/DHCP Services for Linux Administration Guide*.

OES Service	For Additional Installation and Configuration Information
OES eDirectory	See "Installing or Upgrading NetIQ eDirectory on Linux" in the *NetIQ eDirectory Installation Guide*.
OES iManager	See "Installing iManager Server and Workstation" in the *NetIQ iManager Installation Guide*.
iPrint Advanced	See "Installing OES iPrint Advanced Server" in the *OES iPrint Advanced Administration Guide*.
OES Linux User Management	See "Setting Up Linux User Management" in the *Linux User Management Administration Guide*.
OES NCP Server	See "Installing and Configuring NCP Server for Linux" in the *NCP Server for Linux Administration Guide*.
OES Remote Manager	See "Changing the HTTPSTKD Configuration" in the *OES 23.4: OES Remote Manager Administration Guide*.
OES Storage Services	See "Installing and Configuring OES Storage Services" in the *Storage Services File System (NSS) Administration Guide for Linux*.
OES Pre-Migration Server	See "Preparing for Transfer ID" in the *Migration Tool Administration Guide*.
Unified Management Console	See "Installation and Configuration of UMC" in the Unified Management Console Administration Guide.

6.2 Rebooting the Server after Installing NSS

If you install Novell Storage Services (NSS) on an existing OES server, enter `rcnovell-smdrd restart` or `systemctl restart novell-smdrd.service` at the terminal prompt or reboot the server before performing any backups, restores, or server consolidations on the NSS file system.

6.3 Restarting Tomcat

If you install iManager after the server has been installed, Tomcat is not running and you must restart it to run iManager.

To restart Tomcat, enter the following command.

```
systemctl restart novell-tomcat.service
```

6.4 Implementing Digital Certificates in an OES Environment

In an OES environment, you can make all communications secure by implementing a verified secure digital certificate. These certificates should be issued and signed by a Certificate Authority (CA). The CA can be a trusted third-party vendor or your own organizational CA.

This section describes the procedures to implement digital certificates in an OES environment.

6.4.1 Configuring the Digital Certificate

In an eDirectory environment, create a subordinate certificate authority that allows the organization CA to be subordinate to a trusted third-party CA or a CA in another eDirectory tree. For more information on why you should create a subordinate certificate authority, see Subordinate Certificate Authority in the Novell Certificate Server 3.3.8 Administration Guide.

To configure the digital certificate:

1. Create the Certificate Signing Request (CSR) file from your OES environment. For detailed instructions, see Step 1 in Creating a Subordinate Certificate Authority in the Novell Certificate Server 3.3.8 Administration Guide.
2. Get the CSR signed by a trusted third-party CA or another eDirectory tree. For detailed instructions, see Step 2 in Creating a Subordinate Certificate Authority in the Novell Certificate Server 3.3.8 Administration Guide.
3. Acquire the signed CA certificate from the third-party CA or another eDirectory tree. For detailed instructions, see Step 3 in Creating a Subordinate Certificate Authority in the Novell Certificate Server 3.3.8 Administration Guide.
4. Import the signed CA certificates into your OES environment. For detailed instructions, see Step 4 in Creating a Subordinate Certificate Authority in the Novell Certificate Server 3.3.8 Administration Guide.
5. Export the public or private keys to a PKCS#12 file in your OES environment. For detailed instructions, see Step 5 in Creating a Subordinate Certificate Authority in the Novell Certificate Server 3.3.8 Administration Guide.

NOTE: If you already have a certificate signed by a third-party CA, skip Step 2 and Step 3.

For more information on creating and importing certificates using third-party vendors such as VeriSign or RapidSSL, see the TID on How to import a Production VeriSign External Certificate into eDirectory using iManager (3033173).

6.4.2 Reconfiguring Services after Importing the Certificate

The following services must reconfigured so that these services use the latest verified certificate: LDAP, Apache, and LUM.

Reconfiguring LDAP

To point the LDAP server object to the verified certificate:

1. Log in to iManager with administrative privileges.
2. Click the **LDAP > LDAP Options > View LDAP Groups** tab and the LDAP group, then select the **Require TLS for Simple Binds with Password** check box.
3. Click **Apply** and **OK**.
4. Click the **LDAP Options > View LDAP Servers** tab, then click the LDAP server **> Connections**. In the Server Certificate text box, search for and select the certificate that you created.
5. Click **Apply** and **OK**.
6. Repeat Step 4 and Step 5 for all the LDAP servers in the LDAP group.

Reconfiguring Apache

- If you have used an eDirectory SSL certificate, see the TID on How to use eDirectory SSL certificates for Apache2 on SLES OES (7014029) to reconfigure Apache.
- If you have used a third-party SSL certificate, see the TID on Using Apache SSL default certificates or third party certificates on SLES (7004384) to reconfigure Apache.

Reconfiguring LUM

For LUM to use the latest signed certificate:

1. Import an SSL certificate to the local machine using the `namconfig -k` command.
2. Refresh the nam settings using the `namconfig cache_refresh` command.

   For example, to view the certificate details, execute the `openssl x509 -in /var/lib/novell-lum/.198.162.1.1.der -noout -inform der -text` command.

7 Installing and Configuring NSS Active Directory Support

This section describes the procedures to install and configure OES Storage Services Active Directory (NSS AD) support afresh, or after upgrading OES.

- Section 7.1, “Understanding the NSS AD Support,” on page 127
- Section 7.2, “NSS AD Support Matrix,” on page 130
- Section 7.3, “Prerequisites for Installing and Configuring NSS AD,” on page 131
- Section 7.4, “Installing OES 24.4 with NSS AD Support,” on page 132
- Section 7.5, “About Novell Identity Translator (NIT),” on page 136

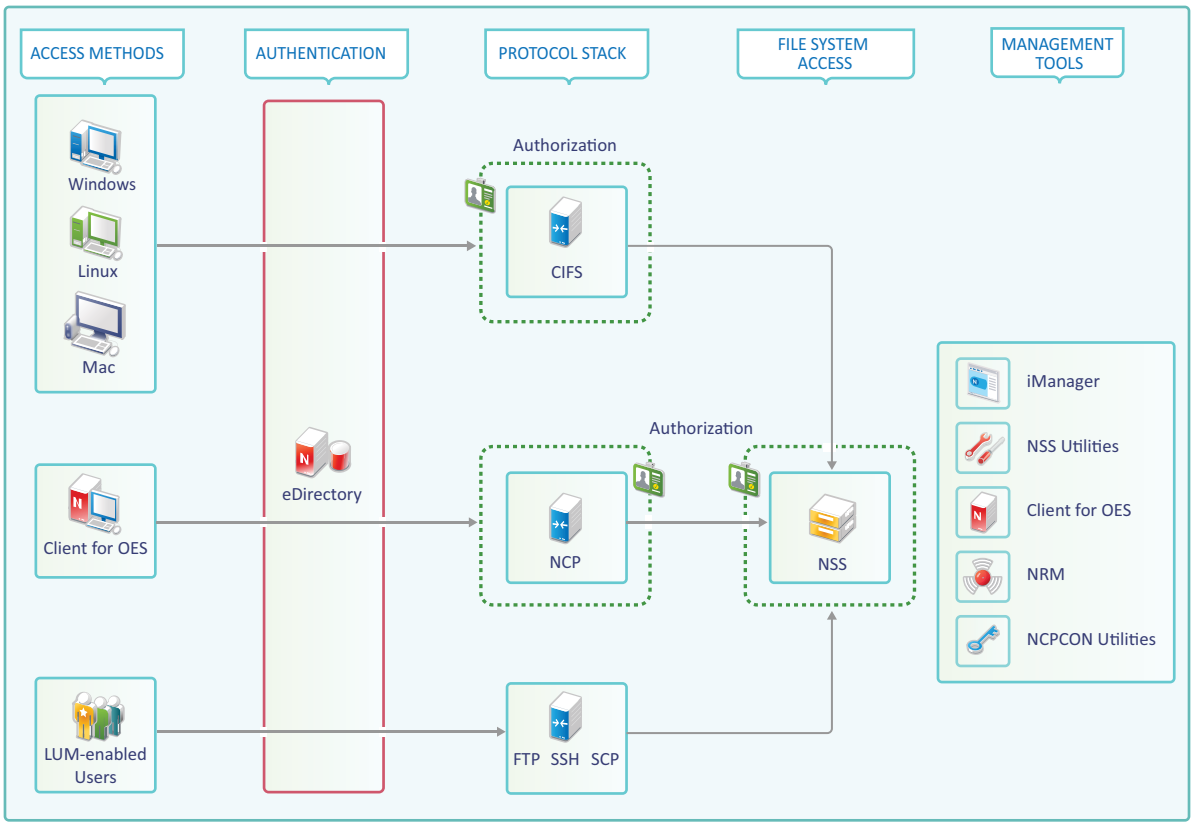
7.1 Understanding the NSS AD Support

Beginning with OES 2015, like the eDirectory users, Active Directory users can also natively access the NSS resources, administer those resources, and provision rights for Active Directory trustees. OES 2015 or later enables you to join to an Active Directory domain and provide seamless access to Active Directory identities for using NSS resources. OES does not duplicate identities across eDirectory and Active Directory, thus enabling users in an Active Directory environment to access NSS resources without having the users exist in eDirectory. This solution is termed as Novell Storage Services Active Directory (NSS AD) Support.

To understand NSS AD, it is essential to know how NSS resource access was until OES 11 SP2 and how it is with OES 2015 or later.

7.1.1 NSS Resource Access Until OES 11 SP2

The following illustration, in a nutshell, depicts how authentication, authorization, and file access was until OES 11 SP2.



File Access

In the traditional OES file access model, Windows and Linux workstations use the CIFS protocol for file access. Client for Open Enterprise Server software for both Windows and Linux uses the NetWare Core Protocol (NCP) to provide the file services and Macintosh workstations communicate using CIFS. To access NSS resources using FTP, SSH, and SCP, users must be LUM-enabled.

Authentication

Only eDirectory is supported as an identity source. All file service access is controlled by eDirectory authentication.

Authorization

The authorization to access NSS resources using NCP and CIFS happens at the respective protocols level. On the other hand, users trying to access NSS resources using FTP, SSH, and SCP are authorized at NSS file system level.

Management Tools and Interfaces

OES provides the following set of management interfaces and tools to manage your network.

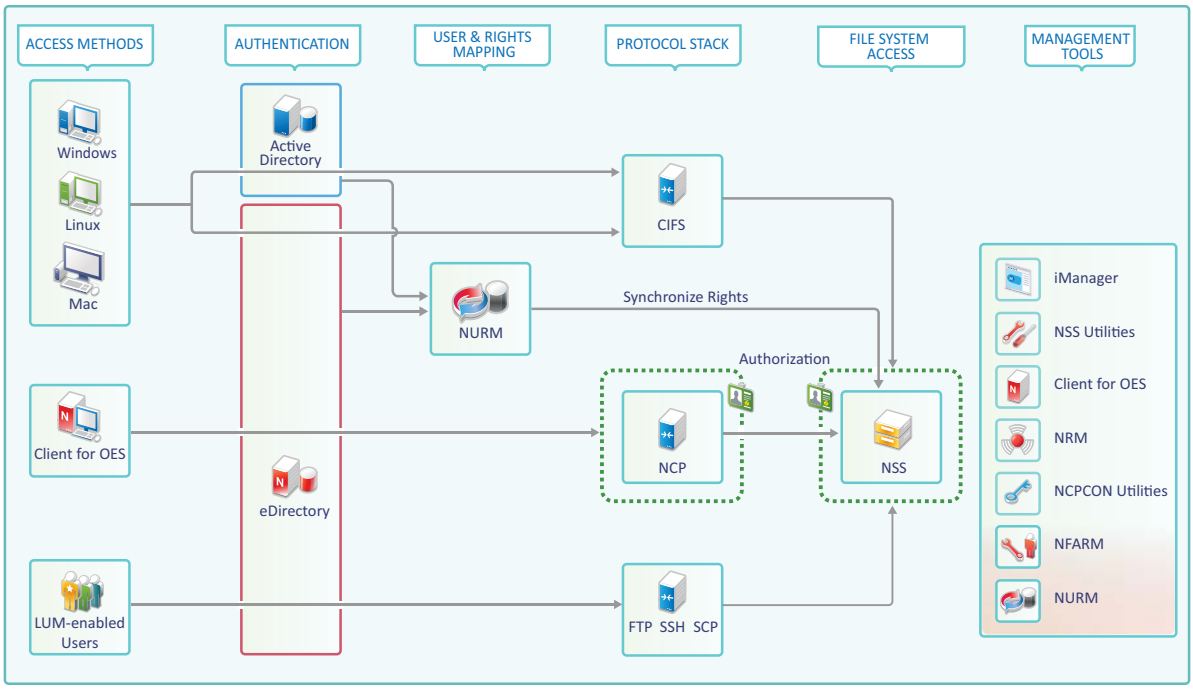
Rights Management: iManager, rights utility, NCPCON utilities, Client for Open Enterprise Server for Windows and Novell Client for Linux

User Management: iManager

Storage Management: iManager, NRM (DST Policy Management, primary shadow volume management and so on), NSSMU, and NLVM.

7.1.2 NSS Resource Access with OES 2015 or Later

The following diagram, in a nutshell, depicts how authentication, authorization, and file access is with OES 2015 or later.



File Access

With OES 2015 SP1 or later, Active Directory users can authenticate to Active Directory and natively access NSS resources using the CIFS and FTP protocol. NSS file access for Active Directory users using NCP is not supported.

There is no change in the way how file access happens for eDirectory users. To know more about file access for eDirectory users, see "File Access" on page 128 under Section 7.1.1, "NSS Resource Access Until OES 11 SP2," on page 127.

Authentication

With OES 2015 or later, both eDirectory and Active Directory are supported as an identity source, and OES enables the NSS file system to accept Active Directory identities as trustees.

CIFS identifies the type of user trying to access the NSS resource and authenticates the user using the respective identity source. For example, when an Active Directory user attempts to access NSS resource, authentication is controlled by Active Directory using kerberos. On the other hand, for eDirectory users, authentication is controlled by eDirectory.

Authentication of eDirectory users using NCP, FTP, SSH, and SCP is controlled by eDirectory.

Authorization

For both eDirectory and Active Directory users using CIFS, the authorization happens at the NSS level.

For eDirectory users using NCP, the authorization happens at NCP level. For eDirectory users using FTP, SSH, and SCP, the authorization happens at the NSS level.

Management Tools and Services

OES 2015 introduced some new tools which are used along with the existing tools to manage your network.

Rights Management: NFARM (AD only), iManager (eDirectory only), rights utility (supports AD and eDirectory), Client for Open Enterprise Server for Windows and Novell Client for Linux (eDirectory only), NCPCON utilities (eDirectory only).

User Management: iManager (only eDirectory). The Active Directory user management is using the native AD tools like MMC (Microsoft Management Console).

Storage Management: iManager, NRM (DST Policy Management, primary shadow volume management and so on), NSSMU and NLVM.

User and ACL Mapping: OES User Rights Management (NURM) is a tool that helps to create and save the mapping of eDirectory and Active Directory users. It is then used to assign ACLs and write them on to NSS media. After mapping, every AD identity that has been mapped to an eDirectory user, group, or container will get the same rights on the NSS resource as that of an eDirectory identity.

NOTE: Beginning with OES 24.4, OES User Rights Map (NURM) is deprecated and not available with OES.

Identity Translator: Novell Identity Translator (NIT) is an identity translator that generates or fetches UIDs based on the configuration and allows eDirectory and Active Directory users to access NSS resources natively. For more information, see Section 7.5, “About Novell Identity Translator (NIT),” on page 136.

7.2 NSS AD Support Matrix

- **OES 24.4:** SLES 15 SP4
- **Active Directory:** Active Directory running on Windows server 2022, Windows server 2019, and Windows server 2016.
- **OES File Access Rights Management Utility (NFARM):** Windows 11, Windows server 2022, Windows 10, Windows server 2019, and Windows server 2016.
- **OES User Rights Map Utility (NURM):** Any web browser that supports, HTML5, CSS3, and Java script.

  NOTE: Beginning with OES 24.4, OES User Rights Map (NURM) is deprecated and not available with OES.

7.3 Prerequisites for Installing and Configuring NSS AD

- **Active Directory:** Ensure that you have a working AD server, and the OES 2018 or later server must resolve the DNS name of the AD domain controller in the domain to which the server will be joined to.
  - **Single Forest Environment:** Create a Universal Group with the sAMAccountName "OESAccessGrp" anywhere in the AD forest. Only the members of this group will have access to the NSS resources based on their trustee assignments. In absence of this group, all the AD users in the forest can access the NSS resources based on their trustee assignments.
  - **Multi Forest Environment:** Create a Domain Local Group (DLG) with the sAMAccountName "DLOESAccessGrp" in the AD domain to which this OES server is joined. Only the members of this group (OES forest and across forest) will have access to the NSS resources based on their trustee assignments. In absence of this group, the AD users across the forest cannot access the NSS resources.
- **Reverse Lookup Entry for the AD Server:** AD server's reverse lookup entry (IPv4 and IPv6) must exist in the DNS server before the domain join operation is performed.
- **Firewall:** For NSS AD to communicate, ensure that ports 389, 636, 88, 749, and 464 are open.
- **Time Synchronization:** The clocks must be synchronized between OES 2018 or later server and the Active Directory Server.
- **DNS A Record:** To access the shared resource on OES, add DNS A record for netbios name of the host or cluster resource.
- **DNS Nslookup Entry for the AD Server:** Ensure to resolve the AD server using DNS Nslookup entry.
- **Rights Required for the Domain Join:** The AD domain administrator or any AD user who has the rights to change password, reset password and create container objects on an AD server can be used for the domain join process.
- **Novell Identity Translator (NIT):** NIT can operate in two modes: Fetch and Generate. If you decide to generate UIDs, ensure to plan and select a UID range that does not conflict with LUM and Linux UID ranges. If you opt for the fetch mode, UID should exist in AD and the UID number attributes must be replicated to the global catalog. Only then the NIT will be able to fetch the users' UID for authorization. For more information on replicating the UIDs to the global catalog, see Microsoft Documentation (http://support2.microsoft.com/kb/248717).

  NOTE: If NIT is configured in generate mode, it generates UIDs even for users who already have a UID stored in AD. For more information on NIT, see Section 7.5, "About Novell Identity Translator (NIT)," on page 136.

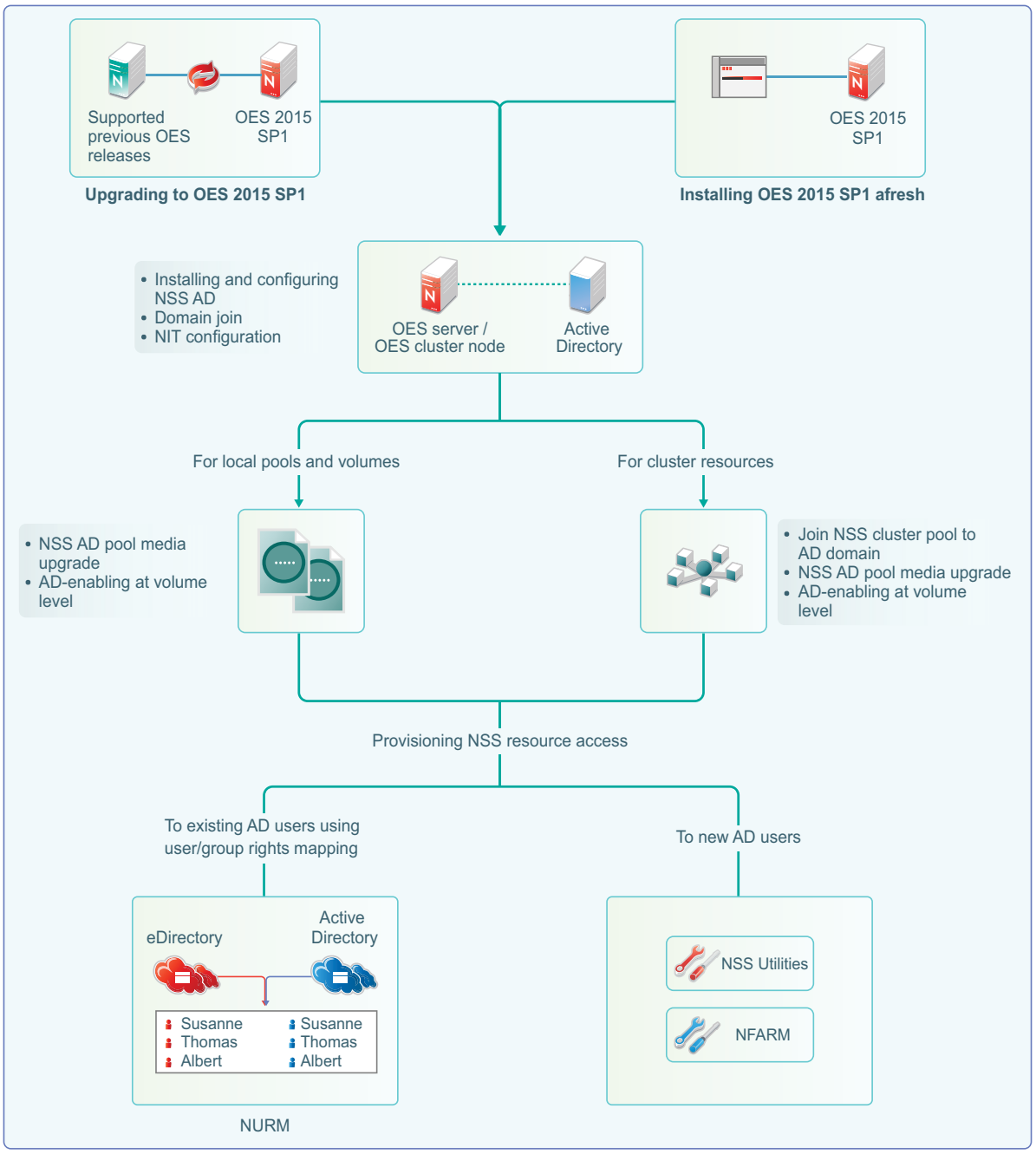
- **NSS AD Coexistence with Other OES Services:** When you configure and install NSS AD, ensure that you do not opt to install DSfW on the same server where NSS AD will be installed and configured.
- **NSS AD's Dependency on CIFS Service:** Before installing and configuring NSS AD, ensure that the CIFS service is installed and running.
- **Cluster Recommendation:** In a cluster environment, if you plan to upgrade to OES 24.4 with NSS AD support, it is recommended to upgrade all the cluster nodes to OES 24.4. NSS cluster resources whose pools have not been NSS AD Media upgraded, volumes AD-enabled, and joined to the AD domain will not be accessible for AD users. For more information on joining the

cluster resources to the AD domain, see "Joining Cluster Pools to the AD Domain" in the *Storage Services File System (NSS) Administration Guide for Linux*. You could also use the `novell-ad-util` CLI tool for the domain join. For more information, see "novell-ad-util Command Line Utility" in the *NSS AD Administration Guide*.

7.4 Installing OES 24.4 with NSS AD Support

Here's how you can install and configure NSS AD afresh or after an OES upgrade.

- Section 7.4.1, "Resolving the AD DNS Name from OES 24.4," on page 134
- Section 7.4.2, "Installing and Configuring NSS AD Support," on page 134
- Section 7.4.3, "Validating the NSS AD Configuration," on page 135



- For information on installing or upgrading to OES 24.4, domain join, and NIT configuration, see Section 7.4.2, “Installing and Configuring NSS AD Support,” on page 134.
- After installing and configuring NSS AD,
  - Media-upgrade the local pools and AD-enable the local volumes to support AD users. For more information on NSS Media upgrade and AD-enabling, see “NSS Media Upgrade Commands” and “Volume AD-enabling” in the *Storage Services File System (NSS) Administration Guide for Linux*.
  - Upgrade your cluster resources to support AD users. Join all cluster pools to the AD domain using NSSMU (see “NSS Management Utility (NSSMU) Quick Reference” in the *Storage Services File System (NSS) Administration Guide for Linux*), upgrade all cluster pools media

and AD-enable the volumes. For more information on media upgrade, and AD-enabling, see “NSS Media Upgrade Commands” and “Volume AD-enabling” in the *Storage Services File System (NSS) Administration Guide for Linux*. NSS AD media upgrade is required only for NSS32 bit pools, and AD-enabling of volumes must be done for both NSS32 and NSS64 pools.

- To enable AD users access the NSS resources, they need to be provisioned with sufficient rights. Use the OES User Rights Map utility to map users and rights between eDirectory and Active Directory users. For more information, see “OES User Rights Map (NURM) ” in the *Storage Services File System (NSS) Administration Guide for Linux*.

  NOTE: Beginning with OES 24.4, OES User Rights Map (NURM) is deprecated and not available with OES.

- To manage AD users’ rights, user quota, owner information, directory quota and so on, use OES File Access Rights Management or rights utility. For more information, see “OES File Access Rights Management (NFARM)” and “rights” in the *Storage Services File System (NSS) Administration Guide for Linux*.

There is no change with the way you install or upgrade to OES 24.4 except in the Storage Services AD Support Configuration screens.

7.4.1 Resolving the AD DNS Name from OES 24.4

To make OES work properly with NSS AD, ensure that AD server and OES servers are mutually resolvable. If you are not able to resolve, do not proceed with the NSS AD installation. Your Domain Search name and Name Server entries might be incorrect.

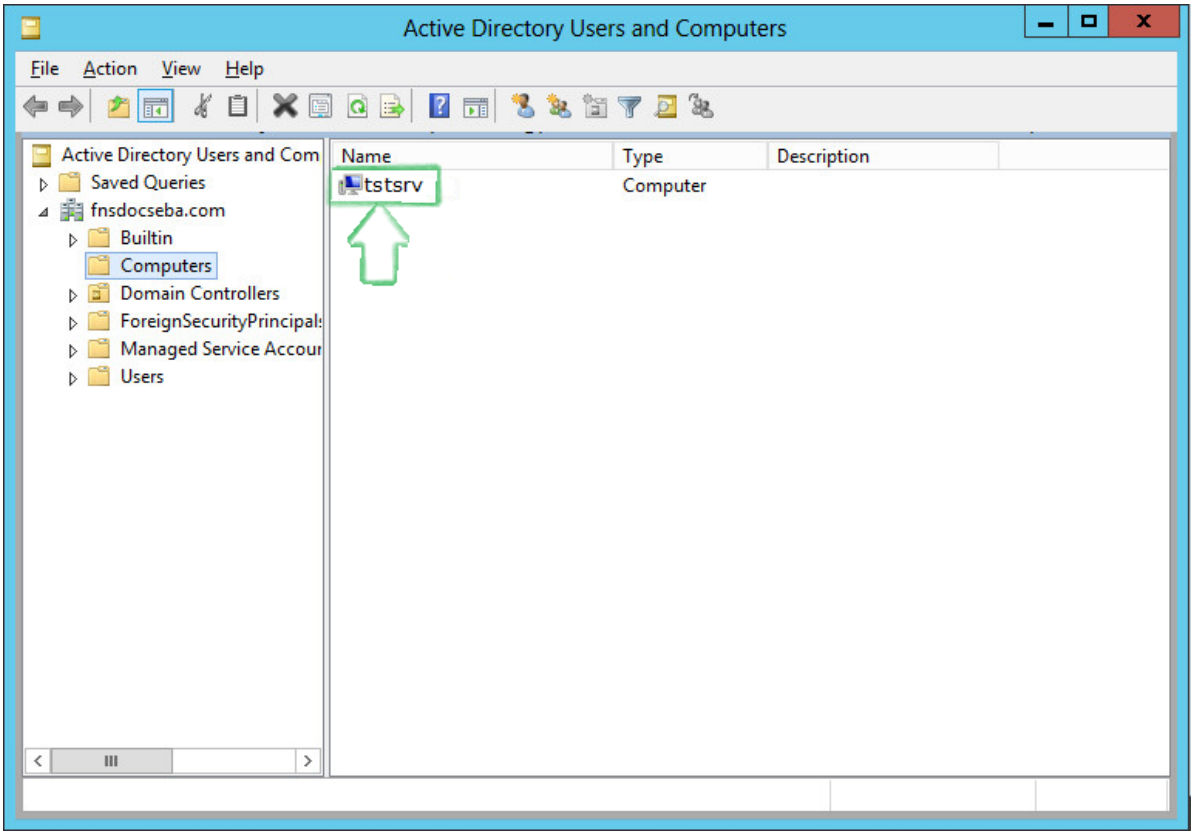
7.4.2 Installing and Configuring NSS AD Support

After resolving the AD DNS Name from the OES server, under the OES Patterns screen, select OES Storage Service AD Support pattern and specify the following details:

- **AD Domain Name:** Specify the appropriate AD domain name.
- **AD Supervisor Group:** Specify the AD supervisor group name. The AD users belonging to this group will have supervisory rights for all the volumes associated with that OES server.
- **AD User Name:** Specify the user name that can be used for the domain join operation. This user should have the following privileges: rights to reset password, create computer objects, delete computer objects, and read and write the `msDs-supportedEncryptionTypes` attribute.
- **Password:** Specify the appropriate password of the user who is used for the domain join operation.
- **Container to Create Computer Object:** You can specify the container under which the OES computer object will be created. The default container is cn=computers. If you have already created an OES computer object in the AD server, select **Use pre-created computer object**, then specify the container name where the pre-created OES computer object exists.
- **NIT - Novell Identity Translator Configuration:** If you want NIT to generate UIDs for AD users, select **Generate UID for AD users**, then specify the UID range. The default range is from 100000 to 200000. If you want NIT to fetch UIDs, do not select the **Generate UID for AD users** option.

7.4.3 Validating the NSS AD Configuration

After successfully installing and configuring NSS AD, you should find an entry for the cluster node object created in the **Active Directory Users and Computers** screen of the AD server as shown in the following image.



You can also execute `klist -k` command and verify that the default keytab entries are created as shown below.

```
tstsrv:~/Desktop #klist -k
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------
-----
   2 tstsrv$@ACME.COM
   2 tstsrv$@ACME.COM
   2 tstsrv$@ACME.COM
   2 cifs/tstsrv.acme.com@ACME.COM
   2 cifs/tstsrv.acme.com@ACME.COM
   2 cifs/tstsrv.acme.com@ACME.COM
   2 cifs/tstsrv@ACME.COM
   2 cifs/tstsrv@ACME.COM
   2 cifs/tstsrv@ACME.COM
   2 host/tstsrv.acme.com@ACME.COM
   2 host/tstsrv.acme.com@ACME.COM
   2 host/tstsrv.acme.com@ACME.COM
tstsrv:~/Desktop #
```

This command updates the default keytab, `/etc/krb5.keytab` and `/etc/krb5.conf` files. OES 2018 or later supports three strongest encryption types: AES128, AES256, RC4HMAC. For each encryption type, an entry is made in the default key tab.

7.5 About Novell Identity Translator (NIT)

The Novell Identity Translator (NIT) is briefly explained in the following sections:

- A New NSS Authorization Model
- Not All Users Have UIDs
- Ensuring that Your CIFS-NSS Users Have UIDs
- Which OES Components Rely on NIT

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

A New NSS Authorization Model

OES includes a new authorization model for CIFS-user access to NSS volumes.

The new model requires that eDirectory and Active Directory (AD) users all have unique User IDs (UIDs).

Not All Users Have UIDs

- **eDirectory:** LUM-enabled eDirectory users have UIDs; non-LUM-enabled eDirectory users do not.
- **Active Directory:** Generally speaking, AD users don't have UIDs, but AD can be configured to assign the uidNumber attribute to users when required.

Ensuring that Your CIFS-NSS Users Have UIDs

The Novell Identity Translator (NIT) lets you ensure that all users requiring NSS authorization have the required UIDs.

- **eDirectory:** When NIT is properly configured, all eDirectory users can access NSS using OES CIFS, as summarized in Table 7-1.

Table 7-1 *NIT Guarantees UIDs for All eDirectory Users*

User UID Status in eDirectory	What NIT Does
LUM-enabled user	Retrieves the UID from eDirectory
Non-LUM-enabled user	Generates a UID within the specified UID range

- **Active Directory:** If needed, you can configure NIT to simply retrieve and pass along UIDs that are set in Active Directory by deselecting the **Generate UIDs for AD Users** option when you Configure the NSS for Active Directory service. However, you must then ensure that all AD users who need access to NSS through CIFS have the uidNumber attribute set on their AD account. This caveat is summarized in Table 7-2.

Table 7-2 *NIT Must Be Properly Configured to Guarantee UIDs for Active Directory Users Who Need Them*

UIDs in Active Directory	UID Generation	What NIT Does
The `uidNumber` attribute is set for some or all AD users. Those users have a UID number in Active Directory.	Enabled	Generates UIDs within the specified UID range for all AD users needing NSS access. The `uidNumber` attribute in Active Directory is ignored.
	Disabled	Retrieves the `uidNUmber` from Active Directory when available. Users without a `uidNumber` cannot access NSS.
The `uidNumber` attribute is not set for any AD users.	Enabled	Generates UIDs within the specified UID range for all AD users needing NSS access.
No AD users have a UID number in Active Directory	Disabled	No users can access NSS because none of them has a UID.

Which OES Components Rely on NIT

NIT is used as an infrastructure component by various OES components, including OES CIFS, NSS, and SMS.

8 Updating (Patching) an OES Server

The instruction in this chapter are for updating or patching the OES server with patches or innovation releases. These steps can be performed either during the installation or upgrade or after the installation or upgrade is complete.

- Section 8.1, “Overview of Updating (Patching),” on page 139
- Section 8.2, “Supported OES Update Paths,” on page 140
- Section 8.3, “Preparing the Server for Updating,” on page 141
- Section 8.4, “Registering the Server in the Customer Center,” on page 142
- Section 8.5, “Updating the Server,” on page 144
- Section 8.6, “GUI Based Patching,” on page 148
- Section 8.7, “Frequently Asked Questions about Updating,” on page 149
- Section 8.8, “Patching From Behind a Proxy Server,” on page 149
- Section 8.9, “Using SUSE Manager to Patch an OES Server,” on page 149
- Section 8.10, “Using ZENworks Server to Patch an OES Server,” on page 151
- Section 8.11, “Installing the Latest iManager NPMs After Applying OES Patches,” on page 151
- Section 8.12, “Restarting the OES Instance of Tomcat After Applying a Tomcat Update,” on page 152

8.1 Overview of Updating (Patching)

- Section 8.1.1, “The Patch Process Briefly Explained,” on page 139
- Section 8.1.2, “Update Options,” on page 140

8.1.1 The Patch Process Briefly Explained

The OES patch process consists of the following processes:

1. The patch tool (zypper, Package Kit, or YaST Online Update [YOU]) checks for available patches on its configured patch update repositories and displays them for selection.
2. The patch administrator selects which patches to apply.
3. The patch tool checks cross-dependencies and displays any messages regarding situations or conflicts that require administrator input.
4. The patches are downloaded.

   If any downloaded patches contain information or instructions, these are displayed for administrator acknowledgement. For example, administrators might be instructed to restart a service or run a configuration script file to complete the process after the patch process completes.

5. After all of the messages have been acknowledged, the downloaded patches are installed.
6. The administrator is prompted to restart the server.

8.1.2 Update Options

OES administrators have three options for updating servers with patches from OpenText.

- **Online Update Servers (NCC):** For those who don't require an internal update source, OES servers can be easily configured to directly access the online patch repository. Instructions for doing this are included in the sections that follow.
- **Subscription Management Tool (MFSMT):** This product doesn't require a separate license. It lets you host patches from the OES online update repository on a server, which provides more security and greatly reduces Web traffic related to server updates. SMT is available for download on the OpenText Marketplace.

  NOTE: OES patch channels are available through NCC. If you are using SMT for update, ensure that it is SUSE SMT on SLES 11 or Micro Focus SMT and it communicates only with NCC and not with SCC.

- **SUSE Manager:** SUSE Manager is a server solution for providing updates, patches, and security fixes for single SUSE Linux Enterprise, OES, and Red Hat Enterprise Linux clients. It comes with a set of tools and a Web-based user interface for management tasks. For more information, see Using SUSE Manager to Patch an OES Server.
- **ZENworks Linux Management:** An enterprise-level product that requires a separate license. It provides updates for SUSE Linux Enterprise, OES, and Red Hat Enterprise Linux (RHEL) products. In addition to hosting updates for download, ZENworks Linux Management is also capable of pushing the updates to targeted devices through a single Web interface. For more information, see Using ZENworks Server to Patch an OES Server.

IMPORTANT: OES patches are not cumulative. A patch update to a specific component does not necessarily contain all related RPMs for that component. When you patch a server that has any version of OES, either by directly using the update catalogs from nu.novell.com or by mirroring the update catalogs from nu.novell.com to a local SMT server, you must apply all available patches as they are offered through the official update repositories. Do not apply partial patches, or apply patches intermittently or out of sequence.

Each patch release assumes that you will apply the new patches to a fully patched system, and that you will apply all of the patches in the release. We do not support applying only selected patches from a specific scheduled maintenance patch, skipping a scheduled maintenance patch, or applying patches out of their intended order.

8.2 Supported OES Update Paths

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

Table 8-1 *Supported Paths for Updating OES*

Source Version	Supported Methods	Additional Information
OES 24.4, OES 24.4.1, OES 25.1, or OES 25.2	NCC Subscription Management Tool (SMT) SUSE Manager ZENworks	Before update, you must register to NCC, SMT, SUSE Manage, or ZENworks.

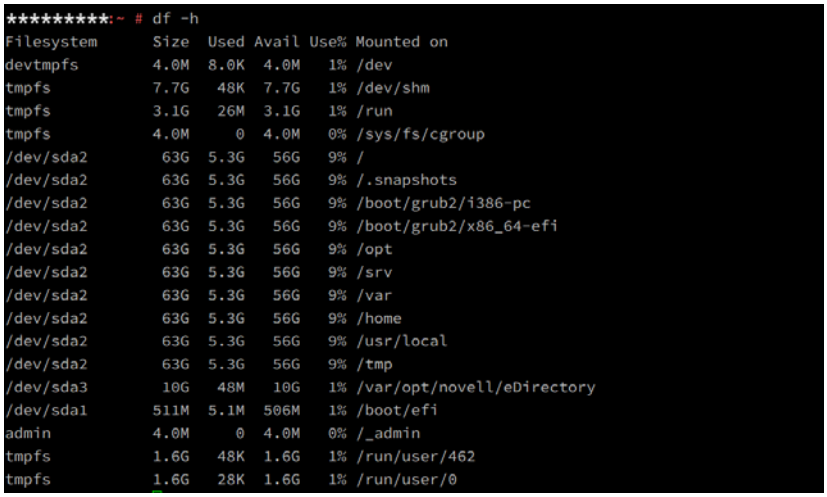
8.3 Preparing the Server for Updating

1. Make sure you have installed all the services that you need on the server.
2. Before starting your update, make note of the root partition and available space.

   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 `/`).

   Example: List with df -h.



   In particular, ensure that you have enough space where the update process downloads all the updates to in `/var/cache/zypp/`.

   Depending on the number of patches that you are going to apply, you might need about 3 GB for OES server.
3. Before updating the server, secure the current data on the server.

   Copy all configuration files to a separate medium, such as a streamer, removable hard disk, USB stick, or ZIP drive. 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.

8.4 Registering the Server in the Customer Center

Before you can patch an OES server with updates, you must register the server either during installation or later by using the instructions in this section.

If you register through evaluation codes, your server can receive patches for only 60 days, at which time the codes expire.

You need to register each server with the Customer Center only once. After you have registered the server, you can update the server at any time. This includes replacing evaluation codes with purchased codes. You can use the desktop interface (GUI) or the command line to accomplish this task.

This section contains the following information:

- Section 8.4.1, “Prerequisites,” on page 142
- Section 8.4.2, “Registering the Server in the Customer Center Using the Command Line,” on page 142
- Section 8.4.3, “Registering the Server in the Customer Center Using the GUI,” on page 143

8.4.1 Prerequisites

To complete these procedures, you must have the following:

- An Access for Registration Service account.

  This is the same account that you use for Bugzilla. For more information about Registration Service account, see OpenText Software Licenses and Downloads - Frequently asked questions (https://sld.microfocus.com/mysoftware/contact/faqsQuestion).
- The activation codes for OES that you received when you purchased your product.
- An established connection to the Internet.

8.4.2 Registering the Server in the Customer Center Using the Command Line

To register a new server or to replace evaluation activation codes with standard codes.

1. Log in to the server as `root` or su to `root`
2. At the command line, enter

   ```
   suse_register -a email=email_address -a regcode-oes=oes_registration_code
   ```

   For example:

   ```
   suse_register -a email=joe@example.com -a regcode-oes=30a74ebb94fa
   ```

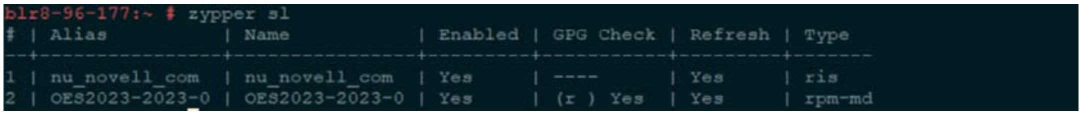
   IMPORTANT: If you are replacing evaluation codes with purchased codes, simply enter the codes. No further action is required.

3 Verify that the server is registered by checking whether you have the service types and catalogs needed for updates:

3a To verify the service type, enter

```
zypper ls
```

The results should be similar to the following:



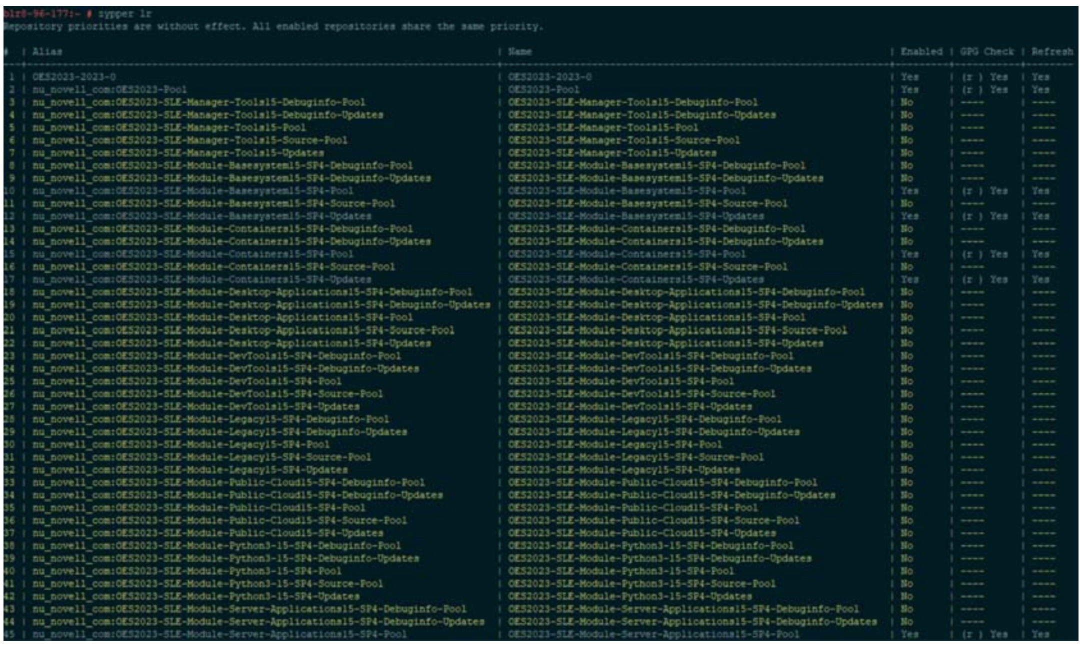
```
blr8-96-177:~ # zypper sl
# | Alias             | Name              | Enabled | GPG Check | Refresh | Type
--+-------------------+-------------------+---------+-----------+---------+-------
1 | nu_novell_com     | nu_novell_com     | Yes     | ----      | Yes     | ris
2 | OES2023-2023-0    | OES2023-2023-0    | Yes     | (r ) Yes  | Yes     | rpm-md
```

The URIs you see for the ZYPP type differ based on your installation source.

3b To verify the catalogs, enter

```
zypper lr
```

The results should be similar to the following:



```
blr8-96-177:~ # zypper lr
Repository priorities are without effect. All enabled repositories share the same priority.

#  | Alias                                                                  | Name                                                           | Enabled | GPG Check | Refresh
---+------------------------------------------------------------------------+----------------------------------------------------------------+---------+-----------+--------
1  | OES2023-2023-0                                                         | OES2023-2023-0                                                 | Yes     | (r ) Yes  | Yes
2  | nu_novell_com:OES2023-Pool                                             | OES2023-Pool                                                   | Yes     | (r ) Yes  | Yes
3  | nu_novell_com:OES2023-SLE-Manager-Tools15-Debuginfo-Pool               | OES2023-SLE-Manager-Tools15-Debuginfo-Pool                     | No      | ----      | ----
4  | nu_novell_com:OES2023-SLE-Manager-Tools15-Debuginfo-Updates            | OES2023-SLE-Manager-Tools15-Debuginfo-Updates                  | No      | ----      | ----
5  | nu_novell_com:OES2023-SLE-Manager-Tools15-Pool                         | OES2023-SLE-Manager-Tools15-Pool                               | No      | ----      | ----
6  | nu_novell_com:OES2023-SLE-Manager-Tools15-Source-Pool                  | OES2023-SLE-Manager-Tools15-Source-Pool                        | No      | ----      | ----
7  | nu_novell_com:OES2023-SLE-Manager-Tools15-Updates                      | OES2023-SLE-Manager-Tools15-Updates                            | No      | ----      | ----
8  | nu_novell_com:OES2023-SLE-Module-Basesystem15-SP4-Debuginfo-Pool       | OES2023-SLE-Module-Basesystem15-SP4-Debuginfo-Pool             | No      | ----      | ----
9  | nu_novell_com:OES2023-SLE-Module-Basesystem15-SP4-Debuginfo-Updates    | OES2023-SLE-Module-Basesystem15-SP4-Debuginfo-Updates          | No      | ----      | ----
10 | nu_novell_com:OES2023-SLE-Module-Basesystem15-SP4-Pool                 | OES2023-SLE-Module-Basesystem15-SP4-Pool                       | Yes     | (r ) Yes  | Yes
11 | nu_novell_com:OES2023-SLE-Module-Basesystem15-SP4-Source-Pool          | OES2023-SLE-Module-Basesystem15-SP4-Source-Pool                | No      | ----      | ----
12 | nu_novell_com:OES2023-SLE-Module-Basesystem15-SP4-Updates              | OES2023-SLE-Module-Basesystem15-SP4-Updates                    | Yes     | (r ) Yes  | Yes
13 | nu_novell_com:OES2023-SLE-Module-Containers15-SP4-Debuginfo-Pool       | OES2023-SLE-Module-Containers15-SP4-Debuginfo-Pool             | No      | ----      | ----
14 | nu_novell_com:OES2023-SLE-Module-Containers15-SP4-Debuginfo-Updates    | OES2023-SLE-Module-Containers15-SP4-Debuginfo-Updates          | No      | ----      | ----
15 | nu_novell_com:OES2023-SLE-Module-Containers15-SP4-Pool                 | OES2023-SLE-Module-Containers15-SP4-Pool                       | Yes     | (r ) Yes  | Yes
16 | nu_novell_com:OES2023-SLE-Module-Containers15-SP4-Source-Pool          | OES2023-SLE-Module-Containers15-SP4-Source-Pool                | No      | ----      | ----
17 | nu_novell_com:OES2023-SLE-Module-Containers15-SP4-Updates              | OES2023-SLE-Module-Containers15-SP4-Updates                    | Yes     | (r ) Yes  | Yes
18 | nu_novell_com:OES2023-SLE-Module-Desktop-Applications15-SP4-Debuginfo-Pool    | OES2023-SLE-Module-Desktop-Applications15-SP4-Debuginfo-Pool    | No | ---- | ----
19 | nu_novell_com:OES2023-SLE-Module-Desktop-Applications15-SP4-Debuginfo-Updates | OES2023-SLE-Module-Desktop-Applications15-SP4-Debuginfo-Updates | No | ---- | ----
20 | nu_novell_com:OES2023-SLE-Module-Desktop-Applications15-SP4-Pool       | OES2023-SLE-Module-Desktop-Applications15-SP4-Pool             | No      | ----      | ----
21 | nu_novell_com:OES2023-SLE-Module-Desktop-Applications15-SP4-Source-Pool | OES2023-SLE-Module-Desktop-Applications15-SP4-Source-Pool     | No      | ----      | ----
22 | nu_novell_com:OES2023-SLE-Module-Desktop-Applications15-SP4-Updates    | OES2023-SLE-Module-Desktop-Applications15-SP4-Updates          | No      | ----      | ----
23 | nu_novell_com:OES2023-SLE-Module-DevTools15-SP4-Debuginfo-Pool         | OES2023-SLE-Module-DevTools15-SP4-Debuginfo-Pool               | No      | ----      | ----
24 | nu_novell_com:OES2023-SLE-Module-DevTools15-SP4-Debuginfo-Updates      | OES2023-SLE-Module-DevTools15-SP4-Debuginfo-Updates            | No      | ----      | ----
25 | nu_novell_com:OES2023-SLE-Module-DevTools15-SP4-Pool                   | OES2023-SLE-Module-DevTools15-SP4-Pool                         | No      | ----      | ----
26 | nu_novell_com:OES2023-SLE-Module-DevTools15-SP4-Source-Pool            | OES2023-SLE-Module-DevTools15-SP4-Source-Pool                  | No      | ----      | ----
27 | nu_novell_com:OES2023-SLE-Module-DevTools15-SP4-Updates                | OES2023-SLE-Module-DevTools15-SP4-Updates                      | No      | ----      | ----
28 | nu_novell_com:OES2023-SLE-Module-Legacy15-SP4-Debuginfo-Pool           | OES2023-SLE-Module-Legacy15-SP4-Debuginfo-Pool                 | No      | ----      | ----
29 | nu_novell_com:OES2023-SLE-Module-Legacy15-SP4-Debuginfo-Updates        | OES2023-SLE-Module-Legacy15-SP4-Debuginfo-Updates              | No      | ----      | ----
30 | nu_novell_com:OES2023-SLE-Module-Legacy15-SP4-Pool                     | OES2023-SLE-Module-Legacy15-SP4-Pool                           | No      | ----      | ----
31 | nu_novell_com:OES2023-SLE-Module-Legacy15-SP4-Source-Pool              | OES2023-SLE-Module-Legacy15-SP4-Source-Pool                    | No      | ----      | ----
32 | nu_novell_com:OES2023-SLE-Module-Legacy15-SP4-Updates                  | OES2023-SLE-Module-Legacy15-SP4-Updates                        | No      | ----      | ----
33 | nu_novell_com:OES2023-SLE-Module-Public-Cloud15-SP4-Debuginfo-Pool     | OES2023-SLE-Module-Public-Cloud15-SP4-Debuginfo-Pool           | No      | ----      | ----
34 | nu_novell_com:OES2023-SLE-Module-Public-Cloud15-SP4-Debuginfo-Updates  | OES2023-SLE-Module-Public-Cloud15-SP4-Debuginfo-Updates        | No      | ----      | ----
35 | nu_novell_com:OES2023-SLE-Module-Public-Cloud15-SP4-Pool               | OES2023-SLE-Module-Public-Cloud15-SP4-Pool                     | No      | ----      | ----
36 | nu_novell_com:OES2023-SLE-Module-Public-Cloud15-SP4-Source-Pool        | OES2023-SLE-Module-Public-Cloud15-SP4-Source-Pool              | No      | ----      | ----
37 | nu_novell_com:OES2023-SLE-Module-Public-Cloud15-SP4-Updates            | OES2023-SLE-Module-Public-Cloud15-SP4-Updates                  | No      | ----      | ----
38 | nu_novell_com:OES2023-SLE-Module-Python3-15-SP4-Debuginfo-Pool         | OES2023-SLE-Module-Python3-15-SP4-Debuginfo-Pool               | No      | ----      | ----
39 | nu_novell_com:OES2023-SLE-Module-Python3-15-SP4-Debuginfo-Updates      | OES2023-SLE-Module-Python3-15-SP4-Debuginfo-Updates            | No      | ----      | ----
40 | nu_novell_com:OES2023-SLE-Module-Python3-15-SP4-Pool                   | OES2023-SLE-Module-Python3-15-SP4-Pool                         | No      | ----      | ----
41 | nu_novell_com:OES2023-SLE-Module-Python3-15-SP4-Source-Pool            | OES2023-SLE-Module-Python3-15-SP4-Source-Pool                  | No      | ----      | ----
42 | nu_novell_com:OES2023-SLE-Module-Python3-15-SP4-Updates                | OES2023-SLE-Module-Python3-15-SP4-Updates                      | No      | ----      | ----
43 | nu_novell_com:OES2023-SLE-Module-Server-Applications15-SP4-Debuginfo-Pool    | OES2023-SLE-Module-Server-Applications15-SP4-Debuginfo-Pool    | No | ---- | ----
44 | nu_novell_com:OES2023-SLE-Module-Server-Applications15-SP4-Debuginfo-Updates | OES2023-SLE-Module-Server-Applications15-SP4-Debuginfo-Updates | No | ---- | ----
45 | nu_novell_com:OES2023-SLE-Module-Server-Applications15-SP4-Pool        | OES2023-SLE-Module-Server-Applications15-SP4-Pool              | Yes     | (r ) Yes  | Yes
```

8.4.3 Registering the Server in the Customer Center Using the GUI

1 In the **YaST Control Center**, under **Supports** > **Customer Center Configuration**.

2 On the Customer Center Configuration configuration page, select all of the following options, then click **Next**.

- **Configure Now:** Proceeds with registering this server and the OES product with the Customer Center.
- **Hardware Profile:** Sends information to the Customer Center about the hardware that you are installing OES on.
- **Optional Information:** Sends optional information to the Customer Center for your registration. For this release, this option doesn't send any additional information.
- **Registration Code** Makes the registration with activation codes mandatory.

- **Regularly Synchronize with the Customer Center:** Keeps the installation sources for this server valid. It does not remove any installation sources that were manually added.

After you click **Next**, the **Contacting Server** message is displayed. Wait until this message disappears and the Manual Interaction Required page displays.

3. On the Manual Interaction Required page, note the information that you will be required to specify, then click **Continue**.
4. On the Customer Center Registration page, specify the required information in the following fields:
   - **Email Address:** The e-mail address for your Login account.
   - **Confirm Email Address:** The same e-mail address for your Login account
   - **Open Enterprise Server 24.4(optional):** Specify your purchased or 60-day evaluation registration code for the OES product.

     If you don't specify a code, the server cannot receive any updates or patches.
   - **System Name or Description (optional):** The hostname for the system is specified by default. If you want to change this to a description for the Customer Center, specify a description to identify this server.
5. Click **Submit**.
6. When the message to complete the registration displays, click **Continue**.

   After you click **Continue**, the **Contacting Server** message is displayed with the Manual Interaction Required page. Wait until this message disappears and the Customer Center Configuration Was Successful page displays.
7. When you see the message that the Customer Center was successful, click **OK**.

When the registration is successful, the server is registered in the Customer Center and the installation sources for patches are configured on the server.

8.5 Updating the Server

After the server has been registered in the Customer Center, you can apply the patches. The default GNOME desktop indicates when there are updates available to the server. You can update the server from any of the following interfaces.

- Section 8.5.1, "Updating the Server Using the Command Line," on page 145
- Section 8.6, "GUI Based Patching," on page 148

You could also patch an OES server using Section 8.8, "Patching From Behind a Proxy Server," on page 149.

8.5.1 Updating the Server Using the Command Line

After you have registered the server in the Customer Center, you can update the server by using commands at the command line. The following procedure specifies steps for updating the server with all available patches for OES.

1. Log in to the server as `root` or `su` to `root`.
2. At the command line, enter the following commands.

   2a Refresh all services:

   ```
   zypper ref -s
   ```

   The list of repositories should include the following update repositories:

   Enabled Repositories

   - OES24.4-Pool
   - OES24.4-SLE-Module-Basesystem15-SP4-Pool
   - OES24.4-SLE-Module-Basesystem15-SP4-Updates
   - OES24.4-SLE-Module-Containers15-SP4-Pool
   - OES24.4-SLE-Module-Containers15-SP4-Updates
   - OES24.4-SLE-Module-Desktop-Applications15-SP4-Pool
   - OES24.4-SLE-Module-Desktop-Applications15-SP4-Updates
   - OES24.4-SLE-Module-Server-Applications15-SP4-Pool
   - OES24.4-SLE-Module-Server-Applications15-SP4-Updates
   - OES24.4-SLE-Product-SLES15-SP4-Pool
   - OES24.4-SLE-Product-SLES15-SP4-Updates
   - OES24.4-Updates

   Optional/Disabled Repositories

   - OES24.4-SLE-Manager-Tools15-Debuginfo-Pool
   - OES24.4-SLE-Manager-Tools15-Debuginfo-Updates
   - OES24.4-SLE-Manager-Tools15-Pool
   - OES24.4-SLE-Manager-Tools15-Source-Pool
   - OES24.4-SLE-Manager-Tools15-Updates
   - OES24.4-SLE-Module-Basesystem15-SP4-Debuginfo-Pool
   - OES24.4-SLE-Module-Basesystem15-SP4-Debuginfo-Updates
   - OES24.4-SLE-Module-Basesystem15-SP4-Source-Pool
   - OES24.4-SLE-Module-Containers15-SP4-Debuginfo-Pool
   - OES24.4-SLE-Module-Containers15-SP4-Debuginfo-Updates
   - OES24.4-SLE-Module-Containers15-SP4-Source-Pool
   - OES24.4-SLE-Module-Desktop-Applications15-SP4-Debuginfo-Pool
   - OES24.4-SLE-Module-Desktop-Applications15-SP4-Debuginfo-Updates
   - OES24.4-SLE-Module-Desktop-Applications15-SP4-Updates
   - OES24.4-SLE-Module-DevTools15-SP4-Debuginfo-Pool

- OES24.4-SLE-Module-DevTools15-SP4-Debuginfo-Updates
- OES24.4-SLE-Module-DevTools15-SP4-Pool
- OES24.4-SLE-Module-DevTools15-SP4-Source-Pool
- OES24.4-SLE-Module-DevTools15-SP4-Updates
- OES24.4-SLE-Module-Legacy15-SP4-Debuginfo-Pool
- OES24.4-SLE-Module-Legacy15-SP4-Debuginfo-Updates
- OES24.4-SLE-Module-Legacy15-SP4-Pool
- OES24.4-SLE-Module-Legacy15-SP4-Source-Pool
- OES24.4-SLE-Module-Legacy15-SP4-Updates
- OES24.4-SLE-Module-Public-Cloud15-SP4-Debuginfo-Pool
- OES24.4-SLE-Module-Public-Cloud15-SP4-Debuginfo-Updates
- OES24.4-SLE-Module-Public-Cloud15-SP4-Pool
- OES24.4-SLE-Module-Public-Cloud15-SP4-Source-Pool
- OES24.4-SLE-Module-Public-Cloud15-SP4-Updates
- OES24.4-SLE-Module-Python3-15-SP4-Debuginfo-Pool
- OES24.4-SLE-Module-Python3-15-SP4-Debuginfo-Updates
- OES24.4-SLE-Module-Python3-15-SP4-Pool
- OES24.4-SLE-Module-Python3-15-SP4-Source-Pool
- OES24.4-SLE-Module-Python3-15-SP4-Updates
- OES24.4-SLE-Module-Server-Applications15-SP4-Debuginfo-Pool
- OES24.4-SLE-Module-Server-Applications15-SP4-Debuginfo-Updates
- OES24.4-SLE-Module-Server-Applications15-SP4-Source-Pool
- OES24.4-SLE-Module-Web-Scripting15-SP4-Debuginfo-Pool
- OES24.4-SLE-Module-Web-Scripting15-SP4-Debuginfo-Updates
- OES24.4-SLE-Module-Web-Scripting15-SP4-Pool
- OES24.4-SLE-Module-Web-Scripting15-SP4-Source-Pool
- OES24.4-SLE-Module-Web-Scripting15-SP4-Updates
- OES24.4-SLE-Product-SLES15-SP4-Debuginfo-Pool
- OES24.4-SLE-Product-SLES15-SP4-Debuginfo-Updates
- OES24.4-SLE-Product-SLES15-SP4-Source-Pool

2b See whether updates are available for OES 24.4:

```
zypper patch-check
```

This command search for the patches in all enabled repositories on the system.

To view the updates available on a specific repository, you can run the command as follows:

```
zypper patch-check --repo catalog1 --repo catalog2
```

For example,

```
zypper patch-check --repo OES24.4-Updates
```

```
zypper patch-check --repo OES24.4-SLE-Product-SLES15-SP4-Updates --
repo OES24.4-SLE-Module-Basesystem15-SP4-Updates
```

2c Update the server with all available OES patches:

```
zypper patch
```

2d Repeat Step 2b and Step 2c until no more updates are available.

2e If the patching requires a server reboot, do so when intimated by the system.

Rebooting the server activates the new kernel if it has been updated and ensures that OES services that need restarting after patching are restarted.

IMPORTANT: Always use the `zypper patch` command to update an OES server.

For more information on zypper, see SDB:Zypper usage 11.3 (http://en.opensuse.org/SDB:Zypper_usage_11.3).

You can also update your server with specific maintenance patches.

1. Log in to the server as `root` or `su` to `root`.
2. At the command line, enter the following commands:

2a To refresh all services, enter:

```
zypper ref -s
```

2b To check for available updates, enter:

```
zypper lu
```

2c To list the patches and their status, enter:

```
zypper pch
```

2d To view specific patch information, enter:

```
zypper patch-info patch_name
```

For example:

```
zypper patch-info SUSE-SLE-Module-Basesystem-15-SP4-2022-3307
```

2e To list all installed patches, enter:

```
zypper search -t patch -i
```

2f To update the server with specific patches, choose from the following:

- To install all patches from one or more catalogs of a particular category:

  ```
  zypper patch -g category_name
  ```

  Replace *category_name* with security, recommended, or optional.

  For example:

  ```
  zypper patch -g security
  ```

- To install one version of a patch without confirmation, enter:

  ```
  zypper --non-interactive in -t patch patch_name-version
  ```

  For example:

  ```
  zypper --non-interactive in -t patch SUSE-SLE-Module-Basesystem-
  15-SP4-2022-3307
  ```

- To install all versions of a patch, enter:

  `zypper in -t patch patch_name*`

2g If the update requires a server reboot, do so when intimated by the system. This ensures that any changes to the kernel are activated, and applicable OES services are restarted.

8.6 GUI Based Patching

After you have registered the server in the Customer Center, you can update the server by using the user interface. The following procedure specifies steps for updating the server with all available patches for OES.

1. Log in to the server as `root` or `su` to `root`.
2. In the YaST Control Center, under **Software**, click **Software Repositories**.
3. Verify if the following repositories are available and click **OK**.
   - OES24.4-Pool
   - OES24.4-SLE-Module-Basesystem15-SP4-Pool
   - OES24.4-SLE-Module-Basesystem15-SP4-Updates
   - OES24.4-SLE-Module-Containers15-SP4-Pool
   - OES24.4-SLE-Module-Containers15-SP4-Updates
   - OES24.4-SLE-Module-Desktop-Applications15-SP4-Pool
   - OES24.4-SLE-Module-Desktop-Applications15-SP4-Updates
   - OES24.4-SLE-Module-Server-Applications15-SP4-Pool
   - OES24.4-SLE-Module-Server-Applications15-SP4-Updates
   - OES24.4-SLE-Product-SLES15-SP4-Pool
   - OES24.4-SLE-Product-SLES15-SP4-Updates
   - OES24.4-Updates
4. In the YaST Control Center, under **Software**, click **Online Update**.
5. If the screen displays the 'End of General Support' message, click **OK**. If not, proceed to Step 6. This issue is fixed for OES 24.4.1 and later versions.
6. Select the patches you want to apply and click **Accept**.
7. If the patching requires a server reboot, do so when intimated by the system.

   Rebooting the server activates the new kernel if it has been updated and ensures that OES services that need restarting after patching are restarted.

NOTE: If there is any zypper patch available at the time of update, the zypper patch is updated before updating the selected OES patches.

8.7 Frequently Asked Questions about Updating

This section contains the following information:

- Section 8.7.1, “Do I apply all the patches in the catalogs? How do I know which patches to apply?,” on page 149

8.7.1 Do I apply all the patches in the catalogs? How do I know which patches to apply?

Each patch has a category and a status associated with it. The categories state whether the patch is a security patch, a recommended patch, or an optional patch. The `zypper pch` command shows whether the patch is needed or not needed and whether it has been applied. When you are using the Novell Updater, only the patches that are needed and have not been applied display in the list of patches.

Therefore, you can just apply all the security patches and wait to apply other patches that might change how a feature or product works.

8.8 Patching From Behind a Proxy Server

See TID 7006845.

8.9 Using SUSE Manager to Patch an OES Server

SUSE Manager supports salt method of registration for the OES clients. For more information on SUSE Manager, see the SUSE Manager documentation.

You can use SUSE Manager to patch an OES server.

- Section 8.9.1, “Setting Up SUSE Manager,” on page 149
- Section 8.9.2, “Patching an OES 2018 or Later Server Using SUSE Manager,” on page 151

NOTE: By applying the patch, an OES server is updated to the latest OES version.

8.9.1 Setting Up SUSE Manager

Use the information contained in the following sections to set up a SUSE Manager server:

- “Installing SUSE Manager” on page 150
- “Mirroring the Required OES Channels” on page 150
- “Creating Activation Keys and Registering Clients” on page 151

Installing SUSE Manager

For more information about installing, patching, and mirroring, see the SUSE Manager Getting Started Guide.

1. Install SUSE Manager.
2. Patch SUSE Manager before configuring it.
3. Configure SUSE Manager. Ensure to provide the appropriate mirror credentials to access the OES and SLES channels.

Mirroring the Required OES Channels

1. Mirror the OES 24.4 channels. For more information on mirroring the channels, see Syncing Products from SUSE Customer Center.
   - OES24.4-Pool
   - OES24.4-SLE-Manager-Tools15-Pool for x86_64
   - OES24.4-SLE-Manager-Tools15-Updates for x86_64
   - OES24.4-SLE-Module-Basesystem15-SP4-Pool
   - OES24.4-SLE-Module-Basesystem15-SP4-Updates
   - OES24.4-SLE-Module-Containers15-SP4-Pool
   - OES24.4-SLE-Module-Containers15-SP4-Updates
   - OES24.4-SLE-Module-Desktop-Applications15-SP4-Pool
   - OES24.4-SLE-Module-Desktop-Applications15-SP4-Updates
   - OES24.4-SLE-Module-Server-Applications15-SP4-Pool
   - OES24.4-SLE-Module-Server-Applications15-SP4-Updates
   - OES24.4-SLE-Product-SLES15-SP4-Pool
   - OES24.4-SLE-Product-SLES15-SP4-Updates
   - OES24.4-Updates
2. (Conditional) If this is the first time the OES channel is mirrored, the following error message is displayed:

   ```
   ChannelException: The GPG key for this repository is not part of the
   keyring.
   Please run spacewalk-repo-sync in interactive mode to import it.
   ```

   Use the following steps to resolve the issue:

   2a Run the `spacewalk-repo-sync -c <any-oes-channel-name>` command.

   For example, `spacewalk-repo-sync -c oes2023-pool-x86_64`.

   2b When prompted to import the keys, import the keys and continue with Step 1.

   After the keys are imported, other OES channels are mirrored without any issues.

Creating Activation Keys and Registering Clients

For information on how to create activation keys and register clients, see Registering Clients in the SUSE Manager Documentation.

8.9.2 Patching an OES 2018 or Later Server Using SUSE Manager

1. Ensure that you have completed Setting Up SUSE Manager.
2. Log in to the SUSE Manager Web console (`https://<SUSE Manager Server_hostname or IP_address>`) with administrative credentials.
3. Click **Systems**.

   SUSE Manager lists all the registered OES servers along with the number of patches available for each OES server.
4. Select the OES server, click **Software** > **Software Channels**, and then verify that the required channels are selected.
5. To apply a patch, select the OES server, click **Software** > **Patches**, select all the patches, then click **Apply patches** > Schedule the patch > **Confirm**.

   The **Schedule** tab shows the status of the selected patches. Once all the patches are updated, you must reboot the system.

8.10 Using ZENworks Server to Patch an OES Server

The ZENworks server allows you to perform an unattended, online patching of Open Enterprise Server (OES) by using ZENworks.

NOTE: By applying the patch, an OES server is updated to the latest OES version.

For more information on how to patch an OES server using ZENworks server, see Patching OES 24.4 Server by Using a ZENworks 24.4 Server.

8.11 Installing the Latest iManager NPMs After Applying OES Patches

In an OES environment, applying the latest OES patches does not install the latest iManager NPMs automatically. They will have to be manually installed.

To install the latest iManager NPMs:

1. Ensure that you have applied all the available OES patches.
2. Log on to iManager with admin privileges.
3. Click **Configure > Plug-Installation > Available Novell Plug-in Modules**.

4 Under the **Version** column, select all the modules that have version 3.2 or above associated with it and the following iManager framework modules: iManager Base Content, iManager Framework and iManager Framework Content, then click **Install**.

5 After successfully installing all the NPMs, restart tomcat using the `systemctl restart novell-tomcat.service` command.

NOTE: Ensure to install the latest version of iManager NPMs. Even though the older version of iManager NPMs can be installed successfully on OES 2018 SP2 or later server, they would not contain the latest UI changes.

8.12 Restarting the OES Instance of Tomcat After Applying a Tomcat Update

Whenever there is an update to Tomcat, ensure to restart the OES instance of Tomcat using the `rcnovell-tomcat restart` or `systemctl restart novell-tomcat.service` command. This loads all the latest libraries.

9 Using AutoYaST to Install and Configure Multiple OES Servers

If you need to install OES to multiple systems that perform similar tasks and that share the same environment and similar but not necessarily identical hardware, you might want to use AutoYaST to perform the installation.

To use AutoYaST, first you use the Configuration Management tool (**YaST** > **Miscellaneous** > **Autoinstallation**) to generate an XML profile file (referred to as a control file) and use it to perform OES installations to multiple servers that share the same hardware and environments. You can also tailor this control file for any specific environment. You then provide this control file to the YaST2 installation program.

This section does not provide complete AutoYaST instructions. It provides only the additional information you need when setting up AutoYaST to install multiple OES 24.4 or later servers.

For complete instructions on using AutoYaST2, see AutoYaST Guide. You can also access the documentation locally on an OES server in `/usr/share/doc/packages/autoyast2/html/index.html`.

You can also use the cloning option to create clones of a particular installation. To clone a system:

Select **Clone This System for Autoyast** at the end of the installation.

Or

Use the command `yast2 clone_system` post installation.

This creates `/root/autoinst.xml` that can be used for cloning. For more information, see SUSE AutoYast Guide.

This section contains the following information:

- Section 9.1, “Prerequisites,” on page 153
- Section 9.2, “Setting Up a Control File with OES Components,” on page 154
- Section 9.3, “Setting Up an Installation Source,” on page 159
- Section 9.4, “Cloning an OES Server Post OES Installation and Configuration,” on page 159

9.1 Prerequisites

You need at least the following components to install an OES 24.4 server by using AutoYaST:

- ❒ A server with OES 24.4 already installed.
- ❒ One or more target computers to install the server software to and the following information about each:
  - Number of hard disks

- MAC address
- Monitor types and graphics hardware

❒ A control file.

For information on setting up a control file with OES components, see "Setting Up a Control File with OES Components" on page 154.

❒ A boot scenario set up.

You can boot from media or from an installation source. For more information, see "Setting Up an Installation Source" on page 159.

❒ A source or server that contains the AutoYaST profile (control file).

For more information, see "Setting Up an Installation Source" on page 159.

9.2 Setting Up a Control File with OES Components

The control file is an XML file that contains an installation profile for the target computer. This installation profile contains all the information to complete software installation and configuration on the target computer.

To create a control file:

- You can create the control file manually in a text editor (not recommended).
- When you complete an installation, you can click **Clone for AutoYaST**. If you use this option, the resulting file is `/root/autoinst.xml`. This file must be edited manually before using it.
- You can create or modify a control file by using the AutoInstallation module in YaST. For procedures, see Section 9.2.1, "Using the AutoInstallation Module to Create the Control File," on page 154.

  This system depends on existing modules that are usually used to configure a computer after OES 24.4 is installed on a server.

9.2.1 Using the AutoInstallation Module to Create the Control File

The following procedure contains a quick list of steps to create the control file by using the AutoInstallation module in YaST on a server running OES 24.4.

1. On a server that has OES 24.4installed, click **Computer > YaST Administrator Settings**.
2. Click **Miscellaneous** > **Autoinstallation**.

   The AutoYaST Configuration Management System application window opens, referred to hereafter as the *main window*.
3. Click **Tools** > **Create Reference Profile**.
4. In the Create a Reference Control File dialog box under **Select Additional Resources**, select the **Network Settings** check box, then click **Create**.

   AutoYaST probes the server it is running on for software, partitioning, boot loader, network card information, language settings, mouse, and other system settings. After the information has been collected, the status messages cease and only the main window is displayed.

5 Verify the package selections:

5a In the left frame of the main window, click **Software**, then under **Available Modules**, click **Package Selection**.

5b On the Package Selection page, make sure the items are the same as you previously installed on the server. For more information on the add-ons (software selections) that are selected in the base selections or patterns, see "Deciding What Patterns to Install" on page 25. If the configuration contains the packages and selections you need, skip to Step 7. If not, continue with Step 6.

6 If necessary, change the package selections for the target servers:

6a In the Package Selection dialog box, click **Configure**.

6b On the Software Selection page, click **Patterns** in the **Filter** field.

6c Select the specific software items that you want to be added, then click **Accept**.

6d If you are prompted to accept the End User License Agreement, click **Accept**.

6e Accept the automatic changes by clicking **Continue** in the Changed Packages dialog box.

7 Specify the Partitioning parameters for the target server:

7a In the left frame of the main window, click **Hardware**, under **Available Modules**, click **Partitioning**, then click the **Edit** button.

7b Set up partitioning on the first drive as desired, then click **Finish**.

See the online help for details about limitations.

For more information on partitioning options, see Partitioning" in Automatic Linux Installation and Configuration with Yast2.

8 Specify the settings for the graphics card and monitor:

8a In the left frame of the main window, click **Hardware**, under **Available Modules**, click **Graphics Card and Monitor**, then click the **Configure** button.

8b In the **General Options** field of the X11 Configuration page, specify the settings that you want.

8c In the **Desktop** field of the X11 Configuration page, select the settings that you want for the Display Manager and Window Manager, then click **Next**.

8d On the Configure Monitor page, select the applicable monitor vendor and model, then click **Next**.

8e Verify the X11 settings. If they are not correct, repeat Step 8a and Step 8d.

If you skip this step, the server keyboard mappings might be German.

9 (Optional) Insert a script to perform a task that you want, such as a script for removing partitions:

For more information on custom user scripts, see "Custom User Scripts" (https://documentation.suse.com/sles/15-SP4/single-html/SLES-autoyast/#createprofile-scripts) in *SUSE Auto YaST guide (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-autoyast.html)*.

9a In the main window, click **Miscellaneous** > **Custom Scripts** > **Configure**.

9b On the User Script Management page, click **New**.

9c In the **File Name** field, specify a descriptive name for the script, such as `hello_world_script`.

9d In the **Script Source** field, specify commands such as the following example script:

```
#!/bin/sh
'echo "hello world" > /tmp/post-script-output'
```

9e Click the **Type** drop-down box, then select **Post**.

This script runs after the installation is complete. For additional options, see the online help for this dialog box.

9f Click **Save**.

9g Make sure your script appears in the **Available Scripts** section of the User Script Management page, then click **Finish**.

9h Make sure your script appears in the **Post Scripts** section of the Custom Scripts page.

10 Set the password for the `root` user:

10a From the main window, click **Security and Users > User Management** > **Configure**.

10b Click **Set Filter**, then select **Select System Users** from the drop-down menu.

10c Select user **root**, then click **Edit**.

10d Type a password for the `root` user in the **Password and Verify Password** fields, click **Accept**, then click **Finish**.

10e Verify that the `root` user appears in the **Users** section of the **User Management** dialog box.

11 Configure OES Services:

11a From the main window, click **Open Enterprise Server** > *module_name* > **Configure**.

All OES services are in the Open Enterprise Server category.

We recommend configuring eDirectory first. Although there are dependencies for some of the components, in this release AutoYaST does not verify whether one module is configured or not.

See the following table for category names and dependencies. You should configure all the modules that were selected for the software selections in Step 5 on page 155. For more information about which modules are in each pattern, see "Deciding What Patterns to Install" on page 25.

Pattern	Other Module Dependencies
OES Backup/Storage Management Services (SMS)	◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
OES Business Continuity Cluster (BCC)	◆ OES Cluster Services (NCS) ◆ OES Linux User Management (LUM) ◆ OES Backup/Storage Management Services (SMS) ◆ OES Remote Manager (NRM)

Pattern	Other Module Dependencies
OES CIFS	◆ OES Backup / Storage Management Services (SMS) ◆ OES eDirectory ◆ OES Storage Services (NSS) ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM) ◆ OES NCP Server
OES Cluster Services (NCS)	◆ OES Backup/Storage Management Services (SMS) ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
OES DHCP	◆ OES Backup/Storage Management Services (SMS) ◆ OES eDirectory ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
OES DNS	◆ OES Backup/Storage Management Services (SMS) ◆ OES eDirectory ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
OES Domain Services for Windows	◆ OES Backup / Storage Management Services (SMS) ◆ OES eDirectory ◆ OES DNS ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
OES eDirectory	◆ OES Backup/Storage Management Services (SMS) ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
OES FTP	◆ OES Backup/Storage Management Services (SMS) ◆ OES eDirectory ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
NetIQ iManager	◆ OES Backup/Storage Management Services (SMS) ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)
iPrint Advanced	◆ OES Backup/Storage Management Services (SMS) ◆ OES Linux User Management (LUM) ◆ OES Remote Manager (NRM)

Pattern	Other Module Dependencies
OES Linux User Management (LUM)	• OES Backup/Storage Management Services (SMS) • OES Remote Manager (NRM)
OES NCP Server / Dynamic Storage Technology	• OES Backup/Storage Management Services (SMS) • OES eDirectory • OES Linux User Management (LUM) • OES Remote Manager (NRM)
OES Pre-Migration Server	• OES Backup / Storage Management Services (SMS) • OES eDirectory (without a replica) • OES Linux User Management (LUM) • OES Remote Manager (NRM)
OES Remote Manager (NRM)	• OES Backup/Storage Management Services (SMS) • OES Linux User Management (LUM)
OES Storage Services (NSS)	• OES Backup/Storage Management Services (SMS) • OES eDirectory • OES NCP Server • OES Linux User Management (LUM) • OES Remote Manager (NRM)
OES Storage Service AD Support	• OES Backup/Storage Management Services (SMS) • OES eDirectory • OES NCP Server • OES Storage Services (NSS) • OES CIFS Services • OES Linux User Management (LUM) • OES Remote Manager (NRM)
OES Unified Management Console (UMC)	• OES Backup/Storage Management Services (SMS) • OES eDirectory • OES Linux User Management (LUM) • OES Remote Manager (NRM) • OES Database
OES MFA Server (MFA)	• OES eDirectory

11b Type or select the information for each field requested on each page, then click **Next** until a summary of settings is displayed for that service.

11c Verify that the settings for each module are what you want.

If not, click **Reset Configuration** and provide the corrected settings.

11d Repeat Step 11a through Step 11c until all the required modules have been configured, then continue with Step 12.

12 Save the file.:

12a Click **File** > **Save**.

12b Browse to a location that you want to save the file to.

12c Type *`filename`*`.xml`, then click **Save**.

Replace *filename* with an appropriate name to identify the control file for the installation you are performing.

By default, the file is saved in the `/var/lib/autoinstall/repository/` directory.

For additional filename requirements and recommendations, see "The Auto-Installation Process" in *Automatic Linux Installation and Configuration with Yast2*.

13 Exit the configuration management tool by clicking **File** > **Exit**.

14 Proceed with "Setting Up an Installation Source" on page 159.

9.3 Setting Up an Installation Source

For OES 2018 or later, you must set up a separate directory for the SLES 12 SP2 or later software and the OES 2018 or later software.

AutoYaST requires an installation source. You have several options. For an explanation of each, see "The Auto-Installation Process" in the SUSE AutoYast Guide.

9.4 Cloning an OES Server Post OES Installation and Configuration

This section describes the procedures to clone an OES server post OES installation and configuration. When there is a server crash, you can use this procedure to reinstall the server with the same configurations that existed before the crash. This is a two step task: generate the `autoinst.xml` file post OES installation and configuration, use that XML file to reinstall and configure the server.

9.4.1 Generating the autoinst.xml File

The autoinst.xml file contains all the configuration details of the components, passwords, IP address, and so on. Store this file in a secure location, and use it to reinstall and reconfigure your OES server when there is a crash.

To generate the `autoinst.xml` file:

1 Log on to the OES server with administrative privileges and execute the following command: `yast2 clone_system`.

This generates an `autoinst.xml` file at `/root`. Generate this file as and when you make some configuration changes to the server.

2 Store this file in a secure location for future use.

NOTE: The generated `autoinst.xml` file will have the XML tags of the OES components that you have not installed and configured. This does not affect any functionality. When you use the generated `autoinst.xml` file, only the components that are available under the `<patterns>` tag will be installed.

9.4.2 Using the autoinst.xml to Install or Reinstall an OES Server

To install or reinstall an OES server using autoinst.xml:

1 Edit the `autoinst.xml` file, and modify the following:

- Replace all instances of “Replace this text with the real password” with eDirectory password.
- Specify eDirectory password inside `runtime_admin_password` and `admin_password` under `oes-ldap` tag.
- If you install or re-install DSfW server, see Installing DSfW Using AutoYaST.
- Locate and remove the entire `net-udev` section that has the details about the MAC address.

```
<net-udev config:type="list">
    <rule>
        <name>eth0</name>
        <rule>ATTR{address}</rule>
        <value>00:0c:29:4d:e0:72</value>
    </rule>
</net-udev>
```

- Locate and remove the user and group gdm entries. For more information, see TID 7006641 Error: Could not update ICEauthority file /var/lib/gdm/.ICEauthority (http://www.novell.com/support/kb/doc.php?id=7006641).

```
<group>root
     <encrypted config:type="boolean">true</encrypted>
     <gid>112</gid>
     <group_password>!</group_password>
     <groupname>gdm</groupname>
     <userlist></userlist>
</group>

<user>
     <encrypted config:type="boolean">true</encrypted>
     <fullname>Gnome Display Manager daemon</fullname>
     <gid>112</gid>
     <home>/var/lib/gdm</home>
     <password_settings>
       <expire></expire>
       <flag></flag>
       <inact></inact>
       <max>99999</max>
       <min>0</min>
       <warn>7</warn>
     </password_settings>
     <shell>/bin/false</shell>
     <uid>107</uid>
     <user_password>*</user_password>
     <username>gdm</username>
   </user>
```

2 Host the modified `autoinst.xml` file in a HTTP server.

3 Boot the OES server with `OES24.4-DVD-x86_64-DVD1.iso`.

4 In the installation screen, select **Install**, and specify the following information:

```
autoyast=<The HTTP location where the autoinst.xml file is hosted>
netsetup=hostip hostip=<enter machine IP> netmask=<enter the netmask>
gateway=<enter the gateway>
```

or

```
autoyast=<The HTTP location where the autoinst.xml file is hosted>
ifcfg="eth0=<ip_address/<netmask>, <gateway>, <nameserver>"
sethostname=0 install=<install_source_location_if_network_based>
```

For example:

```
autoyast=http://198.162.1.1/autoinst.xml netsetup=hostip
hostip=192.168.1.2 netmask=255.255.254.0 gateway=192.164.1.254
```

or

```
autoyast=http://198.162.1.1/autoinst.xml ifcfg="eth0=192.168.1.2/23,
192.164.1.254, 192.164.1.1" sethostname=0
```

5 Press **Enter** and the OES installation and configuration starts and completes without any user intervention.

If OES is running in a UEFI Secure Boot environment, you need to perform additional steps, see Chapter 11, “Deploying OES in a UEFI Secure Boot Environment,” on page 169.

NOTE: Cloud Integrated Storage (CIS) does not work, if autoinst.xml file is copied from already installed and configured OES 2018 or later server (without CIS) and manually add the CIS tags into autoinst.xml and then install OES 2018 or later server using the modified autoinst.xml. For CIS to work, along with adding the CIS tags, ensure to enable the `ipv4_forward` and `FW_MASQUERADE` attributes under firewall section in the autoinst.xml file and then install the OES 2018 or later server.

For example:

```
<ipv4_forward config:type="boolean">true</ipv4_forward>
```

```
<FW_MASQUERADE>yes</FW_MASQUERADE>
```

However, if OES 2018 or later server is installed using autoinst.xml created from already installed OES 2018 or later server (with CIS), then CIS works fine.

---

10 Installing OES on a VM

In Open Enterprise Server (OES), you can install OES as a guest operating system on the SUSE Linux Enterprise Server (SLES) 15 SP4 Linux servers running the following:

- KVM

  See Introduction to KVM Virtualization in the Virtualization Guide.

- Xen

  See Introduction to Xen Virtualization in the Virtualization Guide.

For general information on the virtualization technology in SLES 15 SP4, see the SLES 15 documentation.

You can install OES as a guest operating system on the following hypervisors, which run with the latest versions:

- VMware

  See Introduction to VMware vSphere Virtual Machines in the VMware vSphere Documentation.

- Hyper-V

  See Hyper-V on Windows Server in the Virtualization documentation.

- Citrix Xen

  See Citrix Hypervisor in the Citrix Product documentation.

- Proxmox

  See Proxmox VE Documentation in the Proxmox Virtual Environment.

- Nutanix

  See Nutanix VM (AHV) in the Software Documentation.

  To set up the boot device for a UEFI VM, see Setting up Boot Device in the AHV Administration Guide.

This section documents the system requirements, installation instructions, upgrade and migration instructions, and issues associated with setting up OES server on a Xen-based virtual machine.

- Section 10.1, “System Requirements,” on page 164
- Section 10.2, “Prerequisites,” on page 165
- Section 10.3, “Preparing the Installation Software,” on page 165
- Section 10.4, “Installing an OES 24.4 VM Guest,” on page 165
- Section 10.5, “Setting Up an OES VM Guest to Use Novell Storage Services (NSS),” on page 167

10.1 System Requirements

To create an OES VM guest, you need a SLES 15 SP3 or later server that is set up as a VM host server.

- Section 10.1.1, “VM Host Considerations,” on page 164
- Section 10.1.2, “OES Storage Services Considerations,” on page 164
- Section 10.1.3, “Setup Instructions,” on page 164

10.1.1 VM Host Considerations

When you set up a virtual machine host for OES VM guests, ensure that the host server has the following:

- **Time synchronization:** Set the server’s time configuration to the same reliable, external time source as the eDirectory tree that the virtual machines on that host will be joining.

  To set the time source, use **Yast > NTP Configuration**.

  The time source can be running NTP or Timesync with the NTP option selected.
- **RAM:** Enough memory to support each virtual machine that you want to run concurrently on the host server.

  For example, if you are installing one OES virtual machine, you need a minimum of 2 GB of memory (1 GB for the host plus 1GB for the OES Linux VM).

  If you are installing two virtual machines, and the first VM guest’s services need 1 GB and the second guest’s need 1.5 GB, you need 2.5 GB for the VM guests and 1 GB for the host—a total of 3.5 GB.
- **Disk Space:** Enough disk space on the host for creating and running your VM guests.

  The default disk space required for an OES VM guest is 7 GB and the default allocation for each VM guest in Xen is 10 GB, leaving only approximately 6 GB for data files, etc. The space you need is dependent on what you plan to use the virtual server for and what other virtual storage devices, such as NSS volumes, that you plan to attach to it.
- **SLES Platform:** OES 2018 or later VM is tested as guest on SLES 15 SP3 or later VM hosts.

10.1.2 OES Storage Services Considerations

If you want to set up Novell Storage Services (NSS) on the virtual machine, note the following:

NSS can recognize physical, logical, or virtual devices.

For information, see “Device Size” in the *Storage Services File System (NSS) Administration Guide for Linux*.

10.1.3 Setup Instructions

For setup procedures, see the *Virtualization Guide* (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-virtualization.html).

10.2 Prerequisites

Before creating an OES virtual machine, you need the following:

- If you want to use AutoYaST to specify the Installation settings, create an AutoYaST profile (control) file and download it to a directory on the host machine server or make it available on the network. For more information, see Chapter 9, “Using AutoYaST to Install and Configure Multiple OES Servers,” on page 153.
- A static IP address for each virtual server that you want to create.

10.3 Preparing the Installation Software

- Section 10.3.1, “Downloading the Installation Software,” on page 165
- Section 10.3.2, “Preparing the Installation Source Files,” on page 165

10.3.1 Downloading the Installation Software

For information on downloading the following ISO image files, see Section 2.8, “Preparing Physical Media for a New Server Installation,” on page 33.

10.3.2 Preparing the Installation Source Files

To create an OES 24.4 VM guest, you must make the installation software available in one of the following locations:

- **A Local Installation Source:** The 64-bit ISO files copied to the host server’s local drives.
- **A Network Installation Source:** The 64-bit ISO files used to create a network installation source. For instructions, see Setting Up the Server Holding the Installation Sources in the SLES Deployment Guide.

10.4 Installing an OES 24.4 VM Guest

Creating an OES 24.4 virtual machine requires you to complete the following major tasks.

- Section 10.4.1, “Specifying Options for Creating an OES 24.4 VM Guest,” on page 165

10.4.1 Specifying Options for Creating an OES 24.4 VM Guest

The Create Virtual Machine Wizard helps you through the steps required to create a VM guest and install the desired operating system.

1. Launch the Create Virtual Machine Wizard by using one of the following methods:
   - From the virtualization host server desktop, click **YaST > Virtualization > Create Virtual Machines**
   - From within Virtual Machine Manager, click **New**.
   - At the command line, enter `vm-install`.

If the wizard does not appear or the `vm-install` command does not work, review the process of installing and starting the virtualization host server. The virtualization software might not be installed properly.

2 After specifying that you want to create a virtual machine, click **Forward**.

3 Click **Forward**.

The option to set up a virtual machine based on an existing disk or disk image is supported only if the existing disk or disk image was originally set up through the Create Virtual Machine Wizard.

4 On the Type of Operating System page, select the supported version of SLES for the OES, then click **Forward**.

The Summary page is displayed.

NOTE: Detailed explanations of the Summary page settings are available in "Virtualization: Configuration Options and Settings (https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-xen-config.html)" in the *Virtualization guide (https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-virtualization.html)*.

---

5 Click **Name of Virtual Machine**.

6 Specify a name for the virtual machine in the **Name** field, then click **Apply**.

For example, you might specify *hostname*_vm, where hostname is the DNS name of the server you are installing in the VM.

7 Click **Hardware**.

7a Specify the amount of initial and maximum memory for the virtual machine to consume from the available memory. The initial memory should not be less than 2048 MB.

7b Specify the number of processors that you want the virtual machine to use.

7c Click **Apply**.

8 If you want to change the graphics adapter settings, click **Peripheral Devices** and select the type of graphic support desired, then click **Apply**.

9 Click **Disks**.

The Virtual Disks dialog box lets you create one or more virtual disks that the OES VM guest has access to. If you are installing from a DVD on the host server or from an ISO image file copied to the host server's storage devices, these are also listed as virtual disks.

Initially, a 10 GB file is specified for the partitions/volumes on the virtual server. The default location of the file is `/var/lib/libvirt/images`.

By default, this is a sparse file, meaning that although 10 GB is allocated, the size of the file on the disk is only as large as the actual data it contains. Sparse files conserve disk space, but they have a negative impact on performance.

The OES installation guidelines recommend 10 GB for a server installation. Keep in mind, however, that you are defining the total local disk size for the server. You should allocate as much local space as you anticipate the server needing for data and other files after it is hosting user services.

9a Specify the hard disk space you want to be available to the virtual machine.

9b Click **OK**.

9c To create additional virtual disks, click the Harddisk icon in the Disks wizard.

10 If you are installing OES from a downloaded ISO image file, click DVD, browse to the OES image file, then click **Open > OK > Apply**.

11 If you want to change the network adapter settings, click **Network Adapters**, view the default setting, then edit the default settings.

or

Click **New** and specify the setting for another network board of your choice, then click **Apply**.

12 Click **Operating System Installation**:

12a If you are installing from a downloaded ISO image, ensure that the OES image is specified as the **Virtual Disk** installation source.

12b If you are installing from a network installation source, specify the URL for the OES network installation source.

You specify a network installation source for OES during the install.

12c If you are using an AutoYaST control file to specify the settings for a virtual machine operating system, specify the path to the file in the **AutoYaST File** field or click the **Find** button to the right of the field to locate the file on the local host server.

12d If necessary, use the **Additional Arguments** field to specify additional install or boot parameters to assist the installation.

For example, if you wanted to specify the parameters for an IP address of 192.35.1.10, a netmask of 255.255.255.0, a gateway of 192.35.1.254 for the virtual server, and use ssh to access the installation from another workstation, you could enter the following parameters in the **Additional Argument** field:

```
hostip=192.35.1.10 netmask=255.255.255.0 gateway=192.35.1.254
nameserver=192.35.100.100 domain=example.com usessh=1
sshpassword=password
```

or

```
ifcfg=eth0=192.35.1.10/24,192.35.1.254,192.35.100.100,example.com
ssh=1 sshpassword=password
```

12e Click **Apply**.

13 Click **OK** to start the virtual machine and launch the operating system installation program.

14 Read and accept the license agreement, then continue with Section 3.4, “Specifying Network Settings,” on page 42.

10.5 Setting Up an OES VM Guest to Use Novell Storage Services (NSS)

When you install OES 24.4 on a virtual machine, we recommend that you configure a virtual machine with multiple devices. Use the primary virtual disk as the system device with LVM (the YaST install default) as the volume manager. After the install, you can assign additional storage resources from the host server to the virtual machine.

IMPORTANT: When you create the virtual machine, make sure to configure the size of the primary virtual disk according to the amount of space you need for the `/boot`, `swap`, and root (`/`) volumes.

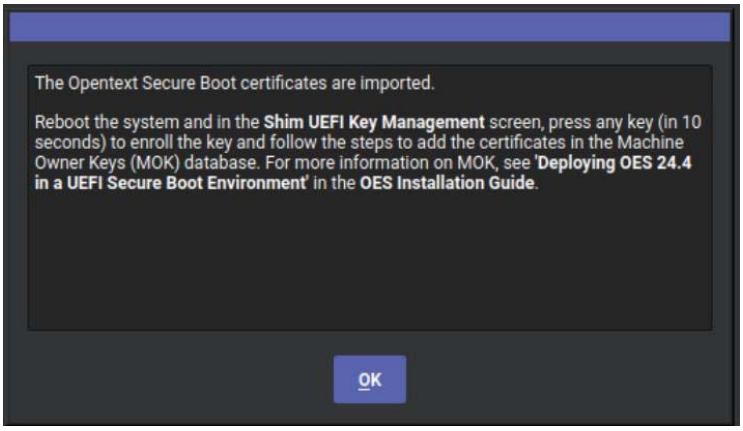
After the virtual machine is set up, you need to perform additional tasks to set up additional Novell Storage Service (NSS) devices. See "Using NSS in a Virtualization Environment" in the *Storage Services File System (NSS) Administration Guide for Linux*.

11 Deploying OES in a UEFI Secure Boot Environment

The signature of the kernel modules is used when OES is running in a UEFI Secure Boot environment. To ensure the integrity of the running kernel, the kernel will only load modules signed with trusted keys. The key is considered trusted once the corresponding Secure Boot certificate is loaded into a UEFI key database.

The OES installation imports the Micro Focus Secure Boot certificate under `/etc/uefi/certs` and prepares it to be enrolled into the Machine Owner Keys (MOK) database of the firmware. You need to complete the enrolling of the certificate by following Step 4 in the UEFI prompt.

If the key is not enrolled when the UEFI prompts during the OES installation stage, the following pop-up is displayed during the OES configuration:



Click **OK** to continue with the configuration.

Whether using YaST or AutoYaST, reboot the server after the configuration is completed. Then, enroll the key in the Shim UEFI Key Management screen by following Step 4 to Step 10.

If for any reason the key is not enrolled properly during the OES installation process, you must manually import the certificate and enroll it in the MOK database.

NOTE: During the OES installation, ensure to select **Yes** for **Enable Secure Boot** in the Installation Settings > Booting tab before the packages are installed.

The steps to manually import and then enroll the certificates in the MOK database is as follows:

1 Import the Micro Focus Secure Boot Certificates to the MOK database using the following command:

```
~# mokutil --root-pw --import /etc/uefi/certs/55E46AAF.crt
```

The --root-pw option enables usage of the root user directly.

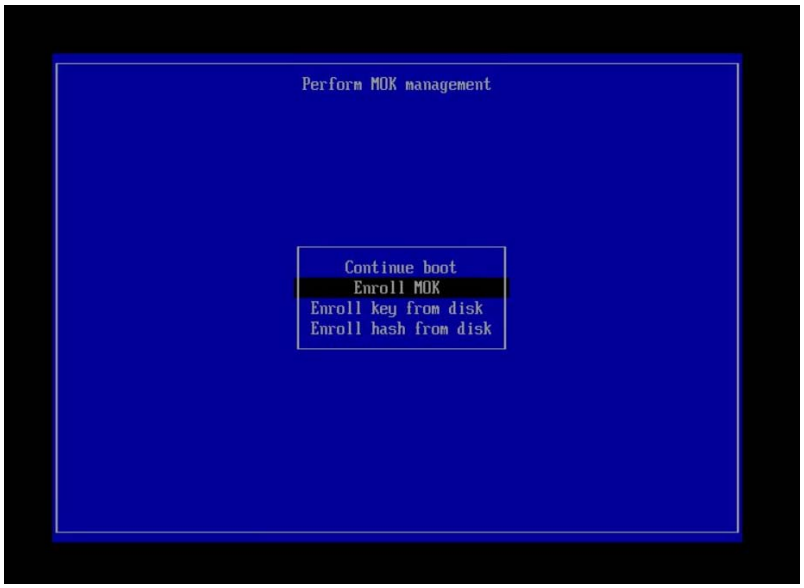
2 Ensure that the imported certificate is listed among the certificates that are prepared to be enrolled using the following command:

```
~# mokutil --list-new
```

3 Reboot the system. Shim launches the MokManager.

4 In the Shim UEFI Key Management screen, press any key (in 10 secs) to enroll certificates in the MOK database.

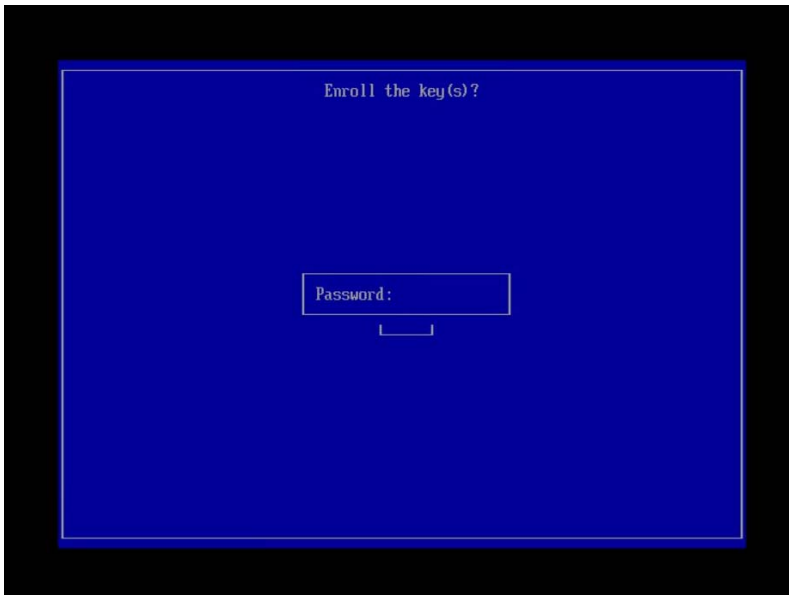
5 In the Perform MOK Management screen, click **Enroll MOK**.



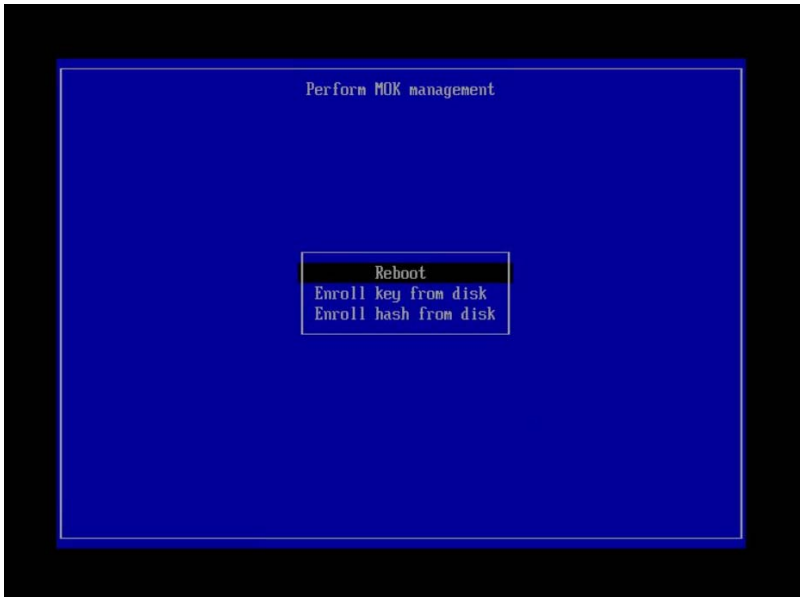
6 In the Enroll MOK screen, click **Continue**.

7 In the Enroll the Key(s) screen, click **Yes**.

8 In the Enroll the Key(s) screen, specify the root password.



9 In the Perform MOK management screen, click **Reboot** to complete the enrollment process.



10 Verify the enrolled key in the kernel messages after the reboot. The `Micro Focus Open Enterprise Secure Boot Signkey` is in the list of loaded certs.

or

Verify the enrolled key using the following command:

```
~# mokutil --list-enrolled
```

12 Switching to SHA-2 SSL Certificates

Major browser vendors are taking steps to phase out SHA-1 signed certificates. OES certificates signed with SHA-1 should be replaced with certificate signed with SHA-2 to avoid warning messages to be displayed in browsers.

- Section 12.1, “Configuring SHA-2 Certificate,” on page 173
- Section 12.2, “Verifying the Certificates with SHA-2 Signature,” on page 174

12.1 Configuring SHA-2 Certificate

- Section 12.1.1, “Prerequisites,” on page 173
- Section 12.1.2, “CA Server,” on page 173
- Section 12.1.3, “Other Servers,” on page 174
- Section 12.1.4, “Servers Running on eDirectory 8.8.7 or OES 11 SP1 or Earlier,” on page 174

12.1.1 Prerequisites

- eDirectory

12.1.2 CA Server

1. Apply patch on the OES server where CA is hosted in the tree.
2. Restart the eDirectory service.

   ```
   rcndsd restart
   ```
3. Delete the existing CA in tree and create a new CA with SHA-2 signing algorithm. For more information, see the TID on Configuring eDirectory to mint certificates with a SHA-2 signature (7016877).
4. Restart the eDirectory service.

   Run the following command to recreate the eDirectory server certificates with SHA-2 algorithm.

   ```
   rcndsd restart
   ```
5. Reboot the server.

   IMPORTANT: Ensure that eDirectory service is restarted before rebooting the server.

   All the OES services will now use the new eDirectory certificates.

12.1.3 Other Servers

1. Apply patch on the OES server.
2. Restart the eDirectory service.

   Run the following command to recreate the eDirectory server certificates with SHA-2 algorithm.

   ```
   rcndsd restart
   ```
3. Reboot the server.

   IMPORTANT: Ensure that eDirectory service is restarted before rebooting the server.

   All the OES services will now use the new eDirectory certificates.

12.1.4 Servers Running on eDirectory 8.8.7 or OES 11 SP1 or Earlier

If there are OES servers (OES 11 SP1 or older versions) in the tree, it is recommended to delete the server certificates of that server and create a new certificate with SHA-2 signing algorithm same as CA. The CA will be hosted on either OES 11 SP3 or later servers in the tree.

12.2 Verifying the Certificates with SHA-2 Signature

- On the OES server, run the following command against the LDAP server (for example, 192.168.211.21) to verify that the certificate is using the SHA-2 signature.

  ```
  openssl s_client -connect 192.168.211.21:636 < /dev/null 2>/dev/null |
  openssl x509 -text -in /dev/stdin | grep "Signature Algorithm"
  ```

  If the return value is: `Signature Algorithm: sha256WithRSAEncryption`, then it is a RSA signature being protected by a SHA256 (SHA-2) accompanying hash function.
- Run the following command to verify the certificate file on the file system.

  ```
  "openssl x509 -in /etc/opt/novell/certs/SSCert.der -inform der -text -
  noout"
  ```

13 Disabling OES Services

Although you can uninstall Open Enterprise Server (OES) service RPMs through YaST, we do not recommend it because so many modules have interdependencies. Uninstalling services can leave the server in an undesirable state. Instead, we recommend disabling the service.

1. Log in as `root`.
2. Disable the service using the command `systemctl disable <service_name>.service`.

NOTE: YaST does not support removing products that create objects or attributes in eDirectory. You need to use iManager to remove these objects and attributes. For procedures, see Deleting an Object in the NetIQ iManager Administration Guide.

---

14 Reconfiguring eDirectory and OES Services

If the eDirectory database becomes corrupt, you need to reconfigure eDirectory and the OES services. This section outlines the steps to be performed, depending on the role of the server with regard to your eDirectory tree.

If a backup of the eDirectory database is not available, you can contact Micro Focus Support or perform the following procedures:

- Section 14.1, “Cleaning Up the eDirectory Server,” on page 177
- Section 14.2, “Reconfiguring the eDirectory Server through YaST,” on page 179
- Section 14.3, “Reconfiguring OES Services,” on page 179

14.1 Cleaning Up the eDirectory Server

IMPORTANT: The instructions in this section have been tested and approved, but it is impossible to anticipate all customer scenarios and the complications that might arise in them.Therefore, we urge that you only proceed when you have problems with eDirectory that aren't resolved by performing regular eDirectory maintenance tasks, or when Micro Focus Technical Support recommends that you do.

- Section 14.1.1, “Before You Clean Up,” on page 177
- Section 14.1.2, “Reconfiguring the Replica Server,” on page 178
- Section 14.1.3, “Reconfiguring the CA Server,” on page 178
- Section 14.1.4, “Cleaning Up eDirectory,” on page 178

14.1.1 Before You Clean Up

- Before the cleanup, make a note of the following eDirectory configuration parameters:
  - eDirectory tree name
  - Replica server IP
  - eDirectory admin context
  - eDirectory server context
  - IP address of servers running NTP and SLP services
- If you are cleaning the master replica server, ensure that you make a read-write replica as a master. For more information, see Section 14.1.2, “Reconfiguring the Replica Server,” on page 178.
- If the reconfiguration is performed on a CA server, transfer the role of CA server to another server or create a new CA server. If you don’t do this, the CA does not work. For more information, see Section 14.1.3, “Reconfiguring the CA Server,” on page 178.

14.1.2 Reconfiguring the Replica Server

1. If the corrupted server is a master replica, make any other replica into the master replica.

   For more information, refer to Managing Partitions and Replicas in the NetIQ eDirectory Administration Guide.

2. Clean up the replica server.

   For more information, see Section 14.1.4, “Cleaning Up eDirectory,” on page 178.

3. Reconfigure the replica server.

   For more information, see Section 14.2, “Reconfiguring the eDirectory Server through YaST,” on page 179.

4. On successful reconfiguration of the replica server, continue with Section 14.3, “Reconfiguring OES Services,” on page 179.

14.1.3 Reconfiguring the CA Server

1. If the corrupted server is a CA server, transfer the CA server role to another server or create a new CA server.

   For more information, refer to Moving the Organizational CA to a Different Server (https://www.netiq.com/documentation/crt33/crtadmin/data/a2ebop8.html#acea8nu) and Creating a Server Certificate Object in the *Novell Certificate Server 3.3.2 Administration Guide*.

2. Clean up the server.

   For more information, see Section 14.1.4, “Cleaning Up eDirectory,” on page 178.

3. Reconfigure the server.

   For more information, see Section 14.2, “Reconfiguring the eDirectory Server through YaST,” on page 179.

4. After successfully reconfiguring the server, continue with Section 14.3, “Reconfiguring OES Services,” on page 179.

14.1.4 Cleaning Up eDirectory

1. Use iManager to delete all the objects from the eDirectory tree.
2. Stop the ndsd daemon:

   ```
   rcndsd stop
   ```

   or

   ```
   systemctl stop ndsd.service
   ```

3. Delete the eDirectory configuration file and eDirectory instance file.:

   ```
   rm -f /etc/opt/novell/eDirectory/conf/nds.conf
   rm -f /etc/opt/novell/eDirectory/conf/.edir/instances.0
   ```

4. Delete the eDirectory database:

   ```
   rm -rf /var/opt/novell/eDirectory/data/dib
   ```

5 Remove the server from the replica ring.

For more information, see Cleaning Up the Replica Ring in the NetIQ eDirectory Administration Guide.

14.2 Reconfiguring the eDirectory Server through YaST

The eDirectory reconfiguration can be done on the Root partition Master replica server, a Read-Write replica server, a server without a replica, or the CA server.

1 Open YaST.

2 Click **Open Enterprise Server > OES Install and Configuration.**

3 On the Software Selection Page, click **Accept**.

The status of eDirectory service is displayed as **Reconfigure is disabled.**

4 To reconfigure, click **disabled** to change the status to **enabled.**

5 Click **eDirectory** to access the configuration dialog box.

6 Provide all the eDirectory configuration information that was noted in Section 14.1.1, “Before You Clean Up,” on page 177:

6a Verify the eDirectory tree name and click **Next.**

6b Specify the admin password and click **Next**.

6c Specify the server context and click **Next**.

6d Specify the IP address of the Network Time Protocol Server.

6e (Conditional) If SLP was configured earlier, select **Configure SLP to use an existing Directory Agent**, then click **Add.**

6f Specify the SLP DA server IP address and click **Add.**

6g Click **Next**.

7 In the NetIQ Modular Authentication Service (NMAS) window, click **Next**.

8 Verify the listed configuration information and click **Next**.

eDirectory is configured and installation is successfully completed.

9 Click **Finish**.

14.3 Reconfiguring OES Services

After you have successfully configured eDirectory, some of the OES services are started by default, some services require a manual start, some services require the eDirectory objects to be re-created, and some services must be reconfigured.

Table 14-1 Services

Starts by Default	Start Manually	Re-create Objects	Reconfigure
SMS	NCS	NSS	DNS
LUM	DHCP	NCP	CIFS
NRM	iPrint		SLP
FTP	iManager		NMAS
Groupwise	NTP		
DST			
DFS			
WBFM			
Welcome Page			
VLOG Utility			

- Section 14.3.1, “Re-creating eDirectory Objects,” on page 180
- Section 14.3.2, “Services Requiring Reconfiguration,” on page 181
- Section 14.3.3, “Manually Starting Services,” on page 182

14.3.1 Re-creating eDirectory Objects

- “Novell Storage Service” on page 180
- “NCP Server” on page 181

Novell Storage Service

Use the NSS Management utility to re-create the eDirectory objects for NSS pools and volumes. For additional information, see NSS Management Utility (NSSMU) Quick Reference in the Storage Services File System (NSS) Administration Guide for Linux.

1 Re-create the eDirectory object for each NSS pool:

1a Start NSSMU by entering the following command at the command prompt:

```
nssmu
```

1b Select **Pools** and press Enter to list all the NSS pools.

1c Select a pool that needs to be re-created and press F4.

1d Select **Yes** when you are prompted to delete and re-create an NDS pool object.

The selected NDS pool object is re-created.

1e Repeat from Step 1c for each NDS pool object that needs to be re-created.

2 Re-create the eDirectory object for each NSS volume:

2a In NSSMU, select **Volumes** and press Enter to list all the NSS volumes.

2b Select a volume and press F4.

2c Select **Yes** when you are prompted to delete and re-create the NDS volume object.

The selected volume object is re-created.

2d Repeat from Step 2b for each NDS volume object that needs to be re-created.

3 (Conditional) If the eDirectory object for _ADMIN volume exists, execute the following command:

```
rcadminfs restart
```

NCP Server

Use the NCP server console (NCPCON) utility to delete and re-create the eDirectory objects for the NCP volumes. For more information on the NCPCON utility, see NCP Server Console (NCPCON) Utility in the NCP Server for Linux Administration Guide.

IMPORTANT: If restoration of the eDirectory database is not possible, simply delete the NCP server object.

---

1 Delete the eDirectory object of the NCP volume by entering the following command:

```
ncpcon remove volume SYS
```

2 Re-create the eDirectory object of the NCP volume by entering the following command:

```
ncpcon create volume SYS /usr/novell/sys
```

14.3.2 Services Requiring Reconfiguration

- "OES DNS" on page 181
- "OES CIFS" on page 182
- "SLP" on page 182
- "NMAS" on page 182

OES DNS

1 Open YaST.

2 Click **Open Enterprise Server > OES Install and Configuration.**

3 On the Software selection page, click **Accept.**

The status of the OES DNS service is displayed as **Reconfigure is Disabled.**

4 To reconfigure the DNS service, click **disabled** to change the status to **enabled.**

5 Click the **DNS Services** heading link and enter the admin password to access the configuration dialog box.

6 Validate the displayed information and click **Next.**

7 Ensure that the **Create DNS Server Object** check box is not selected, then click **Next.**

8 Verify the configuration information and click **Next**.

9 Click **Finish** to complete the OES DNS reconfiguration.

OES CIFS

1. Open YaST.
2. Click **Open Enterprise Server > OES Install and Configuration.**
3. Click **Accept** to skip the Software Selection page.

   The status of OES CIFS service is displayed as **Reconfigure is Disabled.**
4. To reconfigure CIFS, click the **Disabled** link to change the status to **Enabled.**
5. Click the **OES CIFS services** heading link and enter admin password to access the configuration dialog box.
6. Validate the displayed information and click **Next.**
7. Provide the user context and select the password policy of the previous CIFS configuration, then click **Next.**
8. Verify the configuration information and click **Next.**
9. Click **Finish** to complete the CIFS reconfiguration.

SLP

The SLP DA IP address is added during eDirectory reconfiguration. See Step 6e on page 179 for more information.

NMAS

The NMAS login method is selected during eDirectory reconfiguration. See Step 7 on page 179 for more information.

14.3.3 Manually Starting Services

Re-create the eDirectory objects of NCP and NSS volumes as directed in the Section 14.3.1, “Re-creating eDirectory Objects,” on page 180, before starting the following services manually:

Table 14-2 *Manually Restarting Services*

Service Name	Starting the Service
OES Cluster Service (NCS)	`rcnovell-ncs start` or `systemctl start novell-ncs.service`
OES DHCP	`rcnovell-dhcpd start` or `systemctl start novell-dhcpd.service`
iPrint	`rcnovell-ipsmd start` or `systemctl start novell-ipsmd.service` `rcnovell-idsd start` or `systemctl start novell-idsd.service`

Service Name	Starting the Service

iManager	After completing the OES installation, if iManager is installed without using YaST, Tomcat must be started manually.
	`systemctl start novell-tomcat.service`
	`rcapache2 restart`

NTP	`rcntpd restart`

15 Centralized Certificate Management

Digital certificates are essential for securing network-wide and intranet communications in an OES environment. The certificate can be signed and issued by an eDirectory Certificate Authority (CA), your organizational CA or a third-party CA.

Until OES 2023, some services that provide secure communication have their default settings configured to use a self-signed server certificate created by YaST. Instead of using self-signed certificates, we recommend, you use an eDirectory server certificate or a CA-signed certificate because they provide more security and trust than the former. For more information on eDirectory Certificate Server, see Understanding the Certificate Server in the NetIQ eDirectory Administration Server

The following issues arise because many OES services need certificates:

- Self-signed certificates offer a minimal level of security and trust.
- Certificate expiration:
  - Services are stopped.
  - The OES services are not trusted by the clients.
- When a certificate is about to expire, the administrator is not notified. As a result, certificate expiration is challenging to avoid.
- No details of services using the certificates, their path and format.
- Insufficient documentation.

We have implemented the following to address all certificate-related issues:

- By default, all services on OES are configured to use eDirectory server certificates.
- New component help in certificate management on OES.

Centralized certificate management helps administrators in managing the certificate lifecycle. The features are:

- Mail notifications notify the administrator and the root user of the certificates' impending expiration.
- Indicates where each service's certificates can be found.
- Indicates the certificate's type, such as whether it is self-signed or CA-signed.
- Indicates whether the certificates are still valid.
- Reconfigures the OES services to use a new certificate when certificates are invalid, corrupted or expired.
- A browser-based tool (Unified Management Console, or UMC) that enables remote management of certificates across servers will be available in the upcoming releases.

This section describes the procedures to install and use centralized certificate management on the OES server.

- Section 15.1, “Installing Centralized Certificate Management Binaries,” on page 186
- Section 15.2, “Upgrading OES Server,” on page 186
- Section 15.3, “Path to Important Certificate Management Files,” on page 187
- Section 15.4, “Usage of Commands,” on page 187
- Section 15.5, “Examples,” on page 191

15.1 Installing Centralized Certificate Management Binaries

The new rpm `oes-cert-mgmt.rpm` is installed on the server by default with the OES 23.4 release.

At `/opt/novell/oes-cert-mgmt/bin`, you will find all the executables that you need to list the certificates, replace certificates and configure services to use new certificates.

Certificate of some of the services is grouped under one service. If certificate is changed for that service, then all services grouped under it will also have the updated certificate.

Table 15-1 *Service groups for certificate*

Certificate	Services
Apache	NURM, iManager, and UMC
eDirectory	NCP

To receive alerts before expiry of certificates, modify the `/etc/opt/novell/oes-cert-mgmt/oes-cert-mgmt.conf` file.

Detailed information is provided in the “Usage of Commands” on page 187.

15.2 Upgrading OES Server

On upgrading OES 23.4 or later server, `oes-cert-mgmt.rpm` is installed with the base rpms.

After upgrading to OES 23.4 or later, it is recommended to move services using self-signed certificates to eDirectory server certificate or any other CA singed certificate.

If services continue using self-signed certificate, you will not be able to take the full advantage of the tool. As the tool does not support self-signed certificates, on expiry, you will not be able to reconfigure the services to use a new self-signed certificate.

15.3 Path to Important Certificate Management Files

Table 15-2 *Certificate Management Files*

Name	Location
Binaries	`/opt/novell/oes-cert-mgmt/bin/`
Alert and Log level configuration file	`/etc/opt/novell/oes-cert-mgmt/oes-cert-mgmt.conf`
Log file	`/var/opt/novell/log/oes-cert-mgmt/oes-cert-mgmt.log`
Service certificate (`.json files`)	`/var/opt/novell/oes-cert-mgmt\`

15.4 Usage of Commands

- Section 15.4.1, “Listing of Certificates Used by OES Services,” on page 187
- Section 15.4.2, “Configuration file,” on page 189
- Section 15.4.3, “Reconfiguring Certificates,” on page 190

15.4.1 Listing of Certificates Used by OES Services

View certificate details of all the services configured on the OES server where the certificate script is executed.

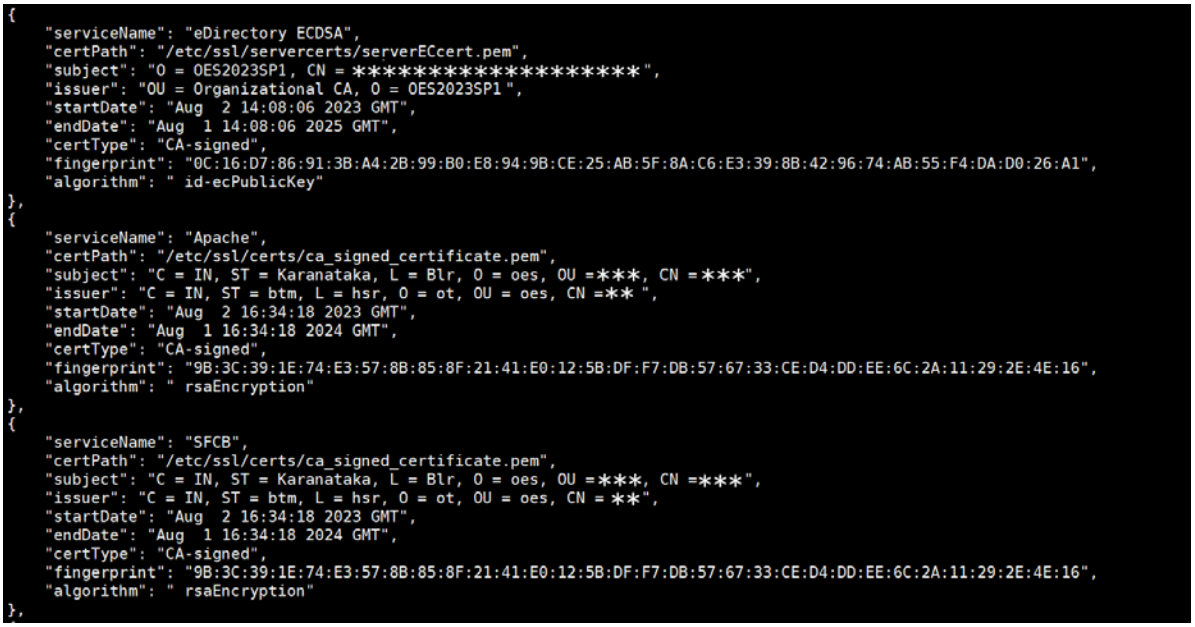
The output of the `--list` command is recorded in the `json` files – Based on services (`certlist-service.json`) and certificates (`certlist-cert.json`). These files capture all the certificate attributes such as certificate path on the OES server, and details of the certificate like subject, issuer, expiry date and whether the certificate is self-signed or CA Signed. For every certificate, details of the services are also listed. The file captures same data in different format in both the files.

Before replacing the `json` files with the output of `--list` command, it is backed up and available at the `/var/opt/novell/oes-cert-mgmt/` location.

Service-specific Format

On OES terminal, execute `/opt/novell/oes-cert-mgmt/bin/oes-cert-mgmt-list --list service`. The output of this command is written to the `/var/opt/novell/oes-cert-mgmt/certlist-service.json` file.

Figure 15-1 *Certilist-service.json file*



Certificate-specific Format

On OES terminal, execute `/opt/novell/oes-cert-mgmt/bin/oes-cert-mgmt-list --list certificate`. The output of this command is written to the `/var/opt/novell/oes-cert-mgmt/certlist-cert.json` file.

Figure 15-2 *Certilist-cert.json file*

15.4.2 Configuration file

- “Configuring Alerts For Certificate Expiry” on page 189
- “Configuring Error Logging” on page 189

Figure 15-3 *oes-cert-mgmt.conf file*

```
[settings]
#Enable and Disable Alerting, Default No
mail-alert=No
#From and To addresses for Mail alerts. Mandatory if mail-alert is set to Yes
mail-alert-to-address=
mail-alert-from-address=

#Valid log levels - ERROR, INFO and DEBUG. Default value DEBUG
log-level=DEBUG
```

Configuring Alerts For Certificate Expiry

The administrator receives an alert about the expiry of the certificates every Friday through an email 90 days in advance. The system date is considered for identifying expiry status of the certificates. Details of expired certificates or certificates getting expired within 90 days are available in json format.

To receive an alert, do the following:

1. On the OES terminal, modify the `/etc/opt/novell/oes-cert-mgmt/oes-cert-mgmt.conf` file.

   1a. Modify the following attributes:

   ```
   mail-alert=Yes
   mail-alert-to-address=claire@gmail.com,albert@gmail.com
   mail-alert-from-address=claire@gmail.com
   ```

   It is recommended to mention your email address in the “`mail-alert-from-address`” attribute too, else specifying server name might be treated as spam by the mailbox.

   Multiple email addresses can be specified in the `mail-alert-to-address` attribute.

2. An email is sent to the address specified in the "`mail-alert-to-address`" attribute and, by default, to the system’s root user. The email is sent only when one or more certificates are expiring within 90 days. The details are specified in the `certificate.json` file.

   Email Frequency: An alert email is sent every Friday at midnight to the root user and the specified email address.

Configuring Error Logging

To configure the error logging setting for the certificate messages, use the `log-level` parameter in the `/etc/opt/novell/oes-cert-mgmt/oes-cert-mgmt.conf` configuration file.

The severity levels available are ERROR, INFORMATION and DEBUG.

To set the severity level, set the following:

`log-level=severity_level (DEBUG,INFO OR ERROR)`

For example,

`log-level=DEBUG`

15.4.3 Reconfiguring Certificates

An admin can reconfigure OES services to use new certificates using the command `/opt/novell/oes-cert-mgmt/bin/oes-cert-mgmt-reconfig`. The existing certificates are backed up with `.cert-mgmt.bak` extension before replacement.

Listed below are the options supported for reconfiguration:

- **certchange:** Replace an existing certificate with a new one and reconfigure all the services to use the new certificate.
- **reconfig:** Reconfigures selected services to use a new certificate.
- **edircertchange:** When the eDirectory server certificate is changed, all the services are configured to use the new certificate.
- **movetoedircert:** Used for reconfiguring services that use self-signed or third-party CA-signed certificates to use the eDirectory server certificate.

Figure 15-4 *Certificate Management Command Line Help*

```
*** *** *** *** :/opt/novell/oes-cert-mgmt/bin # ./oes-cert-mgmt-reconfig -h
usage: oes-cert-mgmt-reconfig [-h] --operation OPERATION
                              [--currentcert CURRENTCERT]
                              [--currentcertkey CURRENTCERTKEY]
                              [--newcert NEWCERT]
                              [--newprivatekey NEWPRIVATEKEY]
                              [--newcacert NEWCACERT]
                              [--listofservices LISTOFSERVICES]
                              [--restart RESTART]

optional arguments:
  -h, --help            show this help message and exit
  --operation OPERATION
                        Reconfiguration operation - certchange, reconfig,
                        edircertchange, movetoedircert
  --currentcert CURRENTCERT
                        Path of the certificate being replaced
  --currentcertkey CURRENTCERTKEY
                        Path of the private key of certificate being replaced
  --newcert NEWCERT     Path of the new server certificate
  --newprivatekey NEWPRIVATEKEY
                        Path of new certificate private key
  --newcacert NEWCACERT
                        Path of CA Certificate of new certificate
  --listofservices LISTOFSERVICES
                        Comma separated list of services to be reconfigured.
                        Supported services are - Apache, SFCB, FTP, iPrint,
                        NRM and Postgres
  --restart RESTART     Restart(yes/no) services after reconfiguration
```

15.5 Examples

The path and certificate names specified are for example purpose and might not be the actual names or path of the certificates.

For creation of new certificates, refer to individual service-specific guides at OES 24.4 website (https://www.microfocus.com/documentation/open-enterprise-server/23.4/).

- Section 15.5.1, “Example - Replacing Expired or Corrupted Certificate,” on page 191
- Section 15.5.2, “Example - Replacing Expired or Corrupted Certificate of CIS Server,” on page 192
- Section 15.5.3, “Example - Reconfiguring Services to Use 3rd party CA Signed Certificate,” on page 193
- Section 15.5.4, “Example - Replacing Expired or Corrupted eDirectory Server Certificate,” on page 193
- Section 15.5.5, “Example - Moving from Self-Signed Certificates to eDirectory Server Certificate On Upgrade,” on page 194

15.5.1 Example - Replacing Expired or Corrupted Certificate

A CA-signed certificate has expired or become corrupted and requires replacement with a new certificate.

The expired certificate is located in `/etc/ssl/servercerts/`, which contains both the .pem files for the server certificate and the private key. The root user copies the new certificate to a temporary location, `/etc/opt/novell/oescerts`, which includes both the `.pem` files for the new server certificate and its private key. The CA certificate is located in `/etc/ssl/certs/` and includes the `.pem` file.

To reconfigure all the services with a new certificate and then restart the services, do the following:

1 On the OES terminal, execute the command `/opt/novell/oes-cert-mgmt/bin/oes-cert-mgmt-reconfig --operation certchange --currentcert /etc/ssl/servercerts/oescert.pem --currentcertkey /etc/ssl/servercerts/oescertserverkey.pem --newcert /etc/opt/novell/oescerts/oesnewservercert.pem --newprivatekey /etc/opt/novell/oescerts/oesnewcertkey.pem --newcacert /etc/ssl/certs/CACert.pem --restart yes`

When you execute this command, all the OES services on this server are automatically restarted and start using the new certificate.

By default, the option `--restart no` is set. A service restart is required to apply the new certificate.

For details, refer to the `/var/opt/novell/log/oes-cert-mgmt/oes-cert-mgmt.log` file.

The `/etc/ssl/servercerts/oescert.pem` and `/etc/ssl/servercerts/oescertkey.pem` content is replaced with `oesnewservercert.pem` and `oesnewcertkey.pem`. The certificates that are getting replaced are backed up in the same location with `.cert-mgmt.bak` extension.

15.5.2 Example - Replacing Expired or Corrupted Certificate of CIS Server

- "eDirectory Certificate" on page 192
- "Cluster Resource Certificate" on page 192

An eDirectory certificate or Cluster Resource certificate has expired or become corrupted and requires replacement with a new certificate on a CIS server.

eDirectory Certificate

The eDirectory certificate is expired or corrupted. To reconfigure CIS service with a new eDirectory server certificate, do the following:

1. Delete existing eDirectory server certificate files from `/etc/ssl/servercerts` location.
2. Regenerate a new eDirectory server certificate and copy it to the `/etc/ssl/servercerts` location.
3. Restart the eDirectory service so the new certificate is applied.
4. On the OES terminal, execute the command `/opt/novell/oes-cert-mgmt/bin/oes-cert-mgmt-reconfig --operation edircertchange –-restart yes`

   When you execute this command, the CIS service and any other services on this server are automatically restarted to use the new eDirectory server certificates from `/etc/ssl/servercerts` location.

   By default, the option `--restart no` is set. CIS service restart is required to apply the new certificate.

   For details, refer to the `/var/opt/novell/log/oes-cert-mgmt/oes-cert-mgmt.log` file.

Cluster Resource Certificate

The certificate is located in `/etc/opt/novell/cis/certs/`, which contains the .pem files for the server. Copy the regenerated certificate to a temporary location, `/etc/opt/novell/cis/temporary`, which includes both the `.pem` files for the new server certificate and its private key. The root certificate is located in `/etc/opt/novell/certs/` and includes the SSCert`.pem` file.

To reconfigure CIS Cluster Resource certificate with a new certificate, do the following:

1. Regenerate a new server certificate and copy to the `/etc/opt/novell/cis/temporary/` location. For more information, see Creating Certificates in the Cloud Integrated Storage Administration Guide.
2. On the OES terminal, execute the command `/opt/novell/oes-cert-mgmt/bin/oes-cert-mgmt-reconfig --operation certchange --currentcert /etc/opt/novell/cis/certs/servercert.pem --currentcertkey /etc/opt/novell/cis/certs/serverkey.pem --newcert /etc/opt/novell/cis/temporary/servercert.pem --newprivatekey /etc/opt/novell/cis/temporary/serverkey.pem --newcacert /etc/opt/novell/certs/SSCert.pem --restart yes`

When you execute this command, the CIS service on this server is automatically restarted to begin using the new certificate.

By default, the option `--restart no` is set. CIS service restart is required to apply the new certificate.

For details, refer to the `/var/opt/novell/log/oes-cert-mgmt/oes-cert-mgmt.log` file.

The existing certificates are backed up with `.cert-mgmt.bak` extension before getting replaced with a new certificate.

15.5.3 Example - Reconfiguring Services to Use 3rd party CA Signed Certificate

The OES services are using eDirectory certificate. The organization policy has changed and a few of the services (SFCB and Apache) need to consume the new certificates provided by the third-party CA.

The supported list of services that can be reconfigured to use the new certificate are available with the command line parameter `--listofservices`.

The location of the new certificate is `/etc/opt/novell/certs` that includes both the `.pem` files for server and key. The location of the CA certificate `/etc/ssl/certs/` that includes the `.pem` file.

To forcibly make the existing services to use a new certificate, do the following:

1. On the OES terminal, execute the command `/opt/novell/oes-cert-mgmt/bin/oes-cert-mgmt-reconfig --operation reconfig --newcert /etc/opt/novell/certs/oesservercert.pem --newprivatekey /etc/opt/novell/certs/oesserverkey.pem --newcacert /etc/ssl/certs/CompanyCACert.pem --listofservices sfcb,apache --restart yes`

   When you execute this command, SFCB and Apache services are automatically restarted to begin using the new certificate signed by the third-party CA.

   By default, the option `--restart no` is set. A service restart is required to apply the new certificate.

   For details, refer to the `/var/opt/novell/log/oes-cert-mgmt/oes-cert-mgmt.log` file.

15.5.4 Example - Replacing Expired or Corrupted eDirectory Server Certificate

The service is using default eDirectory certificate and it is expired or corrupted. To reconfigure all the services using eDirectory certificate with a new eDirectory server certificate, do the following:

1. Delete existing eDirectory server certificate files from `/etc/ssl/servercerts` location.
2. Admin regenerates a new eDirectory server certificate and copies it to the `/etc/ssl/servercerts` location.
3. Restart the eDirectory service so the new certificate is applied.
4. On the OES terminal, execute the command `/opt/novell/oes-cert-mgmt/bin/ oes-cert-mgmt-reconfig --operation edircertchange –-restart yes`

When you execute this command, all the OES services on this server are automatically restarted to begin using the new eDirectory server certificates from `/etc/ssl/servercerts` location.

By default, the option `--restart no` is set. A service restart is required to apply the new certificate.

For details, refer to the `/var/opt/novell/log/oes-cert-mgmt/oes-cert-mgmt.log` file.

15.5.5 Example - Moving from Self-Signed Certificates to eDirectory Server Certificate On Upgrade

On upgrading services from OES 2023 to OES 23.4 or later server, it is recommended for services to use eDirectory server certificate or any CA signed certificate instead of self-signed certificate.

On OES 2023 server, SFCB and Postgres services are using self-signed certificate. Perform the following steps, so the services can use eDirectory server certificate.

1. Upgrade OES 2023 server to OES 23.4 or later server.
2. Verify the services that use self-signed certificate.
   - **2a** On the OES terminal, execute the `/opt/novell/oes-cert-mgmt/bin/oes-cert-mgmt-list --list certificate`

     In the `/var/opt/novell/oes-cert-mgmt/certlist-cert.json` file, the `"certType":"self-signed"` for SFCB and Postgres.
3. Modify the certificates to use eDirectory server certificate.
   - **3a** On the OES terminal, execute the command `/opt/novell/oes-cert-mgmt/bin/oes-cert-mgmt-reconfig --operation movetoedircert --listofservices sfcb,Postgres --restart yes`

     Success message is displayed for restarting the SFCB and Postgres services. Also, a message stating that selected services are moved to eDirectory server certificate is displayed.

     By default, the option `--restart no` is set. A service restart is required to apply the new certificate.
4. Verify SFCB and Postgres are using eDirectory server certificate.
   - **4a** On the OES terminal, execute the `/opt/novell/oes-cert-mgmt/bin/oes-cert-mgmt-list --list certificate`

     In the `/var/opt/novell/oes-cert-mgmt/certlist-cert.json` file, the `"certType":"CA-signed"` for SFCB and Postgres.

16 OES Multifactor Authentication Service

This guide describes the OES Multifactor Authentication (MFA) service, including its configuration and management in the OES environment. It also covers how OES services can implement MFA for their users.

- Section 16.1, “Overview,” on page 195
- Section 16.2, “MFA Server Architecture,” on page 196
- Section 16.3, “Preparing to Deploy an MFA Server,” on page 197
- Section 16.4, “Deployment Recommendation,” on page 198
- Section 16.5, “Setting-Up an MFA Server,” on page 198
- Section 16.6, “Setting-Up Subsequent MFA Servers,” on page 199
- Section 16.7, “Configuring MFA Agent,” on page 200
- Section 16.8, “Configuring OES Services to Use MFA Service,” on page 200
- Section 16.9, “Allowlist to Exempt from MFA,” on page 200
- Section 16.10, “Command Line Utility of MFA Server,” on page 200
- Section 16.11, “Command Line Utility of MFA Agent,” on page 204
- Section 16.12, “Important Files and Folders,” on page 206
- Section 16.13, “Security Configurations,” on page 206
- Section 16.14, “Troubleshooting,” on page 207

16.1 Overview

The OES MFA service provides multifactor authentication for OES services. OES services can enforce MFA during user logins, which leverages the NetIQ Advanced Authentication (AA) server. Instead of configuring each OES server for AA integration, the administrator can setup one or more MFA servers allowing the OES service to utilize the MFA with minimal configuration.

In this release, only the CIFS service utilizes MFA.

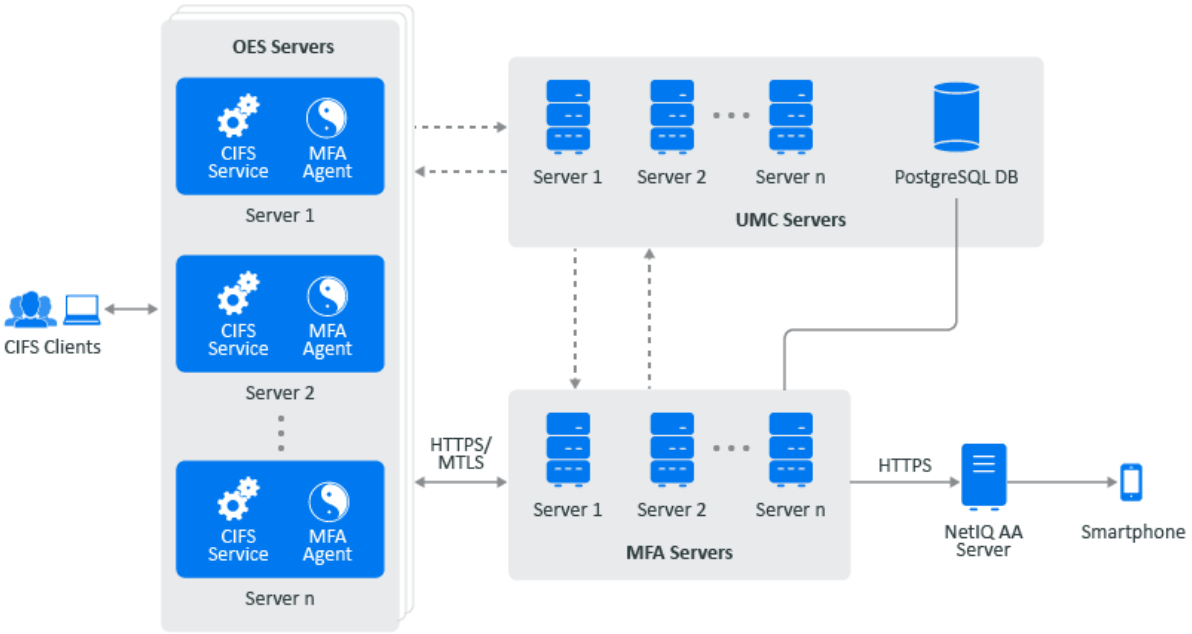
16.1.1 Quick Start - OES MFA Configuration

Follow these steps to configure the OES MFA service in an OES environment:

1. Preparing to Deploy an MFA Server
2. Setting-Up an MFA Server
3. Configuring OES Services to Use MFA Service

16.2 MFA Server Architecture

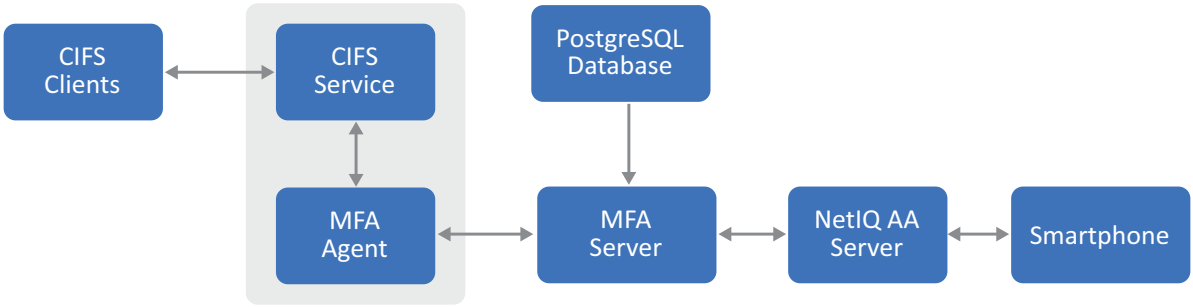
Figure 16-1



- **MFA servers:** One or more centralized servers configured in the eDirectory tree provides MFA service. While a single MFA server is sufficient for MFA functionality, additional servers can be configured for high availability. All MFA servers must reside within the same eDirectory tree.
- **MFA agent:** The MFA agent is installed and active on the OES servers that require the MFA service. MFA agents must reside within the same eDirectory tree as the MFA server. In this release, the MFA agent is operational on all CIFS servers.
- **Database:** The OES MFA server uses the UMC database, and no additional configuration is required.
- **UMC server:** The OES MFA service relies on UMC for database and service discovery. With service discovery, MFA agents discovers the available MFA servers and store address of the servers in the configuration file.
- **OES Services:** The OES services that utilize the OES MFA service for multifactor authentication are currently limited to the CIFS service in this release.
- **AA server:** OES MFA service uses NetIQ Advanced Authentication server in the back-end for multifactor authentication. Smart phone push is the only authentication method supported as of now.

16.2.1 MFA Control Flow Diagram

Figure 16-2 *MFA Control Flow Diagram*



The CIFS client initiates a request to map a network drive to the CIFS server. The CIFS server authenticates the user against Active Directory (AD) or eDirectory. After successful user authentication, the CIFS server sends a request to the MFA agent to perform multifactor authentication for the user.

The MFA agent forwards the authentication request to the MFA server, which in turn forwards it to the Advanced Authentication (AA) server. The AA server triggers the second factor authentication (smart phone push) and sends the result back to the MFA server, then to the MFA agent, and finally to the CIFS server. The CIFS server then sends a response back to the CIFS client, indicating whether the authentication was successful or failed.

Each successful MFA authentication session is stored in the database.

16.3 Preparing to Deploy an MFA Server

To deploy an MFA server, the OES environment must have the following:

- Unified Management Console (UMC) server (OES 24.4)

  Ensure that either all the instances of UMC servers use the same database or the databases used by different instances of UMC server are synchronized.

  Ensure that all instances of UMC server are updated to OES 24.4.

- NetIQ Advanced Authentication (AA) server (AA 6.3 and AA 6.4 versions)

  AA server should have a valid server certificate, and its CA certificate must be available in the MFA server and smartphone. The Smartphone Push method does not work, if CA certificate is not available in smartphone. If CA certificate is not available in the MFA server, it can be installed by copying it to the path `/usr/share/pki/trust/anchors`.

NOTE: eDirectory administrator credentials are required to configure the MFA server.

16.4 Deployment Recommendation

16.4.1 Number of MFA Servers

While one MFA server is sufficient to provide the functionality, more than one MFA servers provide high availability. MFA agent uses only one MFA server at any point of time. If one MFA server becomes unavailable, the MFA agent reconfigures itself to use next available MFA server.

Load balancing is not available in this release.

16.4.2 MFA Agents

MFA agents run as a service in every OES server where CIFS service is configured. To disable the MFA agent service, execute the following commands:

```
systemctl stop mfa-agent.service
```

```
systemctl disable mfa-agent.service
```

16.5 Setting-Up an MFA Server

OES MFA service uses the NetIQ Advanced Authentication (AA) server in the back-end. For more information, see NetIQ Advanced Authentication documentation.

Prerequisite Parameters Required from the AA Server

1. **Endpoint:** Endpoint ID and Endpoint Secret of the Endpoint created.
2. **Chain:** Create a chain in the AA server, which contains smart phone (with push notification) as the only method.
3. **Event:** Name of the Event created in the AA server, which contains the chain created in step 2.
4. **Repository:** (Optional) Repository name can be configured in MFA only if all the eDirectory users who require MFA exist in one repository of the AA server. If the eDirectory users who require MFA are spread across different repositories in AA, no need to configure the repository name in the MFA server.

   For Active Directory users, repository configuration is not required in the MFA server.

Configuring the MFA Server

1 Select the **OES MFA server** pattern in YaST during or post OES installation.

2 After successful installation of OES MFA Server pattern, run the command from the terminal console.

```
mfa-server-cli service-config
```

During `service-config`, enter the eDirectory administrator credentials and confirm the host name to be used for the MFA server.

NOTE: By default, the host name is automatically fetched from the system. MFA agent establish HTTPS connection using this host name, so it should match with the DNS name in the server certificate used by Apache server.

This initialize the database and brings up the MFA server service and **isDbConfigured** parameter appears as **true** (Shown in `mfa-server-cli print-config`).

Run `systemctl status mfa-server.service` command to check the status of MFA server service. To view the configuration parameters, run `mfa-server-cli print-config` command.

3 Run the command to configure the AA server details.

`mfa-server-cli auth-server --authSrvHost=`<AA server details> `--endPointID=`<id> `--endPointSecret=`<secret>

This updates the AA server address and AA endPoint information. The parameter **isAuthSrvConfigured** appears as **true** on the configuration parameter page.

4 Run the command to configure the information from the AA server.

`mfa-server-cli policy-config --event=`<AA event name> `--eDirRepo=`<Name of eDirectory repository in AA server>

This updates the AA event and repository information and the **isPolicyConfigured** appears as **true** on the configuration parameter page.

NOTE: eDirRepo configuration is optional, but recommended for better performance. Only one repository can be configured. eDirRepo can be configured, only if all eDirectory users who require MFA exist in one repository of the AA server. If eDirectory users are spread across different repositories in AA, repository name configuration is not required.

For Active Directory users, no configuration of repository is required in the MFA server. MFA server can identify the repository name of AD user.

5 On successful completion of steps 1 to 4, perform `mfa-server-cli print-config`.

If the MFA server configuration is successful, the **mfa-server** > **isConfigured** parameter appears as **true**, else perform a `service-cleanup`, and then do a `service-reconfig` to bring up the MFA server.

Configuration parameters can be modified using the utility `mfa-server-cli` as described in "Command Line Utility of MFA Server" on page 200.

16.6 Setting-Up Subsequent MFA Servers

Multiple MFA servers can be configured for high availability even though a single MFA server is sufficient for this functionality to work. All MFA servers run as replicas, using the same database and configuration.

NOTE: It is recommended to complete the configuration of the first server before setting up the additional MFA servers, so that new MFA servers can start with the configuration of the first server.

1 Select the **OES MFA server** pattern in YaST during or post the OES installation.

2 After successful OES installation, run the command from the terminal console.

`mfa-server-cli service-config`

This MFA server functions as a replica of the first server, utilizing the same database and configuration.

16.7 Configuring MFA Agent

MFA agent does not require any configuration to be functional. MFA agent runs automatically with the default configuration.

By default, MFA agent will be installed and running on all OES servers where an OES service which requires OES MFA service is configured. In this release, CIFS is the only service which require OES MFA service. It performs a service discovery to identify the available MFA servers in the eDirectory tree and automatically configures itself to use one of them. This discovery process can take up to 5 minutes.

Use the command `systemctl status mfa-agent.service` to check the status of MFA agent service. Use the command `mfa-agent-cli print-config` to view the configuration parameters of MFA agent.

Configuration parameters can be modified using the utility `mfa-agent-cli` as described in "Command Line Utility of MFA Agent" on page 204.

16.8 Configuring OES Services to Use MFA Service

NOTE: In this release, only the CIFS service utilizes the OES MFA service.

16.8.1 Configuring OES CIFS to Use MFA Service

For more information, see Multi-Factor Authentication for CIFS Service in OES CIFS for Linux Administration Guide.

16.9 Allowlist to Exempt from MFA

Admin can exempt the users or workstations from multifactor authentication by adding them to the allowlist. You can add or remove the allowlist entries such as eDirectory or Active Directory users, eDirectory or Active Directory groups, IP address of CIFS client workstation, IP address range of CIFS client workstations, or subnet of CIFS client workstations. Use `mfa-server-cli` utility to manage the allowlist in OES MFA server.

16.10 Command Line Utility of MFA Server

The utility `mfa-server-cli` can be used to configure MFA server.

16.10.1 Syntax

mfa-server-cli command [options]

```
mfa-server-cli --help

mfa-server-cli service-config

mfa-server-cli mfa-server [--port=<MFA server port> |
--clientCertCAPath=<CA certificate path> | --enforceClientAuth=<true/
false> | --mfaValidity=<Validity of MFA in minutes> |
--groupBasedAllowlist=<true/false>]

mfa-server-cli auth-server [--authSrvHost=<AA server address>
--endPointID=<id> --endPointSecret=<secret>]

mfa-server-cli policy-config [--event=<AA event name> |
--eDirRepo=<eDirectory repository in AA server>]

mfa-server-cli mfa-manage [--printAllMfaSessions=yes |
--deleteAllMfaSessions=yes | --allowlistType=<user/usergroup/address/
range/subnet> | --addToAllowlist=<allowlist entry value> |
--removeFromAllowlist=<allowlist entry value> | --printAllowlist=yes]

mfa-server-cli logging [--logLevel=<error/warn/info/debug> |
--logFilePath=<path> | --logTimeStampFormat=<format>]

mfa-server-cli service-cleanup

mfa-server-cli service-reconfig

mfa-server-cli print-config
```

16.10.2 MFA Server Commands and Options

service-config

Service configuration requires eDirectory tree administrator credentials. Confirm the host name to be used for the MFA server; it should match the DNS name in Apache server's default virtual host SSL certificate. Successful service configuration initializes the database and brings up the MFA server.

mfa-server

--port=<MFA server port>

The MFA server can use any port in range of 1024 to 65535. By default, MFA server uses port 3456. If the specified port number is not available, the MFA server uses the next available port.

--clientCertCAPath=<CA certificate path>

Path of CA certificate file used by MFA server to validate the client certificate of MFA agent. By default, this path is configured to use the eDirectory CA certificate.

--enforceClientAuth=<true/false>

If set to true, the validation of the client certificate presented by the MFA agent is enforced. By default, this value is true.

--mfaValidity=<Validity of MFA in minutes>

The period during which multifactor authentication (MFA) is valid for users. If the validity expires, the user is required to complete the second factor of authentication during their next login.

--groupBasedAllowlist=<true/false>

If set to true, eDirectory group or Active Directory group can be added to the allowlist. By default, this option is false.

auth-config

--authSrvHost=<AA server address>

IP address or host name of the AA server.

--endPointID=<id>

ID of endpoint created in AA server.

--endPointSecret=<secret>

Secret of the AA endpoint.

policy-config

--event=<AA event name>

Name of the event created in AA server.

--eDirRepo=<eDirectory repository in AA server>

Name of the eDirectory repository in the AA server, which is used for multifactor authentication of the eDirectory users. If the repository name is not configured, the AA server searches for the user in every available repository. For Active Directory (AD) users, the repository name is automatically detected by CIFS, and no additional configuration is required.

mfa-manage

--printAllMfaSessions=<yes>

Lists all valid MFA sessions. Expired sessions are not listed.

--deleteAllMfaSessions=<yes>

Deletes all the MFA sessions.

--allowlistType=<user/usergroup/address/range/subnet>

Specifies the type of entry to be added or removed from the allowlist. Use the `--allowlistType` with `--addToAllowlist` or `--removeFromAllowlist` options.

NOTE: Use LDAP format for eDirectory users or groups and SAM account Type format for Active Directory users or groups.

The following are the various allowlist entry types:

user

eDirectory user in LDAP format (example: cn=alen,o=myorg) or AD user in the format <netbios_name_of_domain\\username> (example: corpdom\\alex).

usergroup

eDirectory group in LDAP format (example: cn=salesteam,o=myorg) or AD user in the format <netbios_name_of_domain\\groupname> (example: corpdom\\salesteam).

IP address

IP address of CIFS client workstation (example: 168.10.100.25).

range

Range of IP address of CIFS client workstations (example: 168.10.100.1-168.10.100.100).

subnet

Subnet of CIFS client workstations (example: 168.10.100.0/24).

--addToAllowlist= <allowlist entry value>

Adds entry to the allowlist. Use this option with the `--allowlistType`. Entry can be eDirectory user, AD user, eDirectory group, AD group, workstation IP address, workstation IP address range, or workstation subnet depending on the `--allowlistType` specified.

--removeFromAllowlist= <allowlist entry value>

Removes entry from the allowlist. Use this option with the `--allowlistType`. Entry can be eDirectory user, AD user, eDirectory group, AD group, workstation IP address, workstation IP address range or workstation subnet depending on the `--allowlistType` specified.

--printAllowlist=<yes>

Prints the allowlist.

logging

--logLevel=<error/warn/info/debug>

Configures the log level. Default log level is info.

--logFilePath=<path>

Log file path of the MFA server. By default, the log file path is `/var/opt/novell/log/oes/mfaserver/mfaserver-<date>.log`.

--logTimeStampFormat=<format>

Log message time stamp format. By default, the time format is `YYYY-MM-DD HH:mm:ss`.

service-cleanup

Reverts the service configuration and stops the MFA server.

service-reconfig

Reconfigure the MFA server after a service cleanup. eDirectory administrator credentials are not required while reconfiguring an MFA server. Confirm the hostname for the MFA server.

print-config

Prints the configuration parameters of the MFA server.

16.10.3 Examples

mfa-server print-config

Prints the MFA server configuration.

mfa-server-cli service-config

Initializes the database and brings up the MFA server.

mfa-server-cli auth-server --authSrvHost=aafservermultifactor.org --endPointID=c8572fec304411eea6c60242ac110003 --endPointSecret=jzhleNLbwid75IA0AgQNZ30Lca0U6wh0

Adds the AA server details for the MFA server.

mfa-server-cli policy-config --event=cifs_aaf_event --eDirRepo=CIFS_USERS_AAF_REPO

Adds the AA configuration details for the MFA server.

mfa-server-cli service-cleanup

Reverts the service configuration and stops the MFA server.

mfa-server-cli mfa-manage --allowlistType=user --addToAllowlist=cn=alen,o=myorg

Adds an eDirectory user to the allowlist.

mfa-server-cli mfa-manage --allowlistType=usergroup --addToAllowlist=corpdom\\salesteam

Adds an Active Directory group to the allowlist.

mfa-server-cli mfa-manage --allowlistType=address --addToAllowlist=168.10.100.25

Adds the IP address of CIFS client workstation to the allowlist.

mfa-server-cli mfa-manage --allowlistType=subnet --removeFromAllowlist=168.10.100.0/24

Removes a subnet of CIFS client workstations from the allowlist.

mfa-server-cli mfa-manage --allowlistType=range --removeFromAllowlist=168.10.100.1-168.10.100.100

Removes an IP address range of CIFS client workstations from the allowlist.

16.11 Command Line Utility of MFA Agent

The utility `mfa-agent-cli` can be used to change the configuration parameters of MFA agent.

16.11.1 Syntax

mfa-agent-cli command [options]

```
mfa-agent-cli --help
```

```
mfa-agent-cli mfa-agent [--enableServiceDiscovery=<true or false> |
--clientCertPath=<certificate path> | --clientCertKeyPath=<certificate key
file path> | --logLevel=<error/warn/info/debug> | --logFilePath=<path> |
--logTimeStampFormat=<format>]
```

```
mfa-agent-cli mfa-server [--AddMfaServerHost=<MFA server address> |
--RemoveMfaServerHost=<MFA server address>]
```

```
mfa-agent-cli print-config
```

16.11.2 MFA Agent Commands and Options

`mfa-agent`

--enableServiceDiscovery=<true or false>

If set to true, MFA agent automatically discovers the MFA servers available in the eDirectory tree. By default, this value is true.

--clientCertPath=<certificate path>

Path of the client certificate file used by MFA agent. By default, this is configured to use the eDirectory certificate.

--clientCertKeyPath=<certificate key file path>

Path of the client certificate private key used by MFA agent. By default, this is configured to use the eDirectory certificate private key.

---logLevel=<error/warn/info/debug>

Configures the log level. Default log level is info.

--logFilePath=<path>

Log file path of MFA agent. By default, the log file path is `/var/opt/novell/log/oes/mfaagent-<date>.log`.

--logTimeStampFormat=<format>]

Time stamp format in log message. By default, the time format is `YYYY-MM-DD HH:mm:ss`.

`mfa-server`

These configurations are used only when the **enableServiceDiscovery** is **false**.

--AddMfaServerHost=<MFA server address>

Adds the IP address or host name of the server to the list of MFA servers. Any number of MFA servers can be added to the list.

--RemoveMfaServerHost=<MFA server address>

Removes the server from the list of MFA servers.

`print-config`

Prints the configuration parameters of the MFA agent.

16.12 Important Files and Folders

MFA server log file is available in the path:

`/var/opt/novell/log/oes/mfaserver`

MFA agent log file is available in the path:

`/var/opt/novell/log/oes/mfaagent`

16.13 Security Configurations

- Section 16.13.1, “mTLS between MFA Server and MFA Agent,” on page 206
- Section 16.13.2, “HTTPS Communication between Advanced Authentication Server, MFA Server, and Smartphone,” on page 207

16.13.1 mTLS between MFA Server and MFA Agent

Communication between MFA server and MFA agents is protected using mutual TLS (mTLS). MFA server runs behind Apache server using it as a reverse proxy, hence TLS connection terminates at Apache server.

By default, Apache server uses eDirectory server certificate available at `/etc/ssl/servercerts/servercert.pem`. The CA certificate of this server certificate is installed by default on all MFA agents. If administrator want to use any server certificate other than the default eDirectory certificate, its CA certificate must be available in all MFA agents. If the certificate is not available, it can be installed by copying it to the path `/usr/share/pki/trust/anchors`.

By default, MFA agents use eDirectory certificate available at `/etc/ssl/servercerts/servercert.pem` as client certificate. MFA servers verify the client certificates using the CA certificate before allowing connections from MFA agents. By default, CA certificate of eDirectory certificate is installed in MFA servers. If administrators want to use any client certificate other than the default eDirectory certificate, its CA certificate should be available in the MFA server. If the certificate is not available, it can be installed by copying it to the path `/usr/share/pki/trust/anchors`.

By default, validation of the client certificate is enforced at the MFA server. This can be disabled using the command `mfa-server-cli mfa-server --enforceClientAuth=false`.

16.13.2 HTTPS Communication between Advanced Authentication Server, MFA Server, and Smartphone

Communication between AA server, MFA server, and smartphone are secured using TLS. AA server should be configured with a valid server certificate and its CA certificate should be available in MFA servers and smartphone. If CA certificate is not available in the MFA server, it can be installed by copying it to the path `/usr/share/pki/trust/anchors`.

16.14 Troubleshooting

- Section 16.14.1, ""Unable to verify the first certificate" message in MFA server log," on page 207
- Section 16.14.2, ""Unable to verify the first certificate" message in MFA agent log," on page 207
- Section 16.14.3, "Unable to configure MFA server or MFA agents or unable to discover MFA servers," on page 207
- Section 16.14.4, "Configuration changes done on one MFA server is not reflecting on the other MFA servers," on page 208
- Section 16.14.5, "Unable to configure MFA server post Transfer ID migration of the UMC server," on page 208
- Section 16.14.6, "Unable to configure MFA parameters with a value that begin with the character `$`," on page 208

16.14.1 "Unable to verify the first certificate" message in MFA server log

Action: Administrator must install CA certificate for the server certificate used by AA server in MFA server.

To install CA certificate, copy the CA certificate to the location `/usr/share/pki/trust/anchors`.

16.14.2 "Unable to verify the first certificate" message in MFA agent log

Action: Administrator must install CA certificate for the server certificate used by MFA server in MFA agent.

To install CA certificate, copy the CA certificate to the path `/usr/share/pki/trust/anchors`. By default, MFA server uses eDirectory certificate and the CA certificate is installed on all MFA agents.

16.14.3 Unable to configure MFA server or MFA agents or unable to discover MFA servers

To verify the status of the MFA server, run the following commands:

```
systemctl status mfa-server.service
```

```
systemctl status microfocus-umc-backend.service
```

```
systemctl status apache2.service
```

```
mfa-server-cli print-config
```

To verify the status of the MFA agent, run the following commands:

```
systemctl status mfa-agent.service
```

```
systemctl status microfocus-umc-backend.service
```

```
mfa-agent-cli print-config
```

To verify the status of the UMC server, run the following commands:

```
systemctl status microfocus-umc-server.service
```

```
umcServiceHealth -a
```

16.14.4 Configuration changes done on one MFA server is not reflecting on the other MFA servers

Action: Administrator must restart the mfa service on the MFA servers where the configuration changes are not reflecting.

To restart the MFA service, run the command `systemctl restart mfa-server.service`.

16.14.5 Unable to configure MFA server post Transfer ID migration of the UMC server

Action: Post Transfer ID migration, if the UMC server is not available, perform the steps provided in UMC Unavailable on the Target Server of the Migration Tool Administration Guide.

When UMC server is available, configure the MFA server.

16.14.6 Unable to configure MFA parameters with a value that begin with the character $

Action: To resolve this issue, enter “\” followed by the parameter value.

For example, mfa-server-cli policy-config --event=\$xyz

17 Security Considerations

This section includes issues that you should consider when installing and configuring a Open Enterprise Server (OES) Linux server.

- Section 17.1, “SSRF through Host Header Injection,” on page 209
- Section 17.2, “Enforce Secure HTTPS Browser Connections with Apache,” on page 210
- Section 17.3, “Access to the Server During an Installation or Upgrade,” on page 210
- Section 17.4, “Remote Installations Through VNC,” on page 210
- Section 17.5, “Improperly Configured LDAP Servers,” on page 211

17.1 SSRF through Host Header Injection

Server-Side Request Forgery (SSRF) through Host header injection occurs when attackers use unauthorized malicious Host headers and manipulate server-side requests to redirect traffic, bypass access controls, or exploit server behavior.

You can fix this issue by dynamically allowing only trusted Host headers (IP address or hostname) by denying unauthorized requests to prevent exploitation of SSRF and Host Header Injection vulnerabilities.

For authorized requests, RewriteCond ensures that the Host header request matches the accepted entries.

For unauthorized requests, RewriteRule denies the Host header request with a 403 Forbidden response (F) and stops further rule processing (L).

To resolve the SSRF vulnerability issues, perform the following steps:

1. In the terminal window, locate `/opt/novell/oes-install/util/fixHeaderInjectionVhost.py` file.
2. Execute `python3 /opt/novell/oes-install/util/fixHeaderInjectionVhost.py`

   The script dynamically updates the `/etc/apache2/vhosts.d/vhost-ssl.conf` Apache SSL virtual host configuration file with the IP address and hostname.

   ```
   RewriteCond %{HTTP_HOST} !^(<server-ip>|<server-hostname>|127\.0\.0\.1|localhost)$ [NC]
   ```

   RewriteRule ^ - [F,L]

   `<server-ip>`: IP address of the primary server.

   `<server-hostname>`: FQDN of the server.

   127.0.0.1 (local server): Loopback IP address for localhost.

   Localhost: Default local hostname.

3. Restart Apache service to apply the changes.

   ```
   systemctl restart apache2.service
   ```

NOTE: To add additional IP address or hostname, it must be manually added to `/etc/apache2/vhosts.d/vhost-ssl.conf` Apache configuration file.

```
RewriteCond %{HTTP_HOST} !^(<server-ip>|<server-
hostname>|127\.0\.0\.1|localhost|additional-ip|additional-hostname)$ [NC]
```

Apache service must be restarted to apply the changes.

17.2 Enforce Secure HTTPS Browser Connections with Apache

OES uses Apache as web server for services such as UMC, iManager, and MFA. The HTTP Strict Transport Security (HSTS) response header must be added to the virtual host configuration to enforce HTTPS.

To enable HSTS, perform the following steps:

1. In the terminal window, open the file `/etc/apache2/vhosts.d/vhost-ssl.conf`.
2. In <VirtualHost _default_:443> block, add HSTS header line.

   Example 17-1 *Sample HSTS header to enforce HTTPS for two years (max age in seconds)*

   ```
   Header always set Strict-Transport-Security max-age=63072000
   ```
3. Restart Apache using `systemctl restart apache2` command.

For more information, see Apache Documentation.

17.3 Access to the Server During an Installation or Upgrade

Because eDirectory passwords are not obfuscated in system memory during the installation or upgrade, we recommend not leaving a server unattended during installation, upgrade, or configuration.

You can use SSH (secure shell) to access the system to perform an installation. However, only authorized users can access the installation.

17.4 Remote Installations Through VNC

When you install the server, we recommend that you do not use Virtual Network Computing (VNC) for remote installation in an untrusted environment. Consider using one of the more secure options (such as SSH) as outlined in "Installation Scenarios for Remote Installation" in the *SLES 15 SP4 Deployment Guide*.

17.5 Improperly Configured LDAP Servers

Issue 1: Improperly configured LDAP servers allow any user to connect to the server and query for information.

An eDirectory LDAP server enables NULL BIND by default, but allows it to be disabled on the server. To enhance the security of the OES server, disable the NULL BIND on LDAP server port 389. See Configuring LDAP Services for NetIQ eDirectory in the NetIQ eDirectory Administration Guide.

Issue 2: Improperly configured LDAP servers allow the directory BASE to be set to NULL. This allows information to be culled without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous user can query your LDAP server through a tool such as LdapMiner.

An eDirectory LDAP server allows the directory BASE to be set to NULL, and there is no way to disable it. However, with the NULL BIND disabled, as previously mentioned, the security threat posed by this feature is minimized. For more information on NULL BIND, see Nessus Scan Results in the NetIQ eDirectory Administration Guide.

18 Troubleshooting

This section presents information on troubleshooting the OES installation and configuration.

- Section 18.1, “Prompt for Untrusted GnuPG Key During Upgrade,” on page 213
- Section 18.2, “Upgrade Failure in SUSE Xen Hypervisor Environment,” on page 213
- Section 18.3, “PID File Unavailable Message,” on page 214
- Section 18.4, “`systemctl kill Not Supported,” on page 214`
- Section 18.5, “Executing kinit Command Fails in .LOCAL Domain,” on page 214
- Section 18.6, “The OES Service Pattern Icons are not Displayed and OES Patterns are not in the Proper Order,” on page 214
- Section 18.7, “Deleting the Existing eDirectory Objects when Reinstalling the OES Server or Reconfiguring the eDirectory,” on page 215
- Section 18.8, “Problem In Assigning IP Address For autoinst.xml-based Installations,” on page 215
- Section 18.9, “eDirectory Restart Results in an Error Message on a Non-DSfW Server,” on page 215
- Section 18.10, “The DEFAULT SLP Scope Gets added to the slp.conf File During an Upgrade to OES 2018 or later,” on page 216
- Section 18.11, “The change_proxy_pwd.sh Script Fails to Synchronize Password,” on page 216
- Section 18.12, “OES Installation Fails Due to Encrypted OES Media URL in the autoinst.xml File,” on page 217
- Section 18.13, “Installing or Upgrading to OES 24.4 using AutoYaST Creates the OES Repository Name Using Random Characters,” on page 217
- Section 18.14, “Verification of the Container Object Fails During the AD Domain Join Process,” on page 218
- Section 18.15, “Timing Issues for OES on Xen,” on page 218

18.1 Prompt for Untrusted GnuPG Key During Upgrade

Issue: During an upgrade with NU, SMT, or SUSE Manager registration, you may see a prompt to Import an Untrusted GnuPG Key with the message **The key has expired** for the *OES24.4-SLE-Module-Basesystem15-SP4-Pool* repository.

Workaround: Click **Trust** to continue.

18.2 Upgrade Failure in SUSE Xen Hypervisor Environment

Upgrade to OES 23.4 fails in a SUSE Xen environment. This issue is fixed with the latest ISO. Download the ISO before performing an upgrade.

18.3 PID File Unavailable Message

After the service start is complete, systemd verifies for the presence of PID file. If the PID file is not found, the following message can be seen in /var/log/messages and also through systemctl status command.

`<service>.service: PID file <file path>.pid not readable (yet?) after start: No such file or Directory`

Such messages can be ignored, because the service would still be coming up in the background and creating its PID file later.

18.4 `systemctl kill` Not Supported

The command `systemctl kill <service name>.service` is not supported by many of the OES services. You can instead use the command `systemctl stop <service name>.service`.

18.5 Executing kinit Command Fails in .LOCAL Domain

If mDNS is installed in OES and LOCAL domain is used, the DNS name resolution on .LOCAL domain by default go to mDNS and kinit utility try to resolve the hostname of the domain controller. If mDNS is not properly configured in the network, then the name resolution and kinit fails.

To resolve this issue, change the order of name resolution method in `/etc/nsswitch.conf` as follows:

Old configuration: "hosts: files mdns4_minimal [NOTFOUND=return] dns"

New configuration: "hosts: files dns mdns4_minimal [NOTFOUND=return]"

18.6 The OES Service Pattern Icons are not Displayed and OES Patterns are not in the Proper Order

To install or configure any new OES service, OES media should be available and the priority should be higher than the OES pools repositories. This issue occurs when the OES media is not available or the media has lower or equal priority than the OES pool.

To resolve this issue, add OES media. If the problem still exist, run the following command to increase the OES media priority.

`zypper mr -p <priority> <OES_medianame>`

For example, `zypper mr -p 98 OES_media`

18.7 Deleting the Existing eDirectory Objects when Reinstalling the OES Server or Reconfiguring the eDirectory

When you reinstall an existing OES server with the same name or reconfigure eDirectory, the system might throw an error prompting to delete the existing eDirectory objects.

Before clicking Retry, ensure to delete the following objects using iManager. Else, the OES re-installation or eDirectory reconfiguration will not proceed.

The list of objects that must be deleted:

- NCP Server Object
- HTTP Server Object
- SAS Objects
- SNMP Group Objects
- LDAP Server and Group objects
- Certificates (IP AG, SSL Certificate IP, DNS AG, and SSL Certificate DNS)

18.8 Problem In Assigning IP Address For autoinst.xml-based Installations

When you use the `autoinst.xml` for a new installation, you will not be able to set the IP address on the target server unless the following change is made:

Before starting the installation, remove the <net-udev> tags along with its contents from the `autoinst.xml` file, and then use modified file for the new installation.

OR

Before starting the installation, edit the autoinst.xml file and change the mac address in the following tag <\value> enter mac address of the target server </value> that is available under the <net-udev> tag.

18.9 eDirectory Restart Results in an Error Message on a Non-DSfW Server

On a non- DSfW Server, if you restart eDirectory, the following error message is received: “Method load failed: libxadnds.so.2: cannot open shared object file: No such file or directory.”

This is because three NMAS methods (IPCExternal, Kerberos, and Negotiate) fail to load on the server. These NMAS methods that are specific to DSfW are part of the `novell-xad-nmas-methods` rpm and depend on the libraries from the `novell-xad-framework` rpm. Since the `novell-xad-framework` rpm is part of the DSfW pattern and is installed only on a DSfW server, you receive this error message on a non-DSfW server.

If you receive this error message, you can ignore this message as these DSfW NMAS methods do not function in a non-DSfW server and do not impact any eDirectory functionality.

18.10 The DEFAULT SLP Scope Gets added to the slp.conf File During an Upgrade to OES 2018 or later

When you upgrade an OES server that is configured as an SLP DA to OES 2018 or later, the DEFAULT SLP scope gets added to the `slp.conf` file along with the SLP scope configured by you. This might result in adding extra load to the OES server.

To prevent the extra load, remove the term DEFAULT from the following line in the `/etc/slp.conf` file, and restart the OES server for the changes to take effect.

```
net.slp.useScopes = DEFAULT,<slp scope configured by you>
```

NOTE: This issue is not applicable to OES servers that point to an SLP DA or whose SLP scope is DEFAULT.

This issue will not be seen in upgrades from OES 2015 to future OES releases.

18.11 The change_proxy_pwd.sh Script Fails to Synchronize Password

Whenever the common proxy user password is not synchronized across OES Credential Store, eDirectory and various other OES services, the change_proxy_pwd.sh script fails with the following error: NDS error failed authentication -669.

To resolve:

1. Take a note of the current proxy user name and password using the following commands:

   ```
   /opt/novell/proxymgmt/bin/cp_retrieve_proxy_cred username
   /opt/novell/proxymgmt/bin/cp_retrieve_proxy_cred password
   ```

2. Try logging into NDS using the following command: `ndslogin <proxy user name in dot format>`. Example: `ndslogin cn=OESCommonProxy_wgp-drs22.o=novell`.

   Successful login indicates that the common proxy credentials are in sync with eDirectory and OES Credential Store. If the login is unsuccessful, change the common proxy user password in eDirectory using iManager, then follow Step 1 and Step 3.

3. To synchronize the passwords across OES Credential Store, eDirectory and various other OES services, export the proxy user password to the service specific environment variable, then run the service specific proxy credential script (`<service_name>_update_proxy_cred.sh`) that is available at `/opt/novell/<service_name>/bin`.

   For example, to synchronize the password of the CIFS service with OES Credential Store and eDirectory:

   - Export the proxy user password to the CIFS environment variables using the `export OES_CIFS_DATA="proxy user password retrieved in Step 1"` command.
   - Run the CIFS proxy credentials update script using the `/opt/novell/cifs/bin/cifs_update_proxy_cred.sh <specify proxy username retrieved in Step 1>` command.

   Repeat this step for each of the services installed on your OES server.

18.12 OES Installation Fails Due to Encrypted OES Media URL in the autoinst.xml File

The `autoinst.xml` file generated on an OES server that is subscribed to the Micro Focus Customer Center channel will have the OES media URL in an encrypted form. An OES installation with that XML file will fail with the following error: “failed to add add-on product.”

To resolve this issue, replace the OES media URL with the actual installation source path and retry the installation.

```
<add_on_products config:type="list">
  <listentry>
     <media_url><![CDATA[https://
866254f853cb4f668594269ecec05dd9:f62283a76d964e4b8c0cebd447fdd54a@nu.novel
l.com/repo/$RCE/OES23.4-Pool/sle-15-x86_64]]></media_url>
       <product>OES</product>
     <product_dir></product_dir>
  </listentry>
</add_on_products>
```

18.13 Installing or Upgrading to OES 24.4 using AutoYaST Creates the OES Repository Name Using Random Characters

Before you start the installation of OES 24.4, ensure to edit the `autoinst.xml` file and modify the OES alias name to a meaningful one. Else, the OES alias name will be displayed in some random characters.

```
<add_on_products config:type="list">
  <listentry>
    <media_url><![CDATA[http://192.168.1.1/install/OES23.4/GMC/x86_64]]></
media_url>
         <product>OES</product>
         <product_dir>/</product_dir>
         <name>MyOES_name</name>
         <alias>MyOES_alias</alias>
  </listentry>
</add_on_products>
```

18.14 Verification of the Container Object Fails During the AD Domain Join Process

“Error: Verification of container object failed. Ensure that the AD Server is reachable.”

If you encounter the above error during the AD domain join process, ensure that you have set the following:

- AD server's reverse lookup entry (IPv4) in the DNS server before the domain join operation is performed.
- AD domain name to which the OES server will be joined to as part of the Domain Search in OES server network settings.

18.15 Timing Issues for OES on Xen

eDirectory relies on time being synchronized; connections with eDirectory are lost if the system time is different in the host operating system (SLES 15 SP4). Ensure that you understand and follow the instructions in Xen Virtual Machine Clock Settings in the Virtualization Guide.

A OES File and Data Locations

This section contains information about the general rules and conventions that Micro Focus follows when determining where various data types and program components are stored on the Linux file system.

Where possible, we have tried to ensure that Open Enterprise Server (OES) components follow Linux Standard Base (LSB) requirements regarding file location. Efforts to do this are detailed here.

- Section A.1, “General Rules,” on page 219
- Section A.2, “Exceptions,” on page 220

A.1 General Rules

Where possible, product design has followed these rules:

- **/opt/novell:** Contains all static data in the following standard subdirectories.

`/opt/novell/bin`	Executable files that are used by multiple products or are intended to be executed by an end user.
`/opt/novell/`*`service`*`/sbin`	Executable files that are used only by a product and are not executed by an end user.
`/opt/novell/lib`	Shared libraries that are used by multiple products and shared or static libraries that are part of an SDK.
`/opt/novell/include`	Header files for SDKs, typically in a product subdirectory.
`/opt/novell/lib64`	Contains 64-bit shared libraries.

- **/etc/opt/novell:** Generally contains host-specific configuration data.

  If a product has a single configuration file, it is named *`product or service`*`.conf`.

  If a product uses multiple configuration files, they are placed in a subdirectory named for the product or service.
- **/etc/opt/novell/*service_name*:** Contains various OES service configuration files.
- **/var/opt/novell:** Contains all variable data.

  Variable data (data that changes during normal run time operations) is stored in a product or service subdirectory.
- **/var/opt/novell/log:** Generally contains log files.

  If a product or service has a single log file, it is stored in a file with the product or service name.

  If a product or service has multiple log files, they are stored in a subdirectory named for the product or service.

- **/var/log:** Contains the log messages and the YaST logs.
- All files and directories that could not follow the above rules have the prefix *novell-* where possible.

A.2 Exceptions

Some files must reside in nonstandard locations for their products to function correctly. Two examples are systemd unit files for OES services, and cron scripts, which must be in `/etc/cron.d`. When possible, these files have a `novell-` prefix.

When standard conventions preclude the use of prefixes (such as PAM modules, which use suffixes instead of prefixes), the standard conventions are followed.

B AutoYaST XML Tags

This section describes the XML tags used in the `autoinst.xml`, which is generated during the OES clone process. For more information on the XML tags related to SLES, see SUSE Linux Enterprise Server 15 SP4 AutoYaST.

NOTE: The description of tags provided here are for information only. Do not modify any of the tags in a real-time environment other than the ones specified in the Section 9.4, “Cloning an OES Server Post OES Installation and Configuration,” on page 159 section. All the passwords stored in the `autoinst.xml` file will be in clear text.

- Section B.1, “edirectory,” on page 221
- Section B.2, “imanager,” on page 227
- Section B.3, “iprint,” on page 228
- Section B.4, “ncpserver,” on page 228
- Section B.5, “ncs,” on page 228
- Section B.6, “novell-cifs,” on page 230
- Section B.7, “novell-dhcp,” on page 231
- Section B.8, “novell-dns,” on page 232
- Section B.9, “novell-lum,” on page 233
- Section B.10, “nss,” on page 235
- Section B.11, “oes-ldap,” on page 235
- Section B.12, “sms,” on page 236
- Section B.13, “novell-nssad,” on page 237
- Section B.14, “oes-umc,” on page 238
- Section B.15, “oes-database,” on page 238

B.1 edirectory

Attribute Name	Description
ocs_store	Always set this to 'yes' so that the proxy credentials are stored in OCS. Example: <ocs_store>yes</ocs_store>

Attribute Name	Description
cert_mutual	Set this to 'yes' when you want to implement the Certificate Mutual login method. It implements the Simple Authentication and Security Layer (SASL) EXTERNAL mechanism, which uses SSL certificates to provide client authentication to eDirectory through LDAP. Example: <cert_mutual>no</cert_mutual>
challenge_response	Set this to 'yes' when you want to enable the Challenge-Response login method. It works with the Identity Manager password self-service process. This method allows either an administrator or a user to define a password challenge question and a response, which are saved in the password policy. Then, when users forget their passwords, they can reset their own passwords by providing the correct response to the challenge question. Example: <challenge_response>yes</challenge_response>
create_server_object	Set this to 'Yes' when you want to create a DNS server object. Example: <create_server_object>yes</create_server_object>
dib_location	Specify the path of the nds databse. Example: <dib_location>/var/opt/novell/eDirectory/data/dib</dib_location>
digest_md5	Set this to 'yes' when you want to implement the Digest MD5 login method. It implements the Simple Authentication and Security Layer (SASL) DIGEST-MD5 mechanism as a means of authenticating the user to eDirectory through LDAP. Example: <digest_md5>no</digest_md5>
domain_name	Specify the DSfW DNS domain name. The value of this tag and xad_domain_name tag should be same. Example: <domain_name>acme.com</domain_name>
existing_dns_ip	Specify the existing DNS server IP address. Example: <existing_dns_ip>192.168.1.1</existing_dns_ip>
group_context	Specify the DNS DHCP group object context. Example: <group_context>ou=OESSystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</group_context>
host_name	Specify the host name of the current server where the installation is being done. Example: <host_name>acme-208</host_name>
http_port	Specify the HTTP port of the eDirectory server where the installation is being done. Example: <http_port t="integer">8028</http_port>
https_port	Specify the HTTPS port of the current eDirectory server. Example: <https_port t="integer">8030</https_port>

Attribute Name	Description
install_secretstore	Set to 'yes' when you want to install the secret store. Example: <install_secretstore>yes</install_secretstore>
install_universalstore	Set to 'yes' when you want to install the universal store. Example: <install_universalstore>no</install_universalstore>
ldap_basedn	Specify the DNSs server's CN name. This is required only in case of DSfW server. Example: <ldap_basedn>ou=OESSystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</ldap_basedn>
ldap_server	Specify the IP address of the DNS LDAP server. Example: <ldap_server>192.168.1.1</ldap_server>
locator_context	Specify the DNS locator object context where the DNS servers or zones are present. Example: <locator_context>ou=OESSystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</locator_context>
migrate_option	Always set this to 'no' as the migrate NKDC realm to DSfW domain is discontinued. Example: <migrate_option>no</migrate_option>
nds	Set to this to 'yes' when you want to use the NDS login method that provides secure password challenge-response user authentication to eDirectory. Example: <nds>yes</nds>
ntp_server_list	Specify reliable NTP servers IP addresses. Example: <ntp_server_list t="list"> <listentry>192.168.1.5</listentry> </ntp_server_list>
overwrite_cert_files	Set this to 'yes' when you want eDirectory to automatically back up the currently installed certificate and key files and replace them with files created by the eDirectory Organizational CA (or Tree CA). Example: <overwrite_cert_files>yes</overwrite_cert_files>
replica_server	Specify the IP address of the master eDirectory server. Example: <replica_server>192.168.1.5</replica_server>
runtime_admin	Specify the common proxy user context of the DNS. Example: <runtime_admin>cn=OESCommonProxy_host1,ou=OESSystemObjects,dc=acme,dc=com</runtime_admin>

Attribute Name	Description
runtime_admin_password	Specify the common proxy DNS password. Example: <runtime_admin_password>SAM23#$</runtime_admin_password>
sasl_gssapi	Set this to 'yes' when you want to implement the SASL GSSAPI login method. It implements the Generic Security Services Application Program Interface (GSSAPI) authentication using the Simple Authentication and Security Layer (SASL) that enables users to authenticate to eDirectory through LDAP using a Kerberos ticket. Example: <sasl_gssapi>no</sasl_gssapi>
server_context	Specify the eDirectory server context where there eDirectory server object needs to be created. Example: <server_context>ou=wdc,o=acme</server_context>
server_object	Specify the eDirectory server object name that has the object name and context. Example: <server_object>cn=DNS_edir-acme-208,ou=OESSystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</server_object>
simple_password	Set this to 'yes' when you want to implement the Simple Password NMAS login method. It provides password authentication to eDirectory. The Simple Password is a more flexible but less secure alternative to the NDS password. Simple Passwords are stored in a secret store on the user object. Example: <simple_password>no</simple_password>
slp_backup	Set this to 'yes' when you want the SLP server to periodically back up all registrations. This works only when the server is configured as a DA (Directory Agent). Example: <slp_backup>yes</slp_backup>
slp_backup_interval	Specify the SLP backup time in seconds. The default is (900 seconds or 15 minutes). If the server is configured as Director Agent, this value will be used. Example: <slp_backup_interval>900</slp_backup_interval>
slp_da	Specify the list of IP addresses of the SLP Directory Agents. Example: <slp_da t="list"> <listentry>198.162.1.1</listentry> </slp_da>
slp_dasync	Set this to 'yes' when you want to enable SLPD to sync service registration between SLP Das on startup. If the server is configured as Director Agent, this value be used. Example: <slp_dasync>no</slp_dasync>

Attribute Name	Description
Slp_mode	Specify the SLP mode to multicast, da, or da_server. By default, it is set to multicast. Example: <slp_mode>da</slp_mode>
slp_scopes	This is a comma delimited list of strings indicating the only scopes a UA or SA is allowed when making requests or registering or the scopes a DA must support. The default value is DEFAULT. Example: <slp_scopes>DEFAULT</slp_scopes>
tls_for_simple_binds	Set this to 'yes' when you require TLS for SIMPle binds with passwords. Example: <tls_for_simple_binds>yes</tls_for_simple_binds>
tree_type	Specify the type of eDirectory tree: new or existing. Example: <tree_type>new</tree_type>
use_secure_port	Set this to 'yes' when you want the DNS to use the secure port for communication in an DSfW environment. Example: <use_secure_port>yes</use_secure_port>
xad_admin_password	Specify the DSfW domain administrator password. Example: <xad_admin_password>SAM23#$</xad_admin_password>
xad_config_dns	Set this to 'yes' when you want to configure this domain controller also as a DNS server. Example: <xad_config_dns>yes</xad_config_dns>
xad_convert_existing_container	Set this to 'yes' for name mapped installations. In named mapped installations, the DSfW domain is mapped to an already existing eDirectory partition in the eDirectory tree. Example: <xad_convert_existing_container>no</xad_convert_existing_container>
xad_domain_name	Specify the DSfW DNS domain name. The value of this tag and domain_name tag should be same. Example: <xad_domain_name>acme.com</xad_domain_name>
xad_domain_type	Specify the DSfW domain type: forest, domain or controller. ◆ Forest: Use it for the first domain in the DSfW forest. ◆ Domain: Use it for the subsequent child domain(s) in the DSfW forest. ◆ Controller: Use it for subsequent domain controller(s) for any DSfW domain in the DSfW forest. Exmple: <xad_domain_type>forest</xad_domain_type>

Attribute Name	Description
xad_existing_container	Specify the eDirectory partition that the DSfW domain is being mapped to. This is effective only when the xad_convert_existing_container tag is set to 'yes'. Example: <xad_existing_container>ou=OESSystemObjects, o=acme</xad_existing_container>
xad_forest_root	Specify the forest root domain name in the DSfW forest. Example: <xad_forest_root>acme.com</xad_forest_root>
xad_ldap_admin_context	Specify the eDirectory tree admin context. In a name-mapped installation, for all the modes of DSfW installation, this tag will point to the (existing) eDirectory tree's tree administrator. Example: cn=admin,ou=admins,o=acme. <xad_ldap_admin_context>cn=admin,ou=admins,o=acme</xad_ldap_admin_context> In a non-name mapped installation, the forest root domain administrator is also the eDirectory tree administrator. For all the modes of installation, this tag will point to the forest root domain administrator. For example, for the forest root domain acme.com, the default forest domain administrator will be <xad_ldap_admin_context>cn=administrator,cn=users,dc=acme,dc=com</xad_ldap_admin_context> For example, for the child domain sales.example.com, the default forest domain administrator will be <xad_ldap_admin_context>cn=administrator,cn=users,dc=example,dc=com</xad_ldap_admin_context>
xad_ldap_admin_password	Specify the eDirectory tree administrator password. Example: <xad_ldap_admin_password>SAM23#$</xad_ldap_admin_password>
xad_netbios	Specify the NetBIOS name of the DSfW domain. Example: <xad_netbios>EXAMPLE</xad_netbios>
xad_parent_domain	Specify the DSfW domain name of immediate DSfW parent domain. For example, for a domain sales.acme.com, the value will be, <xad_parent_domain>acme.com</xad_parent_domain>
xad_parent_domain_address	Specify the IP address of any one of the parent DSfW domain controller. For example, for the domain sales.acme.com, specify the IP address of the DSfW DC hosting the domain acme.com. <xad_parent_domain_address>192.168.1.1</xad_parent_domain_address>
xad_parent_domain_admin_context	Specify the immediate DSfW parent domain's administrator context. For example, for the domain sales.acme.com, <xad_parent_domain_address>cn=administrator,cn=users,dc=acme,dc=com</xad_parent_domain_address>

Attribute Name	Description
xad_parent_domain_admin_password	Specify the immediate DSfW parent domain's administrator password. Example: <xad_parent_domain_admin_password>SAM23#$</xad_parent_domain_admin_password>
xad_replicate_partitions	Always set this to 'yes'. This indicates that the replicas of the configuration and schema partitions will be added to the local domain controller. Example: <xad_replicate_partitions>yes</xad_replicate_partitions>
xad_retain_policies	Set this to 'yes' when you want to retain the existing NMAS universal password policies. Example: <xad_retain_policies>yes</xad_retain_policies> **NOTE:** If set to 'no', the DSfW configuration will override the existing password policies if any.
xad_service_configured	Always specify this value to 'yes' when you want to configure DSfW. Example: <xad_service_configured>yes</xad_service_configured>
xad_site_name	Specify the site name to which this domain controller should be associated with. Otherwise the default value should be 'Default-First-Site-Name'. Example: <xad_site_name>Default-First-Site-Name</xad_site_name>
xad_wins_server	Specify 'yes' when you want to configure the DSfW domain controller as WINS server. Example: <xad_wins_server></xad_wins_server> **NOTE:** Only one domain controller in a DSfW domain should be designated as WINS server.

B.2 imanager

Attribute Name	Description
configure_now	Set this to 'true' always in AutoYaST based installations. Example: <configure_now t="boolean">true</configure_now>
install_plugins	Set to 'yes' to install all the iManager npms. Example: <install_plugins>yes</install_plugins>

B.3 iprint

Attribute Name	Description
ldap_server	Specify the IP or DNS name of the LDAP server that is used for authentication by iPrint during secure printing and management operations. Example: <ldap_server>192.168.1.2</ldap_server>
top_context	Specify the context (and its entire subtree) that is used to find the user during authentication. Example: <top_context>o=acme</top_context>

B.4 ncpserver

Attribute Name	Description
configure_now	Set this to 'true' always as NCP is a must for OES to work. Example: <configure_now t="boolean">true</configure_now>

B.5 ncs

NOTE: Novell Cluster Services does not support using autoyast to configure cluster nodes for new clusters or existing clusters. If you create an autoyast file from a cluster node, you must remove or comment out the NCS section before you use it to build or rebuild a server. After the server is up and running successfully, you can manually configure the node for clustering by using the OES Install and Configuration option in YaST2.

Attribute Name	Description
cluster_dn	Specify the Fully Distinguished Name (FDN) of the cluster in comma-delimited typeful format. Each of the intermediate containers must already exist. The cluster name must be unique in that path. Example: <cluster_dn>cn=clus134,ou=ncs,o=acme</cluster_dn>
cluster_ip	Specify the IP address (in IPv4 format) assigned to the cluster. This is the Master IP Address that provides a single point for cluster access, configuration, and management. The cluster IP address is bound to the master node and remains with the master node regardless of which server is the master. The cluster IP address is required to be on the same IP subnet as the nodes in the cluster. Example: <cluster_ip>192.168.1.1</cluster_ip>

Attribute Name	Description
config_type	Specify whether the node is being configured for a "New Cluster" or an "Existing Cluster". Example: <config_type>Existing Cluster</config_type>
ldap_servers	Specify the IP address (in IPv4 format, comma-delimited with no spaces) of one or more LDAP servers in the tree that you want NCS on this server to use for LDAP (eDirectory) communications. If you specify multiple LDAP servers, the local LDAP server is recommended to be the first IP address in the list. The LDAP servers must have a master replica or a Read/Write replica of eDirectory. Example: <ldap_servers>192.168.1.1,192.168.1.2</ldap_servers>
sbd_dev	If this is the first node in the cluster (that is, you specified a <config_type>New Cluster</config_type>), you typically specify a device to use for the SBD (split-brain detector). The device must already be initialized and marked as Shareable for clustering. Specify the leaf node name of the device, such as sdc. If the <sbd_dev> tag is not used, the SBD is not created. Example: <sbd_dev>sdc</sbd_dev>
sbd_dev2	If this is the first node in the cluster and you are creating an SBD, you can mirror the SBD by specifying a second device to use for the mirror. The device must already be initialized and marked as Shareable for clustering. Specify the leaf node name of the device, such as sdd. Example: <sbd_dev2>sdd</sbd_dev2>
sbd_size	Specify a size in MB to use for the SBD. A single size value applies to the SBD and its mirror (if specified). The size must be at least 8 MB. A minimum size of 20MB is recommended. To use the maximum size (all free space on the device), specify a size of "-1". If you mirror the SBD, the maximum size is limited to the lesser of the free space available on either device. Specify only a value with no units. Example: ◆ For Default size: <sbd_size>8</sbd_size> ◆ For 1024 MB (1 GB): <sbd_size>1024</sbd_size> ◆ For Maximum size: <sbd_size>-1</sbd_size>
server_name	Specify the hostname of the server where you are configuring. Example: NCS.<server_name>avalon</server_name>
start	Specify whether to start NCS automatically after the configuration completes by specifying a start value of "Now". To start the NCS manually, specify "Later". Example: <start>Now</start>

B.6 novell-cifs

Attribute Name	Description
ldap_server	Specify the IP address of the eDirectory LDAP server that AFP connects to at install time. Example: <ldap_server>192.168.1.2</ldap_server>
cifs_ldap_port	Specify the LDAP port of the server specified in the ldap_server tag. Example: <cifs_ldap_port t="integer">636</cifs_ldap_port>
use_secure_port	Set this to 'yes' if the LDAP port is mentioned in cifs_ldap_port tag is a secure port, else no. Example: <use_secure_port>yes</use_secure_port>
create_new_user	Set this value to 'yes' when you want to create a CIFS proxy user at install time. Example: <create_new_user>no</create_new_user>
use_ocs_for_credentials	Set to 'yes' when you want to store the CIFS proxy user credentials in the OCS store. Setting it to 'no' will store the credentials in an encrypted file locally. It is recommended to use OCS to store the CIFS Proxy user credentials. Example: <use_ocs_for_credentials>yes</use_ocs_for_credentials>
server_context	Specify the context of the local NCP server. Example: <server_context>ou=wdc,o=acme</server_context>
cifs_edir_contexts	Specify a list of CIFS User contexts that are searched when the CIFS user enters a user name for authentication. The server searches through each context in the list until it finds the user object. Example: <cifs_edir_contexts t="list"> <listentry>ou=wdc,o=acme</listentry> <listentry>ou=prv,o=acme</listentry> </cifs_edir_contexts>
subtree_search	Set this value to 'yes' when you want to enable the subtree search feature. Example: <subtree_search>no</subtree_search>
usercontext_rights	Set this to 'yes' for CIFS proxy user to grant search rights over user contexts. This is required for subtree search feature. Example: <usercontext_rights>yes</usercontext_rights>

B.7 novell-dhcp

Attribute Name	Description
certificate_authority	Specify the path of the LDAP CA file that contains the CA certificate. Example: <certificate_authority>/etc/opt/novell/certs/ca.pem</certificate_authority>
check_method	Specify what checks to perform on server certificate in a SSL/TLS session. Specify any one of the following options: ◆ Never: The server does not ask the client for a certificate. ◆ Allow: The server requests for a client certificate but if a certificate is not provided or a wrong certificate is provided, the session still proceeds normally. ◆ Try: The server requests for the certificate, if none is provided, the session proceeds normally. If a certificate is provided and it cannot be verified, the session is immediately terminated. ◆ Hard: The server requests for a certificate and a valid certificate must be provided, otherwise the session is immediately terminated. Example: <check_method>never</check_method>
client_certificate	Specify the path of the LDAP CA file that contains the client certificate. Example: <client_certificate>/etc/opt/novell/certs/client.pem</client_certificate>
client_key	Specify the path of the LDAP client key file that contains the key file for the client certificate. Example: <client_key>/etc/opt/novell/certs/cli_key_cert.pem</client_key>
dhcp_ldap_port	Specify the LDAP port of the server specified in the ldap_server tag. Example: <dhcp_ldap_port t="integer">636</dhcp_ldap_port>
group_context	Specify the DNS DHCP group object context. Example: <group_context>ou=OESSystemObjects,dc=sales,dc=wdc,dc=acme,dc=com</group_context>
interfaces	Specify the network interface name. Example: <interfaces>eth0</interfaces>
ldap_debug_file	Specify the path of the DHCP configuration log file. Example: <ldap_debug_file>/var/log/dhcp-ldap-startup.log</ldap_debug_file>

Attribute Name	Description
ldap_method	Specify static or dynamic. • Static, when you do not want the DHCP server to query the LDAP server for host details. • Dynamic, when you want the DHCP server to query for host details front the LDAP server for every request. Example: <ldap_method>static</ldap_method>
ldap_referrals	Set this to 'yes' when you want to enable LDAP referral. Example: <ldap_referrals>yes</ldap_referrals>
ldap_server	Specify the IP address of the LDAP server. Example: <ldap_server>192.168.1.2</ldap_server>
locator_context	Specify the DHCP locator context. Example: <locator_context>ou=OESSystemObjects.dc=sales.dc=wdc.dc=acme.dc=com</locator_context>
server_context	Specify the DHCP server context. Example: <server_context>ou=OESSystemObjects.dc=sales.dc=wdc.dc=acme.dc=com</server_context>
server_object_name	Specify the DHCP server object name. Example: <server_object_name>DHCP_acme-208</server_object_name>
use_secure_port	Set it to 'yes' when you want to use a secure port for communicating with the LDAP server. Example: <use_secure_port>yes</use_secure_port>
use_secure_port_config	Set this to 'yes' when you want to use a secure port for DHCP configuration. Example: <use_secure_port_config>yes</use_secure_port_config>

B.8 novell-dns

Attribute Name	Description
ocs_store	Set this to 'yes' when you want to store the DNS proxy credentials in OCS. Example: <ocs_store>yes</ocs_store>
create_server_object	Set this to 'yes' when you want to create DNS server object. Example: <create_server_object>no</create_server_object>

Attribute Name	Description
domain_name	Specify the DNS domain name. Example: <domain_name>sales.acme.com</domain_name>
group_context	Specify the DNS DHCP group object context. Example: <group_context>ou=OESSystemObjects,dc=sales,dc=wdc,dc=acme,dc=com</group_context>
host_name	Specify the host name of the current server where the installation is being done. Example: <host_name>acme-208</host_name>
ldap_basedn	Specify the LDAP base DN context. Example: <ldap_basedn>o=acme</ldap_basedn>
ldap_server	Specify the IP address of the LDAP server. Example: <ldap_server>192.168.1.2</ldap_server>
locator_context	Specify the DNS locator context. Example: <locator_context>ou=OESSystemObjects.dc=acme.dc=wdc.dc=acme.dc=com</locator_context>
server_context	Specify the DNS server context. Example: <server_context>ou=sales,o=acme</server_context>
use_secure_port	Set this to 'yes' when you want to use a secure port for communicating with the LDAP server. Example: <use_secure_port>yes</use_secure_port>

B.9 novell-lum

Attribute Name	Description
admin_group	Specify the admin group name. The admin group will be created if it does not exist and will be LUM-enabled. The admin user that is used to configure the LUM service will be added to this admin group and this group will be associated with the workstation object. Example: <admin_group>cn=admingroup,o=acme</admin_group>

Attribute Name	Description
alternate_ldap_servers_list1	Specify a list of the IP addresses of the local eDirectory servers that you are connecting to. Example: <alternate_ldap_servers_list1 t="list"/> <listentry>192.168.1.1</listentry> <listentry>192.168.1.2</listentry> </alternate_ldap_servers_list1>
alternate_ldap_servers_list2	Specify one or more external LDAP servers. Ensure to specify the IP address of a valid LDAP server that is up and running. Example: <alternate_ldap_servers_list2 t="list"/> <listentry>192.168.1.3</listentry> <listentry>192.168.1.4</listentry> </alternate_ldap_servers_list2>
ldap_server	Specify the IP address of the LDAP server. Example: <ldap_server>192.168.1.2</ldap_server>
lum_enabled_services	If you want the LUM-enabled users to accees the following services, set the value of those tags to 'yes': FTP, GDM, Gnome Screensaver, Gnomesu pam, Login, SFCB, SSHD and SU. Example: <lum_enabled_services t="map"> <ftp>no</ftp> <gdm>no</gdm> <gnome-screensaver>no</gnome-screensaver> <gnomesu-pam>no</gnomesu-pam> <login>no</login> <sfcb>yes</sfcb> <sshd>no</sshd> <su>no</su> </lum_enabled_services>
partition_root	Specify the context where UNIX Config Object will be created. Example: <partition_root>o=acme</partition_root>

Attribute Name	Description
restrict_access	Set it to 'yes' if you want to restrict read and write access for users other than the owners of the home directories. Example: <restrict_access>yes</restrict_access>
ws_context	Specify the workstation context. Computers running Linux User Management (LUM) are represented by Unix Workstation objects in eDirectory. The object holds the set of properties and information associated with the target computer, such as the target workstation name or a list of eDirectory groups that have access to the target workstation. Example: <ws_context>o=novell</ws_context>

B.10 nss

Attribute Name	Description
ldap_server	Specify the IP address of the LDAP server. Example: <ldap_server>192.168.1.34</ldap_server>
nit_end_range	Specify the UID end range. This value has to be an integer always. Example: <nit_end_range t="integer">200000</nit_end_range>
nit_start_range	Specify the UID start range. This value has to be an integer always. Example: <nit_start_range t="integer">100000</nit_start_range>
nss_edir_context	Specify the NSS eDirectory context. Example: <nss_edir_context>ou=wdc,o=acme</nss_edir_context>
nssadmin_dn	Specify the NSS admin domain context. Example: <nssadmin_dn>cn=wdcsalesinstall34admin.ou=wdc.o=acme</nssadmin_dn>

B.11 oes-ldap

Attribute Name	Description
admin_context	Specify the LDAP Server Administrator context. Example: <admin_context>cn=admin,o=acme</admin_context>
admin_password	Specify the LDAP Server server Administrator password. Example: <admin_password>SAM23#$</admin_password>

Attribute Name	Description
common_proxy_context	Specify the context where common proxy user is created. Example: <common_proxy_context>ou=servers, o=acme</common_proxy_context>
ldap_servers	Specify the details of the list of LDAP servers in a particular tree. ◆ ip_address: Specify the IP address of the LDAP server. ◆ ldap_port: Specify the LDAP non-secure port number. ◆ ldaps_port: Specify the LDAP secure port number. Example: <ldap_servers t="list"> <listentry t="map"> <ip_address>192.168.1.2</ip_address> <ldap_port t="integer">389</ldap_port> <ldaps_port t="integer">636</ldaps_port> </listentry> </ldap_servers>
tree_name	Specify the eDirectory tree name. Example: <tree_name>sales_wdc_acme</tree_name>
use_common_proxy	Set it to 'yes' when you want to use the default common proxy. Example: <use_common_proxy>yes</use_common_proxy>
xad_tree_admin_context	Specify domain tree admin FQDN context. Example: <xad_tree_admin_context></xad_tree_admin_context>
xad_tree_admin_password	Specify domain tree admin password. Example: <xad_tree_admin_password>SAM23#$</xad_tree_admin_password>

B.12 sms

Attribute Name	Description
ldap_server	Specify the IP address of the eDirectory LDAP server that SMS connects to at install time. Example: <ldap_server>192.168.1.2</ldap_server>

B.13 novell-nssad

Attribute Name	Description
ad_context	Specify Active Directory Context. Example: <ad_context>CN=Computers</ad_context>
ad_uid_generate_mode	If you want NIT to generate UIDs specify this to ‘yes’. Example: <ad_uid_generate_mode>no</ad_uid_generate_mode>
admin_name	Specify the Active Directory administrator user name or an equivalent user that can be used for the AD domain join operation. Example: <admin_name>Administrator</admin_name>
admin_password	Specify the administrator password. Example: <admin_password>pa55word</admin_password>
domain_admin_group	Specify the Active Directory domain admin group name. Example: <domain_admin_group>Domain Admins</domain_admin_group>
domain_name	Specify the Active Directory domain name. Example: <domain_name>ACME.COM</domain_name>
nit_end_range	Specify the UID end range. This value has to be an integer always. Example: <nit_end_range t="integer">200000</nit_end_range>
nit_start_range	Specify the UID start range. This value has to be an integer always. Example: <nit_start_range t="integer">100000</nit_start_range>
pre_created_object	If you want to use any pre-created objects, set this to ‘yes’. Example: <pre_created_object>no</pre_created_object>

B.14 oes-umc

Attribute Name	Description
umc_edirapi_port	Specify the port for the eDir API. By default, the eDir API port is 9010. Example: <umc_edirapi_port>9010</umc_edirapi_port>

B.15 oes-database

Attribute Name	Description
oes_db_hostname	Specify the hostname of the DB server. Example: <oes_db_hostname>dbserver.testdomain.com</oes_db_hostname>
oes_db_password	Specify the password of the DB server. Example: <oes_db_password>SAM23#$</oes_db_password>
oes_db_port	Specify the port of the DB server. By default, the database port is 5432. Example: <oes_db_port>5432</oes_db_port>
oes_db_type	Specify the type of the DB. Example: <oes_db_type>local/remote</oes_db_type>
oes_db_username	Specify the username of the DB server. Example: <oes_db_username>dbadm</oes_db_username>
oes_open_db_port	Set this to ‘yes’ to open port in the firewall for DB. Example: <oes_open_db_port>yes</oes_open_db_port>