

Open Enterprise Server 2018

Installation Guide

November 2017

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

Copyright © 2017 Micro Focus. All Rights Reserved.

Contents

About This Guide	9
1 What's New or Changed in the OES Install	11
1.1 What's New (Update 3 - OES 2018 eDirectory 9.1)	11
1.2 What's New (OES 2018)	11
2 Preparing to Install OES 2018	13
2.1 Before You Install	13
2.2 Meeting All Server Software and Hardware Requirements	13
2.2.1 Server Software	13
2.2.2 Server Hardware	14
2.3 NetIQ eDirectory Rights Needed for Installing OES	15
2.3.1 Rights to Install the First OES Server in a Tree	15
2.3.2 Rights to Install the First Three Servers in an eDirectory Tree	15
2.3.3 Rights to Install the First Three Servers in any eDirectory Partition	15
2.4 Installing and Configuring OES as a Subcontainer Administrator	15
2.4.1 Rights Required for Subcontainer Administrators	16
2.4.2 Providing Required Rights to the Subcontainer Administrator for Installing and Managing Samba	18
2.4.3 Starting a New Installation as a Subcontainer Administrator	20
2.4.4 Adding/Configuring OES Services as a Different Administrator	20
2.5 Preparing eDirectory for OES 2018	20
2.5.1 Extending the Schema	20
2.6 Deciding What Patterns to Install	22
2.7 Obtaining OES 2018 Software	31
2.8 Preparing Physical Media for a New Server Installation or an Upgrade	31
2.9 Setting Up a Network Installation Source	31
2.9.1 SUSE Linux as a Network Installation Source Server	32
2.9.2 Windows as a Network Installation Source Server	34
2.10 Install Only One Server at a Time	34
2.11 What's Next	34
3 Installing OES 2018 as a New Installation	35
3.1 Linux Software RAID's Are Not Cluster Aware	35
3.2 Linux Software RAID's	36
3.3 Starting the OES 2018 Installation	36
3.3.1 Installing from Physical Media	36
3.3.2 Installing from a Network Source	37
3.4 Specifying Network Settings	37
3.5 Specifying Customer Center Configuration Settings	38
3.6 Specifying the Add-On Product Installation Information	39
3.7 Specifying System Role	39
3.8 Setting Up Disk Partitions	40
3.8.1 Guidelines	40
3.8.2 NSS on the System Disk	41
3.8.3 Security Flag Recommendations	41
3.8.4 Partitioning X86 Machines	42

3.8.5	Disk Partition Statistics	42
3.8.6	Combining Hard Disk Partitions	43
3.9	Setting Up the Clock and Time Zone	43
3.10	Creating Local User	43
3.11	Specifying the Password for the System Administrator "root"	43
3.12	Specifying the Installation Settings	44
3.12.1	Customizing the Software Selections	44
3.12.2	Configuring the Firewall Settings	46
3.12.3	Setting Systemd Target	48
3.12.4	Accepting the Installation Settings	48
3.13	Configuring Open Enterprise Server	48
3.13.1	Typical Configuration	48
3.13.2	Custom Configuration	49
3.13.3	Specifying eDirectory Configuration Settings	49
3.13.4	Specifying LDAP Configuration Settings	55
3.13.5	Configuring OES Services	55
3.13.6	Configuration Guidelines for OES Services	56
3.14	Finishing the Installation	81
3.15	Verifying That the Installation Was Successful	81
3.16	What's Next	82

4 Installing or Configuring OES Services on an Existing OES 2018 Server 83

4.1	Adding/Configuring OES Services on an Existing Server	83
4.2	Adding/Configuring OES Services on a Server That Another Administrator Installed	85
4.3	What's Next	86

5 Upgrading to OES 2018 87

5.1	Supported Upgrade Paths	87
5.2	Planning for the Upgrade to OES 2018	88
5.2.1	Be Sure to Check the Release Notes	88
5.2.2	Understanding the Implications for Other Products Currently Installed on the Server	88
5.2.3	Upgrading in Text Mode	89
5.3	Meeting the Upgrade Requirements	89
5.3.1	Securing Current Data	89
5.3.2	Ensuring That There Is Adequate Storage Space on the Root Partition	89
5.3.3	Preparing the Server You Are Upgrading	90
5.3.4	Checking the Server's DNS Name	90
5.3.5	Ensuring That the Server Has a Server Certificate	90
5.3.6	Changing the Mount Options Before an Upgrade	91
5.3.7	Preparing an Installation Source	91
5.3.8	Synchronizing the OES Configuration Information before Starting an Upgrade	91
5.3.9	Moving to Common Proxy Users Before an Upgrade	92
5.4	Upgrading to OES 2018	93
5.4.1	Using Physical Media to Upgrade	93
5.4.2	Specifying the Partition to Update	94
5.4.3	Reviewing the Previously Used Repositories	94
5.4.4	Specifying Customer Center Configuration Settings	94
5.4.5	Specifying the Add-On Product Installation Information	96
5.4.6	Verifying and Customizing the Update Options in Installation Settings	96
5.4.7	Accepting the Installation Settings	98
5.4.8	Specifying Configuration Information	98
5.4.9	Finishing the Upgrade	101
5.5	Using AutoYaST for an OES 2018 Upgrade	102
5.5.1	Prerequisites	102
5.5.2	Creating an Answer File to Provide the eDirectory and DSfW Passwords	102

5.5.3	Upgrading an OES 11 SP2, OES 11 SP3, OES 2015, or OES 2015 SP1 Server to OES 2018	104
5.5.4	Upgrading an OES 11 SP2, OES 11 SP3, OES 2015, and OES 2015 SP1 XEN Guest Server to OES 2018	104
5.5.5	Troubleshooting an AutoYaST Upgrade	105
5.6	Verifying That the Upgrade Was Successful	106
5.7	What's Next	107
6	Completing OES Installation or Upgrade Tasks	109
6.1	Determining Which Services Need Additional Configuration	109
6.2	Rebooting the Server after Installing NSS	110
6.3	Restarting Tomcat	110
6.4	Implementing Digital Certificates in an OES Environment	110
6.4.1	Configuring the Digital Certificate	111
6.4.2	Reconfiguring Services after Importing the Certificate	111
7	Installing and Configuring NSS Active Directory Support	113
7.1	Understanding the NSS AD Support	113
7.1.1	NSS Resource Access Until OES 11 SP2	113
7.1.2	NSS Resource Access with OES 2015 or Later	115
7.2	NSS AD Support Matrix	116
7.3	Prerequisites for Installing and Configuring NSS AD	117
7.4	Installing or Upgrading to OES 2018 with NSS AD Support	118
7.4.1	Resolving the AD DNS Name from OES 2018	120
7.4.2	Installing and Configuring NSS AD Support	120
7.4.3	Validating the NSS AD Configuration	120
7.5	About Novell Identity Translator (NIT)	122
8	Updating (Patching) an OES 2018 Server	125
8.1	Overview of Updating (Patching)	125
8.1.1	The Patch Process Briefly Explained	125
8.1.2	Update Options	126
8.2	Preparing the Server for Updating	126
8.3	Registering the Server in the Customer Center	127
8.3.1	Prerequisites	127
8.3.2	Registering the Server in the Customer Center Using the Command Line	128
8.3.3	Registering the Server in the Customer Center Using the GUI	129
8.4	Updating the Server	130
8.4.1	Updating the Server Using the Command Line	131
8.5	GUI Based Patching	133
8.6	Frequently Asked Questions about Updating	133
8.6.1	Do I apply all the patches in the catalogs? How do I know which patches to apply?	133
8.7	Patching From Behind a Proxy Server	133
8.8	Installing the Latest iManager NPMs After Applying OES Patches	134
8.9	Restarting the OES Instance of Tomcat After Applying a Tomcat Update	134
9	Using AutoYaST to Install and Configure Multiple OES Servers	135
9.1	Prerequisites	135
9.2	Setting Up a Control File with OES Components	136
9.2.1	Fixing an Automatically Created Control File	136
9.2.2	Using the AutoInstallation Module to Create the Control File	136
9.3	Setting Up an Installation Source	141

9.4	Cloning an OES Server Post OES Installation and Configuration	141
9.4.1	Generating the autoinst.xml File	141
9.4.2	Using the autoinst.xml to Reinstall an OES Server	142
10	Installing, Upgrading, or Updating OES on a VM	145
10.1	System Requirements	145
10.1.1	VM Host Considerations	145
10.1.2	Novell Storage Services Considerations	146
10.1.3	Setup Instructions	146
10.2	Prerequisites	146
10.3	Preparing the Installation Software	146
10.3.1	Downloading the Installation Software	147
10.3.2	Preparing the Installation Source Files	147
10.4	Installing an OES 2018 VM Guest	147
10.4.1	Specifying Options for Creating an OES 2018 VM Guest	147
10.5	Upgrading an OES VM Guest to OES 2018	149
10.5.1	Before You Start the Upgrade Process	149
10.5.2	Starting the Upgrade	149
10.6	Setting Up an OES 2018 VM Guest to Use Novell Storage Services (NSS)	150
11	Switching to SHA-2 SSL Certificates	151
11.1	Configuring SHA-2 Certificate	151
11.1.1	Prerequisites	151
11.1.2	CA Server	151
11.1.3	Other Servers	151
11.1.4	Servers Running on eDirectory 8.8.7 or OES 11 SP1 or Earlier	152
11.2	Verifying the Certificates with SHA-2 Signature	152
12	Disabling OES 2018 Services	153
13	Reconfiguring eDirectory and OES Services	155
13.1	Cleaning Up the eDirectory Server	155
13.1.1	Before You Clean Up	155
13.1.2	Reconfiguring the Replica Server	156
13.1.3	Reconfiguring the CA Server	156
13.1.4	Cleaning Up eDirectory	156
13.2	Reconfiguring the eDirectory Server through YaST	157
13.3	Reconfiguring OES Services	157
13.3.1	Re-creating eDirectory Objects	158
13.3.2	Services Requiring Reconfiguration	159
13.3.3	Manually Starting Services	160
14	Security Considerations	163
14.1	Access to the Server During an Installation or Upgrade	163
14.2	Remote Installations Through VNC	163
14.3	Improperly Configured LDAP Servers	163
15	Troubleshooting	165
15.1	PID File Unavailable Message	165
15.2	<code>systemctl kill</code> Not Supported	166
15.3	Executing <code>kinit</code> Command Fails in <code>.LOCAL</code> Domain	166

15.4	The OES Service Pattern Icons are not Displayed and OES Patterns are not in the Proper Order	166
15.5	Package Conflict Occurs During the Add-On Install of Novell FTP Pattern	166
15.6	The Health Check Option for CA is not Displayed in iManager	168
15.7	Deleting the Existing eDirectory Objects when Reinstalling the OES Server or Reconfiguring the eDirectory	169
15.8	Problem In Assigning IP Address For autoinst.xml-based Installations	169
15.9	eDirectory Restart Results in an Error Message on a Non-DSfW Server	169
15.10	The DEFAULT SLP Scope Gets added to the slp.conf File During an Upgrade to OES 2018.	170
15.11	The change_proxy_pwd.sh Script Fails to Synchronize Password	170
15.12	OES Installation Fails Due to Encrypted OES Media URL in the autoinst.xml File	171
15.13	Installing or Upgrading to OES 2018 using AutoYaST Creates the OES Repository Name Using Random Characters	171
15.14	Verification of the Container Object Fails During the AD Domain Join Process	171
15.15	Timing Issues for OES on Xen	172
A	OES 2018 File and Data Locations	173
A.1	General Rules	173
A.2	Exceptions	174
B	AutoYaST XML Tags	175
B.1	edirectory	175
B.2	imanager	181
B.3	iprint	181
B.4	ncpserver	181
B.5	ncs	182
B.6	netstorage	183
B.7	novell-afp	184
B.8	novell-cifs	185
B.9	novell-dhcp	186
B.10	novell-dns	187
B.11	novell-lum	189
B.12	novell-samba	190
B.13	nss	192
B.14	oes-cis	192
B.15	oes-ldap	193
B.16	sms	194
B.17	novell-nssad	195
C	Importing New Build Keys to the Keyring	197

About This Guide

This guide describes how to install, upgrade, and update Open Enterprise Server (OES) 2018. 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 the OES Install," on page 11
- ♦ Chapter 2, "Preparing to Install OES 2018," on page 13
- ♦ Chapter 3, "Installing OES 2018 as a New Installation," on page 35
- ♦ Chapter 4, "Installing or Configuring OES Services on an Existing OES 2018 Server," on page 83
- ♦ Chapter 5, "Upgrading to OES 2018," on page 87
- ♦ Chapter 6, "Completing OES Installation or Upgrade Tasks," on page 109
- ♦ Chapter 7, "Installing and Configuring NSS Active Directory Support," on page 113
- ♦ Chapter 8, "Updating (Patching) an OES 2018 Server," on page 125
- ♦ Chapter 9, "Using AutoYaST to Install and Configure Multiple OES Servers," on page 135
- ♦ Chapter 10, "Installing, Upgrading, or Updating OES on a VM," on page 145
- ♦ Chapter 11, "Switching to SHA-2 SSL Certificates," on page 151
- ♦ Chapter 12, "Disabling OES 2018 Services," on page 153
- ♦ Chapter 13, "Reconfiguring eDirectory and OES Services," on page 155
- ♦ Chapter 14, "Security Considerations," on page 163
- ♦ Chapter 15, "Troubleshooting," on page 165
- ♦ Appendix A, "OES 2018 File and Data Locations," on page 173
- ♦ Appendix B, "AutoYaST XML Tags," on page 175
- ♦ Appendix C, "Importing New Build Keys to the Keyring," on page 197

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 the User Comment feature at the bottom of each page of the OES online documentation.

Documentation Updates

The latest version of the *OES 2018: Installation Guide* is available at the [Open Enterprise Server 2018 documentation website](#).

Additional Documentation

For more information about	See
Planning and implementing OES 2018	<i>OES 2018: Planning and Implementation Guide</i>
Migration from and coexistence with other products	“Different Migration Tools” in the <i>OES 2018: Migration Tool Administration Guide</i>
SLES 12 SP2 Deployment details	<i>SUSE LINUX Enterprise Server 12 SP2 Deployment Guide</i> (https://www.suse.com/documentation/sles-12/book_sle_deployment/data/book_sle_deployment.html)
SLES 12 SP2 Administration details	<i>SUSE LINUX Enterprise Server 12 SP2 Administration Guide</i> (https://www.suse.com/documentation/sles-12/book_sle_admin/data/book_sle_admin.html)

1 What's New or Changed in the OES Install

This section describes enhancements or changes to Install for Open Enterprise Server (OES):

1.1 What's New (Update 3 - OES 2018 eDirectory 9.1)

In this patch release on OES 2018, the eDirectory version is upgraded from eDirectory 9.0.3 to eDirectory 9.1 and the iManager version from iManager 3.0.3 to iManager 3.0.4.

If you are applying the patch while upgrading OES from its earlier version to OES 2018, the eDirectory schema is updated automatically.

If you are applying the patch on an existing OES 2018 server, you must manually extend the eDirectory schema by doing the following:

- 1 Install the OES 2018 Update 3 patches.
 - ♦ Update 3 - OES 2018 eDirectory 9.1 - Mandatory
 - ♦ Update 3 - OES 2018 - Recommended
- 2 Reboot the OES server.
- 3 In the terminal console, execute the command `ndsconfig upgrade` to extend the eDirectory schema.

iManager 3.1 is not a part of this patch. To manage eDirectory 9.1 specific features from iManager, you must use the standalone iManager 3.1.

1.2 What's New (OES 2018)

This section describes enhancements to the installation program for Open Enterprise Server (OES) 2018.

OES Install Media

Beginning with OES 2018, OES is installed only through OES Install Media, which is a single integrated install media that includes both SLES and OES.

Traditional OES installation included both add-on install (SLES and OES as separate media) and integrated install media (a single media that includes both SLES and OES). The support for the add-on install is deprecated.

Channel Enhancement

Beginning with OES 2018, a single activation key is used to obtain the OES channels. SLES 12 keys are not required separately. OES includes both SLES and OES update channels.

All OES 2018 channels are available from NCC as earlier.

2 Preparing to Install OES 2018

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

- ♦ [Section 2.1, “Before You Install,” on page 13](#)
- ♦ [Section 2.2, “Meeting All Server Software and Hardware Requirements,” on page 13](#)
- ♦ [Section 2.3, “NetIQ eDirectory Rights Needed for Installing OES,” on page 15](#)
- ♦ [Section 2.4, “Installing and Configuring OES as a Subcontainer Administrator,” on page 15](#)
- ♦ [Section 2.5, “Preparing eDirectory for OES 2018,” on page 20](#)
- ♦ [Section 2.6, “Deciding What Patterns to Install,” on page 22](#)
- ♦ [Section 2.7, “Obtaining OES 2018 Software,” on page 31](#)
- ♦ [Section 2.8, “Preparing Physical Media for a New Server Installation or an Upgrade,” on page 31](#)
- ♦ [Section 2.9, “Setting Up a Network Installation Source,” on page 31](#)
- ♦ [Section 2.10, “Install Only One Server at a Time,” on page 34](#)
- ♦ [Section 2.11, “What’s Next,” on page 34](#)

2.1 Before You Install

Before you install Open Enterprise Server 2018 (OES 2018), review the following information:

- ☐ [“Planning Your OES 2018 Implementation” in the *OES 2018: Planning and Implementation Guide*](#)
- ☐ [OES 2018: Release Notes](#)

2.2 Meeting All Server Software and Hardware Requirements

Before installing OES 2018, ensure that your system meets the following requirements:

- ♦ [Section 2.2.1, “Server Software,” on page 13](#)
- ♦ [Section 2.2.2, “Server Hardware,” on page 14](#)

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, such as Itanium (IA64) and Intel x86(IA32), are not supported for running OES services. NOTE: Services such as SMS and NRM run in 32-bit mode on a 64-bit platform.
Memory	2 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	10 GB of available, unpartitioned disk space	16 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.

Be sure to complete the planning instructions in the [OES 2018: Planning and Implementation Guide](#) for each component that you install.

2.3 NetIQ eDirectory Rights Needed for Installing OES

- [Section 2.3.1, “Rights to Install the First OES Server in a Tree,” on page 15](#)
- [Section 2.3.2, “Rights to Install the First Three Servers in an eDirectory Tree,” on page 15](#)
- [Section 2.3.3, “Rights to Install the First Three Servers in any eDirectory Partition,” on page 15](#)

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 Novell 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 20](#).

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, “NetIQ eDirectory Rights Needed for Installing OES,” on page 15](#) 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 16](#)
- [Section 2.4.2, “Providing Required Rights to the Subcontainer Administrator for Installing and Managing Samba,” on page 18](#)
- [Section 2.4.3, “Starting a New Installation as a Subcontainer Administrator,” on page 20](#)
- [Section 2.4.4, “Adding/Configuring OES Services as a Different Administrator,” on page 20](#)

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	<ol style="list-style-type: none">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	<ol style="list-style-type: none">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	<ol style="list-style-type: none">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 Security container when installing the NMAS login methods	<p>If the subcontainer administrator will install the NMAS login methods:</p> <ol style="list-style-type: none">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.

Rights Needed	Sample Steps to Follow
Create right to its own container (context)	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<p>This is not needed if the Supervisor right was assigned because of NMAS.</p> <p>If the subcontainer administrator won't install the NMAS login methods, do the following:</p> <ol style="list-style-type: none"> 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.
Read right to the NDSPKI:Private Key attribute on the Organizational CA object (located in the Security container)	<ol style="list-style-type: none"> 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. <p>The Read right should be automatically assigned.</p> <ol style="list-style-type: none"> 7. Click Done > OK > OK.
Read and Write rights to the UNIX Config object	<ol style="list-style-type: none"> 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.

Rights Needed	Sample Steps to Follow
Write right to the [All Attribute Rights] property for the admingroup object	<ol style="list-style-type: none"> 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 *OES 2018: DNS/DHCP Services for Linux Administration Guide*.
- ♦ For DHCP, see “[eDirectory Permissions](#)” in the *OES 2018: DNS/DHCP Services for Linux Administration Guide*.

2.4.2 Providing Required Rights to the Subcontainer Administrator for Installing and Managing Samba

Prior to installing any new OES Samba server in a tree, ensure that you provide supervisor rights to the subcontainer administrator for the location mentioned in [Table 2-3](#).

Table 2-3 Subcontainer Administrator Rights Needed to Manage Samba

Rights Needed	Sample Steps to Follow
Supervisor rights to the container where the Linux workstation object will be located	<ol style="list-style-type: none"> 1. In iManager, click View Objects, then browse and select the container where the OES Samba server will be installed. 2. Click Actions > Modify Trustees. 3. On the Modify Trustees page, click Assigned Rights next to the trustee name for which you want to modify rights. 4. Click the desired container admin object to add it to the Selected Objects section. 5. Click OK. 6. Select Property Name rights (All Attribute Rights and Entry Rights) and assign Supervisor rights, then click Done.

Rights Needed	Sample Steps to Follow
Supervisor rights to the container where the Unix config object will be located	<ol style="list-style-type: none"> 1. On the iManager, click View Objects, then in the Tree, browse and select the container where Unix Config object is located. 2. Select the Unix Config object, then click Actions > Modify trustees. 3. On the Modify Trustees page, click Assigned Rights next to the trustee name for which you want to modify rights. 4. Click the desired container admin object to add it to the Selected Objects section. 5. Click OK. 6. Select Property Name rights (All Attribute Rights and Entry Rights) and assign Supervisor rights, then click Done.
Supervisor rights to the container where the Samba/LDAP base context will be located	<ol style="list-style-type: none"> 1. On the iManager, click View Objects, then in the Tree, browse and select the container where the Samba/LDAP base context will reside. 2. Select the Current Level tree object, then click Actions > Modify trustees. 3. On the Modify Trustees page, click Assigned Rights next to the trustee name for which you want to modify rights. 4. Click the desired container admin object to add it to the Selected Objects section. 5. Click OK. 6. Select Property Name rights (All Attribute Rights and Entry Rights) and assign Supervisor rights, then click Done.
Supervisor rights to the container where the Samba proxy user will be installed	<ol style="list-style-type: none"> 1. On the iManager, click View Objects, then in the Tree, browse and select the container where the Samba proxy user context will be installed. 2. Select the Samba proxy object, then click Actions > Modify trustees. 3. On the Modify Trustees page, click Assigned Rights next to the trustee name for which you want to modify rights. 4. Click the desired container admin object to add it to the Selected Objects section. 5. Click OK. 6. Select Property Name rights (All Attribute Rights and Entry Rights) and assign Supervisor rights, then click Done.

2.4.3 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 16
- ♦ The rights described in [“Providing Required Rights to the Subcontainer Administrator for Installing and Managing Samba”](#) on page 18
- ♦ (If applicable) The rights described for the server installations in [“NetIQ eDirectory Rights Needed for Installing OES”](#) on page 15

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.

2.4.4 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 85.

2.5 Preparing eDirectory for OES 2018

- ♦ [Section 2.5.1, “Extending the Schema,”](#) on page 20

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 20
- ♦ [“Which OES Services Require a Schema Extension?”](#) on page 20
- ♦ [“Extending the Schema While Installing OES”](#) on page 21
- ♦ [“Using the YaST Plug-In to Extend the Schema”](#) on page 21
- ♦ [“Extending the Schema for Novell Cluster Services”](#) on page 22

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 21](#)).

- ♦ NetIQ Directory Services*
- ♦ Novell Linux User Management (LUM)*
- ♦ Novell iPrint Services
- ♦ Novell DHCP Services
- ♦ Novell DNS Services
- ♦ Novell NCP Server
- ♦ Novell NetStorage
- ♦ Novell Storage Services (NSS)
- ♦ Novell SMS*
- ♦ Novell Domain Services for Windows
- ♦ NetIQ NMAS*
- ♦ Novell CIFS
- ♦ Novell Clustering
- ♦ Novell Remote Manager
- ♦ Novell Samba
- ♦ 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 16](#).

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 SLES 12 SP2 server, then install OES 2018 without installing any of the services, followed by the `yast2 novell-schema` tool installation.

To run the Novell Schema Tool:

- 1 On the server's desktop, click **Computer** and open the **YaST Control Center**.
- 2 Click **Open Enterprise Server > Novell Schema Tool**.
- 3 Depending on the installation method you used, you might be required to insert your OES 2018 installation media.
- 4 On the NetIQ 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 2018 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 Novell Cluster Services

If you want a subcontainer administrator to install the first instance of Novell Cluster Services in a tree, you can extend the schema by following the instructions in “[Installing, Configuring, and Repairing Novell Cluster Services](#)” in the *OES 2018: Novell 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 2-4 Standard OES Installation Patterns

Pattern	Description
Base System	<p>Consists of all packages that are common to all SUSE Linux Enterprise products. Also provides a Linux Standard Base 3.0 compliant runtime environment.</p> <p>This pattern is selected for installation by default.</p> <p>IMPORTANT: You must either install this pattern or the Common Code Base pattern.</p>
AppArmor	<p>Novell 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 <code>root</code>) 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.</p> <p>This pattern is selected for installation by default.</p>
GNOME Desktop Environment	<p>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.</p> <p>This pattern is selected for installation by default.</p>

Pattern	Description
X Window System	<p>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.</p> <p>This pattern is selected for installation by default.</p>

Table 2-5 OES Services Pattern Descriptions

Pattern	Description
Novell AFP	<p>A Novell AFP server allows Macintosh clients to access data stored on NSS volumes in the same way they access data on a Mac OS X server.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ◆ Novell Backup / Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Storage Services (NSS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) ◆ Novell NCP Server <p>This pattern cannot be installed on the same server as these services:</p> <ul style="list-style-type: none"> ◆ Novell Domain Services for Windows
Novell Backup/Storage Management Services (SMS)	<p>The Novell backup infrastructure (called Storage Management Services or SMS) provides backup applications with the framework to develop a complete backup and restore solution.</p> <p>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.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)

Pattern	Description
Novell CIFS	<p>CIFS (Common Internet File System) is a network sharing protocol. Novell CIFS enables Windows, Linux, and UNIX client workstations to copy, delete, move, save, and open files on an OES 2018 server. CIFS allows read and write access from multiple client systems simultaneously.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ♦ Novell Backup / Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell Storage Services (NSS) ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM) ♦ Novell NCP Server <p>This pattern cannot be installed on the same server as these services:</p> <ul style="list-style-type: none"> ♦ Novell Domain Services for Windows ♦ Novell Samba
Novell Cluster Services (NCS)	<p>Novell 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 NetIQ eDirectory and supports failover, failback, and migration (load balancing) of individually managed cluster resources.</p> <p>Novell 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.</p> <p>Using Novell 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.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM) <p>This pattern cannot be installed on the same server with these services:</p> <ul style="list-style-type: none"> ♦ High Availability

Pattern	Description
Novell DHCP	<p data-bbox="574 218 1414 275">Novell DHCP (Dynamic Host Configuration Protocol) uses eDirectory to provide configuration parameters to client computers and integrate them into a network.</p> <p data-bbox="574 300 1409 384">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 NetIQ eDirectory.</p> <p data-bbox="574 409 1073 432">This pattern selects and installs these services:</p> <ul data-bbox="602 457 1190 617" style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell DNS	<p data-bbox="574 642 1422 699">Novell DNS uses NetIQ eDirectory to deliver information associated with domain names, in particular the IP address.</p> <p data-bbox="574 724 1442 808">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 NetIQ eDirectory.</p> <p data-bbox="574 833 1073 856">This pattern selects and installs these services:</p> <ul data-bbox="602 882 1190 1041" style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)

Pattern	Description
Novell Domain Services for Windows	<p>Novell Domain Services for Windows provides seamless cross-authentication capabilities between Windows/Active Directory and OES 2018 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 Novell-Microsoft environments.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ♦ Novell Backup / Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell DNS ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM) ♦ Novell Storage Services (NSS) ♦ Novell NCP Server <p>This pattern cannot be installed on the same server as these services:</p> <ul style="list-style-type: none"> ♦ Novell Samba ♦ Novell CIFS ♦ Novell AFP ♦ Novell FTP ♦ Novell NetStorage ♦ Novell Pre-Migration Server
NetIQ eDirectory	<p>NetIQ 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.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM) <p>This pattern cannot be installed on the same server as these services:</p> <ul style="list-style-type: none"> ♦ OpenLDAP

Pattern	Description
Novell FTP	<p>Novell FTP (File Transfer Protocol) is integrated with NetIQ eDirectory so that users can securely transfer files to and from OES volumes.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) <p>This pattern cannot be installed on the same server as these services:</p> <ul style="list-style-type: none"> ◆ Novell Domain Services for Windows
Novell iManager	<p>Novell 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.</p> <p>iManager provides the following benefits:</p> <ul style="list-style-type: none"> ◆ Single point of administration for NetIQ 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 <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell iPrint	<p>Novell iPrint lets employees, partners, and customers access printers from a variety of locations across the network and the Internet. From a web browser, users can easily install any printer on the network from any location.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) <p>This pattern cannot be installed on the same server as these services:</p> <ul style="list-style-type: none"> ◆ CUPS
Novell Linux User Management (LUM)	<p>Linux 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.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Remote Manager (NRM)

Pattern	Description
Novell NCP Server / Dynamic Storage Technology	<p>Novell 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.</p> <p>NCP Server includes Novell 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.</p> <p>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.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell NetStorage	<p>Novell NetStorage provides the solution for simple, Internet-based access to file storage. NetStorage is a bridge between a company's protected Novell storage network and the Internet. It lets users access files securely from any Internet location, with nothing to download or install on the user's workstation.</p> <p>With Novell NetStorage, a user can securely access files from any Internet-enabled machine. Users can copy, move, rename, delete, read, write, recover, and set trustee assignments (based on their privilege level) on files between a local workstation and a Novell storage network. Access is available from any Internet-attached workstation, anywhere in the world. There is no need to email or copy data from one machine to another.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ Novell iManager ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM) <p>This pattern cannot be installed on the same server as these services:</p> <ul style="list-style-type: none"> ♦ Novell Domain Services for Windows

Pattern	Description
Novell Pre-migration Server	<p>A Novell Pre-migration Server is not actually a service. Rather, it is a special-purpose server—the target of a Server ID Transfer Migration.</p> <p>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 OES 2018: Migration Tool Administration Guide.</p> <p>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.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ◆ Novell Backup / Storage Management Services (SMS) ◆ NetIQ eDirectory (without a replica) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) <p>This pattern cannot be installed on the same server as these services:</p> <ul style="list-style-type: none"> ◆ Novell Domain Services for Windows
Novell Remote Manager (NRM)	<p>Novell Remote Manager lets you securely access and manage one or more servers from any location through a standard Web browser. You can use Novell Remote Manager to monitor your server's health, change the configuration of your server, or perform diagnostic and debugging tasks.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM)
Novell Samba	<p>Novell Samba provides Windows (CIFS and HTTP-WebDAV) access to files stored on an OES server's file system using an eDirectory user name and password.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) <p>This pattern cannot be installed on the same server as these services:</p> <ul style="list-style-type: none"> ◆ Novell CIFS ◆ Novell Domain Services for Windows

Pattern	Description
Novell Storage Services (NSS)	<p>The Novell 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 Novell Distributed File Services for NSS volumes.</p> <p>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.</p> <p>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.</p> <p>This pattern selects and installs these services:</p> <ul style="list-style-type: none"> ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell NCP Server ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) <p>This pattern cannot be installed on the same server as these services:</p> <ul style="list-style-type: none"> ◆ Xen Virtual Machine Host Server
Novell Storage Service AD Support	<p>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 Novell Storage Services Active Directory (NSS AD) Support.</p> <p>This pattern selects and installs the following services:</p> <ul style="list-style-type: none"> ◆ Novell CIFS ◆ Novell Storage Services (NSS) ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell NCP Server ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) <p>This pattern cannot be installed on the same server as these services:</p> <ul style="list-style-type: none"> ◆ Novell Domain Services for Windows ◆ Novell Samba
Cloud Integrated Storage (CIS)	<p>Cloud Integrated Storage is a hybrid cloud solution that provides a secure gateway to store, manage, and access data across private or public cloud.</p>

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 44](#) and [“Installing or Configuring OES Services on an Existing OES 2018 Server” on page 83](#).

2.7 Obtaining OES 2018 Software

For information on obtaining OES software, see [“Getting and Preparing OES Software” in the *OES 2018: Planning and Implementation Guide*](#).

2.8 Preparing Physical Media for a New Server Installation or an Upgrade

To prepare physical media for an installation or upgrade, you must first download ISO image files and then burn the DVDs that you need for your server. Detailed download instructions are available in [“Getting and Preparing OES Software” in the *OES 2018: Planning and Implementation Guide*](#).

[Table 2-6](#) lists the image files you need.

Table 2-6 Files to Download

Platform	Files needed
64-bit server with DVD drive	<ul style="list-style-type: none">♦ OES ISO (OES2018-DVD-x86_64-DVD1.iso) <p>The ISO file can be downloaded from the OES 2018 download page (http://download.novell.com/index.jsp).</p>

- 1 Download the ISO files you need for your hardware capabilities.
- 2 Ensure that the checksum of the files you have downloaded are the same as those specified on the download page. To get the checksum, use the `md5sum <file name>` command.
- 3 Insert a blank, writable DVD into your DVD burner.
- 4 Select the option to create a DVD from an image file.
- 5 Select **ISO** as the file type.
- 6 Select the first image file (see [Table 2-6](#)) from the location you downloaded it to.
- 7 Complete the DVD creation process.
- 8 Label the disk.
- 9 Repeat this process for each of the ISO image files you downloaded.

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 32](#)
- ♦ [Section 2.9.2, “Windows as a Network Installation Source Server,” on page 34](#)

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”](#) in the *SLES 12 SP2 Deployment Guide*
- ♦ The instructions in the following sections:
 - ♦ [“Requirements”](#) on page 32
 - ♦ [“Procedure”](#) on page 32
 - ♦ [“NFS Protocol Configuration”](#) on page 33
 - ♦ [“FTP Protocol Configuration”](#) on page 33
 - ♦ [“HTTP Protocol Configuration”](#) on page 33

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 *OES 2018: 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 33
- ♦ [“FTP Protocol Configuration”](#) on page 33
- ♦ [“HTTP Protocol Configuration”](#) on page 33

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 *SUSE Linux Enterprise Server 12 SP2 DVD* and label it with that name.

For information on creating this DVD, see [“Preparing Physical Media for a New Server Installation or an Upgrade”](#) on page 31.

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 2018 Installation”](#) on page 36 or [“Upgrading to OES 2018”](#) on page 87.

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 12 SP2.

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 12 SP2 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 2018 as a New Installation” on page 35](#)
- ♦ [“Upgrading to OES 2018” on page 87](#)
- ♦ [“Using AutoYaST to Install and Configure Multiple OES Servers” on page 135](#)
- ♦ [“Installing or Configuring OES Services on an Existing OES 2018 Server” on page 83](#)

3 Installing OES 2018 as a New Installation

The Open Enterprise Server (OES) 2018 is installed using the OES Install Media iso (OES2018-DVD-x86_64-DVD1.iso). This ISO has both OES 2018 and SLES 12 SP2. 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 2018.

For detailed information on performing a SLES installation, see the [SLES 12 SP2 Deployment Guide \(https://www.suse.com/documentation/sles-12/book_sle_deployment/data/book_sle_deployment.html\)](https://www.suse.com/documentation/sles-12/book_sle_deployment/data/book_sle_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 RAID’s Are Not Cluster Aware,” on page 35](#)
- [Section 3.2, “Linux Software RAID’s,” on page 36](#)
- [Section 3.3, “Starting the OES 2018 Installation,” on page 36](#)
- [Section 3.4, “Specifying Network Settings,” on page 37](#)
- [Section 3.5, “Specifying Customer Center Configuration Settings,” on page 38](#)
- [Section 3.6, “Specifying the Add-On Product Installation Information,” on page 39](#)
- [Section 3.7, “Specifying System Role,” on page 39](#)
- [Section 3.8, “Setting Up Disk Partitions,” on page 40](#)
- [Section 3.9, “Setting Up the Clock and Time Zone,” on page 43](#)
- [Section 3.10, “Creating Local User,” on page 43](#)
- [Section 3.11, “Specifying the Password for the System Administrator “root”,” on page 43](#)
- [Section 3.12, “Specifying the Installation Settings,” on page 44](#)
- [Section 3.13, “Configuring Open Enterprise Server,” on page 48](#)
- [Section 3.14, “Finishing the Installation,” on page 81](#)
- [Section 3.15, “Verifying That the Installation Was Successful,” on page 81](#)
- [Section 3.16, “What’s Next,” on page 82](#)

3.1 Linux Software RAID’s Are Not Cluster Aware

Do not use Linux Software RAID’s 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 2018 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 36](#)
 - ♦ [Section 3.3.2, “Installing from a Network Source,” on page 37](#)

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 37.](#)
 - 3b [“Specifying Customer Center Configuration Settings” on page 38](#)
 - 3c [“Specifying the Add-On Product Installation Information” on page 39.](#)
 - 3d [“Specifying System Role” on page 39](#)
 - 3e [“Setting Up Disk Partitions” on page 40](#)
 - 3f [“Setting Up the Clock and Time Zone” on page 43.](#)
 - 3g [“Creating Local User” on page 43](#)
 - 3h [“Specifying the Password for the System Administrator “root”” on page 43](#)

- 3i [“Specifying the Installation Settings” on page 44.](#)
- 3j [“Configuring Open Enterprise Server” on page 48](#)
- 3k [“Finishing the Installation” on page 81.](#)
- 4 Complete the server setup by following the procedures in [“Completing OES Installation or Upgrade Tasks” on page 109.](#)

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 32](#) 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 38](#)
- 7b [“Specifying the Add-On Product Installation Information” on page 39.](#)
- 7c [“Specifying System Role” on page 39](#)
- 7d [“Setting Up Disk Partitions” on page 40](#)
- 7e [“Setting Up the Clock and Time Zone” on page 43.](#)
- 7f [“Creating Local User” on page 43](#)
- 7g [“Specifying the Password for the System Administrator “root”” on page 43](#)
- 7h [“Specifying the Installation Settings” on page 44.](#)
- 7i [“Configuring Open Enterprise Server” on page 48](#)
- 7j [“Finishing the Installation” on page 81.](#)
- 8 Complete the server setup by following the procedures in [“Completing OES Installation or Upgrade Tasks” on page 109.](#)

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.
OES requires a static IP address.
- 3 Click the **Hostname/DNS** tab.
- 4 Specify the **Hostname** associated with the IP address you have or will assign to the server.
- 5 Specify the **Domain Name** for the server.
- 6 In the **Name Servers and Domain Search List**, specify from one to three DNS server IP addresses.
- 7 Click the **Routing** tab.
- 8 Specify the IP address of the default gateway on the subnet where you are installing the OES server.
- 9 Click **Next**.
- 10 Continue with [Section 3.5, "Specifying Customer Center Configuration Settings," on page 38](#).

3.5 Specifying Customer Center Configuration Settings

Registering to Customer Center enables you to receive updates on OES 2018 from Micro Focus, which includes defect fixes.

When you are entering the Customer Center configuration information, it is critical that you enter either your purchased OES 2018 code or the 60-day evaluation code available with your OES 2018 download.

NOTE: Post January 2019, if a new OES 2018 server is installed, the message to import the keys is displayed during the registration of the server to the customer center. For more information, see [Appendix C, "Importing New Build Keys to the Keyring," on page 197](#).

- 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, then click **Next**.

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.

- After you click **Next**, the Contacting server message is displayed.
Wait until this message disappears and the Manual Interaction Required page displays.
- On the Manual Interaction Required page, note the information that you will be required to specify, then click **Continue**.
- 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 2018 (optional)	Specify your purchased or 60-day evaluation registration code for the OES 2018 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.

- 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 screen.
Wait until this message disappears and the Customer Center Configuration page displays.
- Continue with [Section 3.6, "Specifying the Add-On Product Installation Information," on page 39](#).

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 2018. For example, iPrint for OES.

If you do not want to add any add-on products with OES 2018, click **Next** to continue with [Section 3.7, "Specifying System Role," on page 39](#)

3.7 Specifying System Role

Select the system role that meets your requirements best:

Default System

Select this scenario when installing on a "real" machine or a fully virtualized guest.

KVM Virtualization Host

Select this scenario when installing on a machine that should serve as a KVM host that can run other virtual machines.

Xen Virtualization Host

Select this scenario when installing on a machine that should serve as a Xen host that can run other virtual machines.

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.

Beginning with OES 2018, Ext4 is used as default file system because eDirectory 9.0 does not support Btrfs. Changing the default to Btrfs for OES 2018 results in eDirectory configuration failure.

- ♦ [Section 3.8.1, “Guidelines,” on page 40](#)
- ♦ [Section 3.8.2, “NSS on the System Disk,” on page 41](#)
- ♦ [Section 3.8.3, “Security Flag Recommendations,” on page 41](#)
- ♦ [Section 3.8.4, “Partitioning X86 Machines,” on page 42](#)
- ♦ [Section 3.8.5, “Disk Partition Statistics,” on page 42](#)
- ♦ [Section 3.8.6, “Combining Hard Disk Partitions,” on page 43](#)

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 12 SP2 Deployment Guide \(https://www.suse.com/documentation/sles-12/book_sle_deployment/data/book_sle_deployment.html\)](https://www.suse.com/documentation/sles-12/book_sle_deployment/data/book_sle_deployment.html).

Table 3-1 Partition Guidelines

Partition to Create	Other Considerations
<code>/boot</code>	<p>Depending on the hardware, it might be useful to create a boot partition (<code>/boot</code>) to hold the boot mechanism and the Linux kernel.</p> <p>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.</p>
<code>swap</code>	<p>This should normally be twice the size of the RAM installed on your server. If you create a <code>/boot</code> partition, create the <code>swap</code> partition second. Otherwise, create the <code>swap</code> partition first.</p>
<code>/</code>	<p>Define this partition as 3 GB or more. In all cases, create this partition after you create the <code>swap</code> partition. Keep in mind that this root (<code>/</code>) partition contains all of the partitions listed below that you don't specifically create.</p>
<code>/var</code>	<p>This contains system logs and should therefore be a separate partition to avoid impacting system and service stability because of a disk-full condition.</p> <p>Define this partition as 4 GB or more.</p>
<code>/opt</code>	<p>Some (mostly commercial) programs install their data in <code>/opt</code>.</p> <p>Define this partition as 4 GB or more.</p>

Partition to Create	Other Considerations
/usr	<p>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.</p> <p>Define this partition as 4 GB or more.</p>
/srv	<p>This contains the web and FTP servers.</p> <p>Consider making this a separate partition to avoid having someone flood the disk by accident or on purpose, which impacts system and service stability.</p>
/home	<p>User Home directories go here.</p> <p>Consider making this a separate partition to avoid having someone flood the disk by accident or on purpose, which impacts system and service stability.</p> <p>You can allocate the rest of the disk space to this partition.</p>
/tmp	<p>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.</p> <p>Place application-specific files on a separate partition.</p> <p>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.</p>

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)

Mount Point	Mount Options
/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:

<code>df</code>	Displays information about partitions
<code>df -h</code>	Displays information in megabytes or gigabytes as applicable (human readable format)
<code>du</code>	Displays disk usage
<code>du /dirA</code>	Displays the size of each file and directory in dirA
<code>du -sh</code>	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 43](#).

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 Specifying the Password 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.

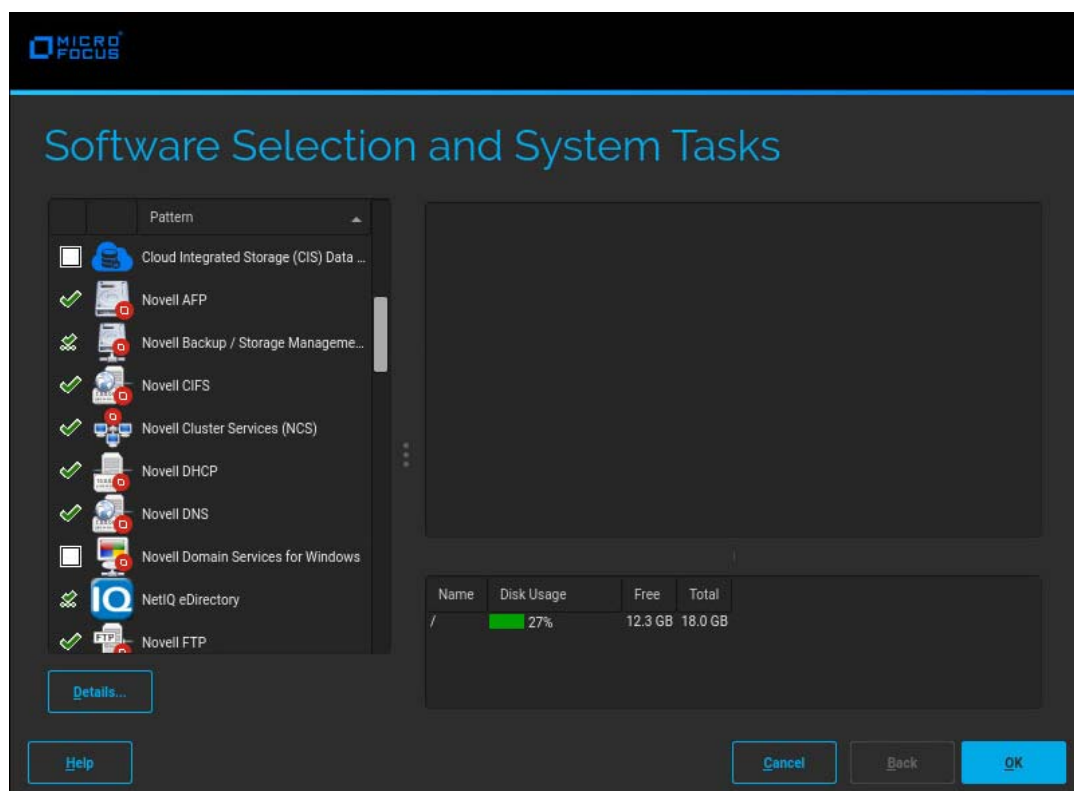
- ♦ [Section 3.12.1, “Customizing the Software Selections,” on page 44](#)
- ♦ [Section 3.12.2, “Configuring the Firewall Settings,” on page 46](#)
- ♦ [Section 3.12.3, “Setting Systemd Target,” on page 48](#)
- ♦ [Section 3.12.4, “Accepting the Installation Settings,” on page 48](#)

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 2018 Server” on page 83](#).

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 2-5 on page 23](#).

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 **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	<ul style="list-style-type: none">♦ 1636 (LDAPS)♦ 1389 (LDAP)♦ 88 (Kerberos TCP and UDP)♦ 135 (RPC Endpoint Manager TCP and UDP)♦ 1024 - 65535 (RPC Dynamic Assignments TCP)♦ 3268 (Global Catalog LDAP TCP)♦ 3269 (Global Catalog LDAP over SSL TCP)♦ 123 (Network Time Protocol UDP)♦ 137 (NetBIOS Name Service TCP and UDP)♦ 138 (NetBIOS Datagram Service TCP and UDP)♦ 139 (NetBIOS Session Service TCP and UDP)♦ 8025 (Domain Service Daemon TCP)♦ 445 (Microsoft-DS traffic TCP and UDP)
NetIQ eDirectory	<ul style="list-style-type: none">♦ 389 (LDAP)♦ 636 (secure LDAP) <p>IMPORTANT: The scripts that manage the common proxy user require port 636 for secure LDAP communications.</p> <ul style="list-style-type: none">♦ 8028 (HTTP for iMonitor)♦ 8030 (secure HTTP for iMonitor)♦ 524 (NCP)
iManager	<ul style="list-style-type: none">♦ 80 (HTTP)♦ 443 (secure HTTP)
iPrint	<ul style="list-style-type: none">♦ 80 (HTTP)♦ 443 (secure HTTP)♦ 631 (IPP)
Novell Identity Translator	<ul style="list-style-type: none">♦ 3268♦ 389
Novell AFP	<ul style="list-style-type: none">♦ 548

Service	Default Ports
Novell CIFS	<ul style="list-style-type: none"> ♦ 139 (Netbios) ♦ 445 (Microsoft-ds)
Cloud Integrated Storage (CIS)	<ul style="list-style-type: none"> ♦ 8343 ♦ 8344 ♦ 636 (LDAP) ♦ 2181 (ZooKeeper) ♦ 3306 (MariaDB) ♦ 9400 (Elasticsearch) ♦ 9092 (Kafka)
Novell Cluster Service	<ul style="list-style-type: none"> ♦ 7023
Novell DHCP	<ul style="list-style-type: none"> ♦ 67
Novell DNS	<ul style="list-style-type: none"> ♦ 953 (secure HTTP) ♦ 53 (TCP) ♦ 53 (UDP)
Novell FTP	<ul style="list-style-type: none"> ♦ 21
Novell Information Portal	<ul style="list-style-type: none"> ♦ 80 (HTTP) ♦ 443 (secure HTTP)
Novell NetWare Core Protocol (NCP)	<ul style="list-style-type: none"> ♦ 524
OES Remote Manager	<ul style="list-style-type: none"> ♦ 8008 (HTTP) ♦ 8009 (secure HTTP)
NURM	<ul style="list-style-type: none"> ♦ 80 ♦ 443
SFCB	<ul style="list-style-type: none"> ♦ 5988 (HTTP) ♦ 5989 (secure HTTP)
Samba	<ul style="list-style-type: none"> ♦ 139 (Netbios) ♦ 445 (Microsoft-ds)
Secure Shell	<ul style="list-style-type: none"> ♦ 22
Storage Management Services (Backup)	<ul style="list-style-type: none"> ♦ 40193 (smdr daemon)
Time Synchronization	<ul style="list-style-type: none"> ♦ 123 (Network Time Protocol UDP)

To adapt the automatic settings to your own preferences:

- 1 On the Installation and Settings page, click **Firewall and SSH**.
- 2 On the Basic Firewall and SSH Configuration page, select the required option and click **OK**.

To disable the firewall:

- 1 On the Installation Settings page, under **Firewall and SSH**, click **disable** on the **Firewall will be enabled** status line.
or
On the Installation Settings page, click **Firewall and SSH**; deselect **Enable Firewall** on the Basic Firewall and SSH 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 48](#).

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 48](#).

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 48](#).

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 49](#), [Section 3.13.4, “Specifying LDAP Configuration Settings,” on page 55](#), [Section 3.13.5, “Configuring OES Services,” on page 55](#), and [Section 3.13.6, “Configuration Guidelines for OES Services,” on page 56](#).

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 49](#)
- ♦ [“Specifying Synchronizing Server Time Options” on page 50](#)
- ♦ [“Creating a New eDirectory Tree and Installing the Server in It” on page 51](#)
- ♦ [“Installing the Server into an Existing eDirectory Tree” on page 51](#)
- ♦ [“Selecting the NetIQ Modular Authentication Services \(NMAS\) Login Method” on page 52](#)
- ♦ [“Specifying OES Common Proxy User Information” on page 53](#)

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.
 - ♦ **DASyncReg:** 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 Scope:** 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 Server** 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 *OES 2018: 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 *OES 2018: 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).

- 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/eDirkey.pem`
- ♦ Certificate file: `/etc/ssl/servercerts/eDircert.pem`

For more information on certificate management, see “[Certificate Management](#)” in the *OES 2018: 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 Micro Focus and 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).

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 *OES 2018: 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:** Selecting this option configures the common proxy user for the following services: CIFS, DNS, DHCP, NetStorage, 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 *OES 2018: 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=novell`. Where `ou` is the organization unit, `acap` is the organization unit name, `o` is the organization, and `novell` 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 `novell`. 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 Name** 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 Micro Focus 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 Micro Focus 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 56](#).
- 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 56](#), or if you are reading online, click a link below:

- ♦ [AFP](#)
- ♦ [Backup/Storage Management Services \(SMS\)](#)
- ♦ [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](#)
- ♦ [NetStorage](#)
- ♦ [Pre-Migration Server](#)
- ♦ [Novell Remote Manager \(NRM\)](#)
- ♦ [Novell Samba](#)
- ♦ [Novell Storage Services](#)
- ♦ [NSS Active Directory Support](#)

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

- 3c** If you want to skip the configuration of a specific component and configure it later, click **Enabled** 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 2018 Server” on page 83](#).

- 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 3.14, “Finishing the Installation,” on page 81](#).

3.13.6 Configuration Guidelines for OES Services

- ♦ [“Service Configuration Caveats” on page 57](#)
- ♦ [“LDAP Configuration for Open Enterprise Services” on page 59](#)
- ♦ [“Novell AFP Services” on page 59](#)
- ♦ [“Novell Backup/Storage Management Services \(SMS\)” on page 60](#)
- ♦ [“Novell CIFS for Linux” on page 60](#)
- ♦ [“Cloud Integrated Storage \(CIS\)” on page 61](#)

- ♦ “Novell Cluster Services” on page 62
- ♦ “Novell DHCP Services” on page 64
- ♦ “Novell DNS Services” on page 66
- ♦ “Novell Domain Services for Windows” on page 68
- ♦ “NetIQ eDirectory Services” on page 68
- ♦ “Novell FTP Services” on page 73
- ♦ “Novell iManager” on page 73
- ♦ “Novell iPrint” on page 74
- ♦ “Novell Linux User Management” on page 74
- ♦ “Novell NCP Server / Dynamic Storage Technology” on page 76
- ♦ “Novell NetStorage” on page 76
- ♦ “Novell Pre-Migration Server” on page 77
- ♦ “Novell Remote Manager” on page 77
- ♦ “Novell Samba” on page 77
- ♦ “Novell Storage Services (NSS)” on page 79
- ♦ “NSS Active Directory Support” on page 80
- ♦ “Deprecated Services:” on page 80

NOTE: Beginning with OES 2015 SP1, Archive and Version Services (AV) and QuickFinder services are not included. Beginning with OES 2018, iFolder service is not included. New installations of OES 2018 will not include patterns to install these components.

If you are upgrading to OES 2018 from an earlier OES server (one that includes these packages), the AV, QuickFinder, and iFolder packages and the associated data will not be accessible on the OES 2018 server. However, the iManager plug-ins for these services are still available in the OES 2018 package, and you can use them to manage servers prior to OES 2018.

Service Configuration Caveats

Keep the following items in mind as you configure the OES 2018:

Table 3-3 *Caveats for Configuring OES Services*

Issue	Guideline
Software Selections When Using Text-Based YaST	<p>Some older machines, such as a Dell 1300, use the text mode install by default when the video card does not meet SLES 12 SP2 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).</p> <p>To view the Software Selection and System Task screen, select Filter > Pattern (or press Alt+F > Alt+I).</p>

Issue	Guideline
Specifying a State identifier for a Locality Class object	<p>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.</p> <p>When using LDAP syntax, use “st” to specify a state. For example:</p> <pre>ou=example_organization,o=example_company,st=utah,c=us</pre> <p>When using NDAP syntax, use “s” to specify a state. For example:</p> <pre>ou=example_organization.o=example_company.s=utah.c=us</pre>
Specifying Typeful Admin Names	<p>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:</p> <pre>cn=admin,ou=example_organization,o=example_company</pre>
Using Dot-Delimited or Comma-Delimited Input for All Products	<p>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.</p> <p>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.</p> <p>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.</p> <p>When using NDAP format (dot), you must escape all embedded dots. For example:</p> <pre>cn=admin.o=novell\provo</pre> <p>When using LDAP format (commas), you must escape all embedded commas. For example: cn=admin,o=novell\,provo</p> <p>The installation disallows a backslash and period (\.) in the CN portion of the admin name.</p> <p>For example, these names are supported:</p> <pre>cn=admin.o=novell cn=admin.o=novell\provo cn=admin.ou=deployment\.linux.o=novell\provo</pre> <p>These names are not supported:</p> <pre>cn=admin\.first.o=novell cn=admin\.root.o=novell</pre> <p>Before LUM-enabling users whose cn contains a period (.), you must remove the backslash (\) from the unique_id field of the User object container.</p> <p>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.</p>

LDAP Configuration for Open Enterprise Services

Table 3-4 LDAP Configuration for Open Enterprise Services Values

Page and Parameters
Configured LDAP Servers
<ul style="list-style-type: none">♦ eDirectory Tree Name: The eDirectory tree name that you specified when configuring eDirectory. The tree that you are installing this server into.
<ul style="list-style-type: none">♦ Admin Name and Context: The eDirectory Admin name you specified when configuring eDirectory.
<ul style="list-style-type: none">♦ Admin Password: The password of the eDirectory Admin user.
<ul style="list-style-type: none">♦ 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 <i>OES 2018: Linux User Management Administration Guide</i>. Default: The eDirectory server you specified when configuring eDirectory.

Novell AFP Services

Table 3-5 Novell Apple Filing Protocol Parameters and Values

Page and Parameters
AFP Configuration - Mac Client Access to NSS Volumes
<ul style="list-style-type: none">♦ Directory Server Address: The IP address of the eDirectory server.♦ Proxy user name with context: Specify the FQDN of the eDirectory containers that contain AFP users, for example ou=afp_users.o=novell. In an existing tree, you can select the context using Browse.

For additional configuration instructions, see [“Installing and Setting Up AFP”](#) in the *OES 2018: Novell AFP for Linux Administration Guide*.

Novell Backup/Storage Management Services (SMS)

Table 3-6 Novell Backup/Storage Management Services Parameters and Values

Page and Parameters
SMS Configuration
<ul style="list-style-type: none">♦ 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.

Novell CIFS for Linux

Table 3-7 Novell CIFS Parameters and Values

Page and Parameters
Novell CIFS Service Configuration
<ul style="list-style-type: none">♦ eDirectory server address or host name: Leave the default or select from the drop-down list to change to a different server.
<ul style="list-style-type: none">♦ LDAP port for CIFS Server: Displays the port value.
<ul style="list-style-type: none">♦ Local NCP Server context: Displays the NCP Server context.
<ul style="list-style-type: none">♦ CIFS Proxy User<ul style="list-style-type: none">♦ Use existing user as CIFS Proxy User: Select this option to use an existing proxy user for the CIFS service. If you specified the server’s common proxy user, this option is selected.♦ Create a new CIFS Proxy User: Select this option to create a new proxy user for the CIFS service.♦ CIFS Proxy User Name: Specify the FQDN (fully qualified distinguished name) of the CIFS proxy user. For example: cn=user, o=novell 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.♦ CIFS Proxy User Password: Specify a password for the CIFS proxy user to use when authenticating to the CIFS server, and verify the password if you are specifying an existing proxy user. For more information on proxy user and password management, see “Planning Your Proxy Users” in the <i>OES 2018: Planning and Implementation Guide</i>.

Page and Parameters

- ♦ **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 2018: Novell CIFS for Linux Administration Guide* and the *OES 2018: Novell AFP for Linux Administration Guide*

Cloud Integrated Storage (CIS)

Table 3-8 Cloud Integrated Storage Services Parameters and Values

Page and Parameters

Cloud Integrated Storage Configuration

- ♦ **ZooKeeper URI:** Specify ZooKeeper URI in the format IP:port or Hostname:Port.

Default: Port 2181

Cloud Integrated Storage Configuration (2)

- ♦ **Directory Server URI:** Specify LDAP URI of an eDirectory server that communicates with the CIS server in the format IP:port or Hostname:Port.

Default: Port 636

- ♦ **CIS admin name with context:** Specify the LDAP distinguished name (DN) of the user who can administer the CIS server.

- ♦ **Admin Password:** Specify the password for the CIS administrator.

- ♦ **Server Certificate file path:** Specify the server certificate file path issued by the eDirectory CA.

Default: `/etc/ssl/servercerts/servercert.pem`

- ♦ **Server Key file path:** Specify the server key file path associated with the server certificate.

Default: `/etc/ssl/servercerts/serverkey.pem`

- ♦ **CA Certificate file path:** Specify the eDirectory CA file path in the format .pem..

Default: `/etc/opt/novell/certs/SSCert.pem`

- ♦ **Server Context:** Specify the LDAP distinguished name (DN) of the container object under which the NCP server objects of the OES server reside that can connect to the CIS server.

- ♦ **Gateway Server Address:** Specify the local host IP address where CIS server is configured.

- ♦ **Cluster Enable:** Allows the CIS server to be part of a cluster resource.

Default: disabled

Cloud Integrated Storage Configuration (3)

Page and Parameters

- ♦ **Database URI:** Specify the MariaDB URI in the format IP:port or Hostname:Port.
Default: Port 3306
 - ♦ **Database User Name and Database Password:** Specify the MariaDB user name and password.
 - ♦ **Elasticsearch URI:** Specify the Elasticsearch URI in the format IP:port or Hostname:Port.
Default: Port 9400
 - ♦ **Use Secure Mode:** Enables or disables secure communication.
Default: enabled
 - ♦ **Server Key file path:** Specify the server key file path associated with the server certificate.
Default: `/etc/ssl/servercerts/serverkey.pem`
 - ♦ **Kafka URI:** Specify the Kafka URI in the format IP:port or Hostname:Port.
Default: Port 9092
-

For additional configuration instructions, see “[Installing and Setting Up Cloud Integrated Storage](#)” in the [OES 2018: CIS Administration Guide](#).

Novell Cluster Services

Table 3-9 *Novell Cluster Services Parameters and Values*

Page and Parameters

Before you configure a node for a Novell Cluster Services cluster, ensure that you have satisfied the prerequisites and have the necessary Administration rights described in “[Planning for Novell Cluster Services](#)” in the [OES 2018: Novell Cluster Services for Linux Administration Guide](#).

Novell Cluster Services (NCS) Configuration

- ♦ **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 2018: Novell Cluster Services for Linux Administration Guide](#).

Page and Parameters

Before you configure a node for a Novell Cluster Services cluster, ensure that you have satisfied the prerequisites and have the necessary Administration rights described in “[Planning for Novell Cluster Services](#)” in the *OES 2018: Novell 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.

- ◆ **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

- ◆ **Optional Device for Mirrored Partitions:** 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 Novell Cluster Services.

Default: none

- ◆ **Desired Partition Size of the Shared Media:** 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

Novell Cluster Services (NCS) Proxy User Configuration (2)

Specify one of the following users as the NCS Proxy user.

- ◆ **OES Common Proxy User:** If the OES common proxy User is enabled in eDirectory, the **Use OES Common Proxy User** check box is automatically selected and the **NCS Proxy User Name** and **Specify NCS Proxy User Password** fields are populated with the credentials of the OES common proxy User.
 - ◆ **LDAP Admin User:** If the OES common proxy User is disabled in eDirectory, the **Use OES Common Proxy User** check box is automatically deselected and the **NCS Proxy User Name** and **Specify NCS Proxy User Password** fields are populated with the credentials of the LDAP Admin user. The fields are also automatically populated with the LDAP Admin credentials if you deselect the **Use OES Common Proxy User** check box.
 - ◆ **Another Administrator User:** Deselect the **Use OES Common Proxy User** check box, then specify the credentials of an administrator user.
-

Page and Parameters

Before you configure a node for a Novell Cluster Services cluster, ensure that you have satisfied the prerequisites and have the necessary Administration rights described in “[Planning for Novell Cluster Services](#)” in the *OES 2018: Novell Cluster Services for Linux Administration Guide*.

Novell 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 2018: Novell Cluster Services for Linux Administration Guide*.

Novell DHCP Services

Table 3-10 Novell 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

- ♦ **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

Page and Parameters

- ♦ **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

Novell 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.

- ♦ **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

- ♦ **LDAP User Name with Context:** Specify a distinguished name and context for an LDAP user. For example: `cn=joe, o=novell`. This user should be an eDirectory user that can access the DHCP server.

During eDirectory configuration, if you have selected the **Use Common Proxy User as default for OES Products** check box, then the proxy user and password fields are populated with common proxy user name and password.

Default: `cn=OESCommonProxy_host name, o=novell`

- ♦ **LDAP User Password:** Type a password for the LDAP user.
-

Page and Parameters

- ♦ **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.
-

Novell DHCP Services Interface Selection

- ♦ **Network Boards for the Novell 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 [OES 2018: DNS/DHCP Services for Linux Administration Guide](#).

Novell DNS Services

Table 3-11 Novell DNS Services Parameters and Values

Page and Parameters

Novell 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:** Specify the FDN of the DNS proxy user.

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.

Default: If you specified a common proxy user, it is used by default. If you didn't specify a common proxy user, the eDirectory Admin name and context that you specified when configuring eDirectory is specified.

- ♦ **Specify Password for Proxy User:** Specify the password for the DNS proxy user.

For more information on proxy user and password management, see "[Planning Your Proxy Users](#)" in the *OES 2018: Planning and Implementation Guide*.

Default: The password that you specified for the OES server you are installing.

- ♦ **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.

- ♦ **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 Novell 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.

- ♦ **Novell 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.

- ♦ **Novell 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.

- ♦ **Novell 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 *OES 2018: DNS/DHCP Services for Linux Administration Guide*.

Novell Domain Services for Windows

There are multiple configuration scenarios, depending on your deployment. For information, see “[Installing Domain Services for Windows](#)” in the *OES 2018: Domain Services for Windows Administration Guide*.

NetIQ eDirectory Services

IMPORTANT: You specified the eDirectory configuration for this server in either “[Specifying LDAP Configuration Settings](#)” on page 55 or “[Specifying eDirectory Configuration Settings](#)” on page 49, 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 Micro Focus 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 3-12 *NetIQ 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 \(https://www.netiq.com/documentation/edirectory-9/edir_admin/data/a2iie1.html\)](https://www.netiq.com/documentation/edirectory-9/edir_admin/data/a2iie1.html)” in the *NetIQ eDirectory 9.0 Administration Guide (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html)*.

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 *OES 2018: 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

♦ **IP Address 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.

Page and Parameters

- ♦ **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.
-

- ♦ **Enter 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 *OES 2018: 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.
 - ♦ **DASyncReg:** 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:** Selecting this option configures the specified common proxy user for the following services: CIFS, DNS, DHCP, NetStorage, and NCS. Optionally, you can specify that LUM use it.

- ♦ **OES Common Proxy User Name:** By default, the common proxy user's name is `OESCommonProxy_hostname`, but you can specify any name that fits your naming methodology. 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:** You can accept the default system-generated password or specify a new password for the common proxy user.
- ♦ **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. 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](#).

Novell FTP Services

No additional configuration is required.

Novell iManager

Table 3-13 *Novell 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.

For additional configuration instructions, see “[Installing iManager Server and Workstation](#)” in the [NetIQ iManager Installation Guide](#).

Novell iPrint

Table 3-14 Novell iPrint Parameters and Values

Page and Parameters
iPrint Configuration
<ul style="list-style-type: none">♦ 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.
<ul style="list-style-type: none">♦ Top-Most Container of eDirectory Tree: iPrint 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 software, iPrint attempts to identify the topmost container of the eDirectory tree and sets the base dn to this container for the AuthLDAPURL entry in <code>/etc/opt/novell/iprint/httpd/conf/iprint_ssl.conf</code>. 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 additional configuration instructions, see “[Installing and Setting Up iPrint on Your Server](#)” in the [OES 2018: iPrint Administration Guide](#).

Novell Linux User Management

Table 3-15 Novell Linux User Management Parameters and Values

Page and Parameters
Linux User Management Configuration
<ul style="list-style-type: none">♦ 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 OES 2018: Linux User Management Administration Guide. Default: The first server selected in the LDAP Configuration list of servers

Page and Parameters

- ♦ **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 Name with Context (Optional):** If you specified a common proxy user, and you select the **Use OES Common Proxy User** option (below) it is used by default. If you didn't specify a common proxy user, you can specify a user (existing or created here) with rights to search the LDAP tree for LUM objects.
-

- ♦ **Proxy User Password:** If you are using the common proxy user, the password is automatically entered for you. Otherwise, you can specify a password (existing or created here) for the Proxy user.

For more information on proxy user and password management, see "[Planning Your Proxy Users](#)" in the *OES 2018: Planning and Implementation Guide*.

- ♦ **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 *OES 2018: Planning and Implementation Guide*.

- ♦ **Services to LUM-enable for authentication via eDirectory:** 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

If you want to use the SSH protocol to define a NetStorage storage location object, you must select SSHD as a LUM-enabled service.

If you do not select **SSHD**, users cannot to log in to NetStorage through SSH to access their files.
 - ♦ **su:** no
 - ♦ **sfcdb:** **yes**

This is selected by default because it is used by many of the OES services such as NSS, SMS, Novell Remote Manager, and Samba. 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 *OES 2018: Linux User Management Administration Guide*.

Novell NCP Server / Dynamic Storage Technology

Table 3-16 Novell 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 *OES 2018: NCP Server for Linux Administration Guide*.

Novell NetStorage

Table 3-17 Novell NetStorage Parameters and Values

Page and Parameters

NetStorage Configuration

Page and Parameters

- ♦ **Authentication Domain Host:** 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 page.

Default: The first server selected in the [LDAP Configuration](#) list of servers.

- ♦ **Proxy User Name with Context:** Specify the proxy user name including the context, or accept the default.

This user performs LDAP searches for users logging into NetStorage.

Default: If you specified a common proxy user, it is used by default. If you didn't specify a common proxy user, the eDirectory Admin name and context that you specified when configuring eDirectory is specified.

- ♦ **Proxy User Password:** Specify a password for the proxy user.

For more information on proxy user and password management, see ["Planning Your Proxy Users"](#) in the [OES 2018: Planning and Implementation Guide](#).

- ♦ **User Context:** Specify the NetStorage user context, or accept the default.

This is the eDirectory context for the users that will use NetStorage. NetStorage searches the eDirectory tree down from the specified context for User objects. If you want NetStorage to search the entire eDirectory tree, specify the root context.

Default: The Organization object you specified while configuring eDirectory

For additional configuration instructions, see ["Installing NetStorage"](#) in the [OES 2018: NetStorage Administration Guide for Linux](#).

Novell Pre-Migration Server

No additional configuration is required. For information, see ["Preparing the Source Server for Migration"](#) in the [OES 2018: Migration Tool Administration Guide](#).

Novell 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 2018: OES Remote Manager Administration Guide](#).

Novell Samba

Table 3-18 Novell Samba Parameters and Values

Page and Parameters

Novell Samba 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.

This is the primary IP address of the LDAP server to which CIFS client users (such as Windows users) authenticate, to use LDAP for access to the directories and files on this OES server.

Default The first server selected in the **LDAP Configuration** list of servers.

- ♦ **Base Context for Samba Users:** The eDirectory context (existing or created here) where the default Samba group is created.

Default: The eDirectory context where the server is installed. Do not change the default unless you are altering the standard Samba configuration.

- ♦ **Proxy User Name with Context:** A user on the specified LDAP server that has rights to search the LDAP tree for Samba users.

The name and context must be specified by using typeful syntax.
(cn=name,ou=organizational_unit,o=organization)

Default: The eDirectory context where the server is installed.

- ♦ **Proxy User Password:** The password of the Proxy User specified above.

For more information on proxy user and password management, see “[Planning Your Proxy Users](#)” in the *OES 2018: Planning and Implementation Guide*.

For additional configuration instructions, see “[Installing the Novell Samba Components](#)” in the *OES 2018: Novell Samba Administration Guide*.

Novell Storage Services (NSS)

Table 3-19 Novell Storage Services Parameters and Values

Page and Parameters
NSS Unique Admin Object
<ul style="list-style-type: none">◆ 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.
<ul style="list-style-type: none">◆ 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 <i>OES 2018: Planning and Implementation Guide</i>. Default: The server hostname concatenated with the LDAP Admin Name you entered for this server,. cn=myserveradmin,o=organization.

For additional configuration instructions, see “[Installing and Configuring Novell Storage Services](#)” in the *OES 2018: NSS File System Administration Guide for Linux*.

NSS Active Directory Support

Table 3-20 NSS Active Directory Support Parameters and Values

Page and Parameters
<ul style="list-style-type: none">♦ 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 <code>msDs-supportedEncryptionTypes</code> 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 <code>CN=Computers</code>. 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 Section 7.5, “About Novell Identity Translator (NIT),” on page 122. 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 113](#).

Deprecated Services:

Beginning with OES 2018, iFolder is not available. Beginning with OES 2015, Archive and Version Services (AV) and QuickFinder services are not included. New installations of OES 2018 will not include patterns to install these components. If you are upgrading to OES 2018 from an earlier OES server (one that includes these packages), the AV, QuickFinder, and iFolder packages and the associated data will not be accessible on the OES 2018 server.

However, the iManager plug-ins for these services are still available in the OES 2018 package but not installed by default. You can install these plug-ins from iManager to manage servers prior to OES 2018.

1. In iManager, select **Configure > Plug-in Installation > Available Novell Plug-in Modules**.
2. Select the plug-ins.
3. Click **Install** to install the selected plug-ins.
4. Restart tomcat for the changes to take effect.

```
rcnovell-tomcat restart
```

Or

```
systemctl restart novell-tomcat.service
```


3.14 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 135](#).

- 2 Finish the installation by clicking **Finish** in the Installation Completed page.
- 3 Continue with [Section 3.15, “Verifying That the Installation Was Successful,” on page 81](#).

3.15 Verifying That the Installation Was Successful

One way to verify that your OES server installation was successful and that 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 component is loading properly.

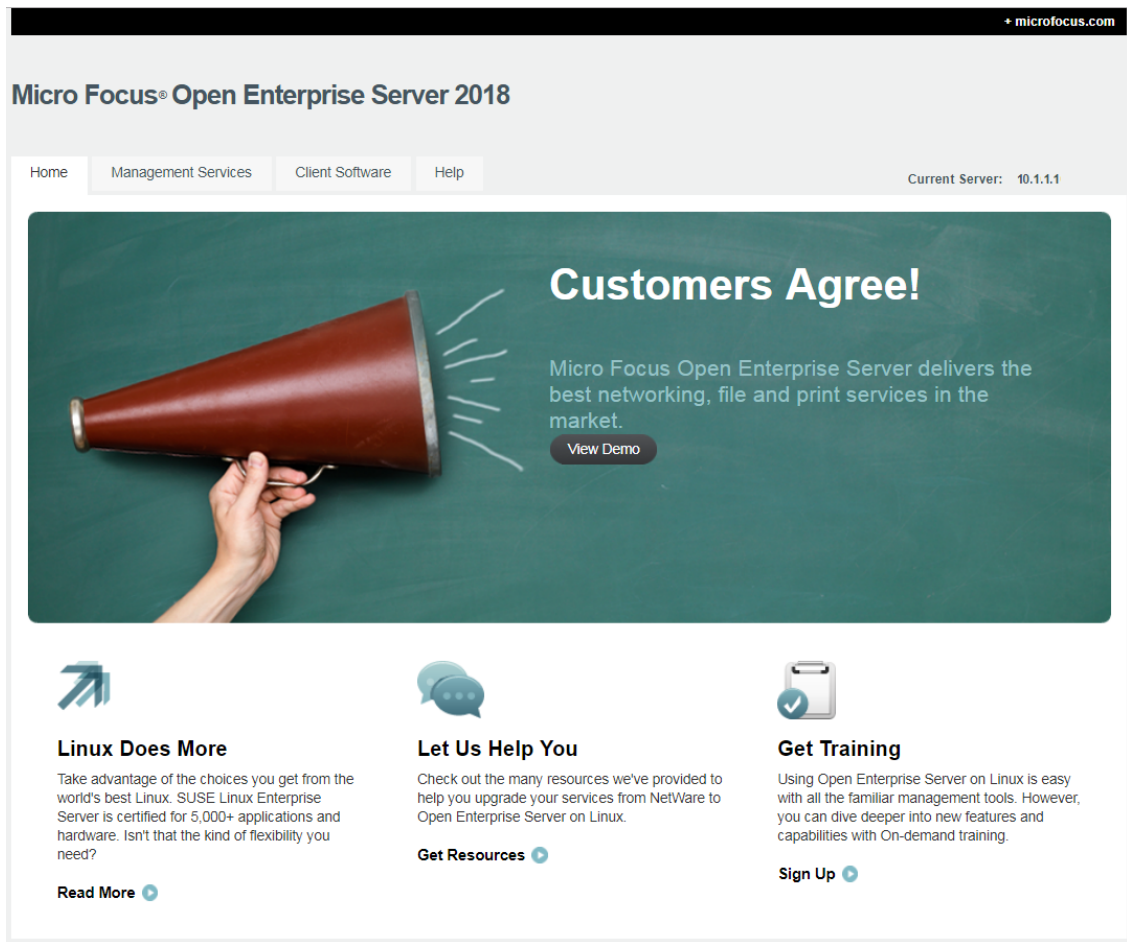
You can also quickly verify a successful installation by accessing the server from your web browser.

- 1 In the Address field of your web browser, enter the following URL:

`http://IP_or_DNS`

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

You should see a web page similar to the following:



- 2 (Optional) If you want to look at the eDirectory tree and begin to see how iManager works, go to the OES Information and Management web page, click **Management Tools** > **iManager**, then log in as user Admin (the user you created during product installation).

You can also access iManager by typing the following URL in a browser window and logging in as user Admin:

`http://IP_or_DNS_name/nps.html`

- 3 Continue with **"What's Next"** on page 82.

3.16 What's Next

After you complete the initial installation, complete any additional tasks you might need to perform. See **"Completing OES Installation or Upgrade Tasks"** on page 109.

4 Installing or Configuring OES Services on an Existing OES 2018 Server

After installing or upgrading to Open Enterprise Server (OES 2018), you can also install additional services and configure them.

- ♦ [Section 4.1, “Adding/Configuring OES Services on an Existing Server,” on page 83](#)
- ♦ [Section 4.2, “Adding/Configuring OES Services on a Server That Another Administrator Installed,” on page 85](#)
- ♦ [Section 4.3, “What’s Next,” on page 86](#)

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 15](#) and then follow the instructions in [Section 4.2, “Adding/Configuring OES Services on a Server That Another Administrator Installed,” on page 85](#).

To add/configure OES services on an existing OES 2018 server:

- 1 Open YaST.
- 2 If an OES installation source has not been added to the server, continue with this step. Otherwise, skip to [Step 3](#).
 - 2a Under **Software**, click **Software Repositories**.
 - 2b Click **Add**.
 - 2c In the Add-On Product Media dialog box, click **DVD > Next**.

If you are using an alternate installation source, click the appropriate option that matches your installation source selection.
 - 2d In the Insert the Add-On Product DVD dialog box, select the appropriate drive where you want to insert the DVD labeled *Novell Open Enterprise Server 2018 DVD 1*.
 - 2e Click **Eject**.
 - 2f Insert the DVD labeled *Novell Open Enterprise Server 2018*, then click **Continue**.
 - 2g Read and accept the Novell Open Enterprise Server 2018 license agreement, then click **Next**.
 - 2h Confirm that the Add-On Product Installation page shows the correct path to the OES media, then click **Next**.
 - 2i Skip to [Step 4](#).

- 3 If an OES installation source has already been added to the server, under **Open Enterprise Server**, click **OES Install and Configuration**.
- 4 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.

NOTE: If you select the Novell FTP pattern, a package conflict warning message is displayed. For more information, see [Section 15.5, “Package Conflict Occurs During the Add-On Install of Novell FTP Pattern,” on page 166](#).

IMPORTANT: You cannot uninstall an OES service by deselecting it. For more information about removing service functionality from the server, see [Chapter 12, “Disabling OES 2018 Services,” on page 153](#).

- 5 If you are only configuring or reconfiguring services that are already installed, click **Accept**, then skip to [Step 9](#).

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 13, “Reconfiguring eDirectory and OES Services,” on page 155](#) and follow the instructions there.

- 6 After selecting the services to install, click **Accept**.
- 7 If package changes are required for your selections, select **Continue**.
- 8 Insert any media required to install the new packages.
- 9 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.

- 9a 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`.

- 9b To enable the configuration status of any disabled service configuration, click the **Disabled** link to change the status to **Enabled**.

- 9c 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 56 or click a link below:

- ♦ [AFP](#)
- ♦ [Backup/Storage Management Services \(SMS\)](#)
- ♦ [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](#)
- ♦ [NetStorage](#)
- ♦ [Pre-Migration Server](#)
- ♦ [Novell Remote Manager \(NRM\)](#)
- ♦ [Novell Samba](#)
- ♦ [Novell Storage Services](#)
- ♦ [Novell Storage Services AD Support](#)

- 10 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.
- 11 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 16.

- 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 Micro Focus 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 9 on page 84](#) in [Section 4.1, "Adding/Configuring OES Services on an Existing Server," on page 83](#) 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 or Upgrade Tasks" on page 109](#).

5 Upgrading to OES 2018

Open Enterprise Server (OES) 2018 provides the option of updating an existing system to the new version without completely reinstalling it. No new installation is needed. Existing data such as home directories and system configuration is kept intact. During the life cycle of the product, you can apply Service Packs to increase system security and correct software defects.

- ♦ [Section 5.1, “Supported Upgrade Paths,” on page 87](#)
- ♦ [Section 5.2, “Planning for the Upgrade to OES 2018,” on page 88](#)
- ♦ [Section 5.3, “Meeting the Upgrade Requirements,” on page 89](#)
- ♦ [Section 5.4, “Upgrading to OES 2018,” on page 93](#)
- ♦ [Section 5.5, “Using AutoYaST for an OES 2018 Upgrade,” on page 102](#)
- ♦ [Section 5.6, “Verifying That the Upgrade Was Successful,” on page 106](#)
- ♦ [Section 5.7, “What’s Next,” on page 107](#)

5.1 Supported Upgrade Paths

[Table 5-1](#) outlines the supported paths for upgrading to OES 2018.

Table 5-1 *Supported OES 2018 Upgrade Paths*

Source Version	Patch Version	Destination	Upgrade Methods Supported
OES 2015 SP1 (64-bit)	Latest patch	OES 2018 (64-bit)	AutoYaST Physical media
OES 2015 (64-bit)	July 2017 Update - OES 2015	OES 2018 (64-bit)	AutoYaST Physical media
OES 11 SP3 (64-bit)	July 2017 OES 11 SP3	OES 2018 (64-bit)	AutoYaST Physical media
OES 11 SP2 (64-bit)	July 2017 OES 11 SP2	OES 2018 (64-bit)	AutoYaST Physical media

Other OES releases can be upgraded by installing the interim OES version. For example, to upgrade from OES 2 SP3 to OES 2018, upgrade to OES 11 SP3 or OES 2015 SP1 first and then upgrade from OES 11 SP3 or OES 2015 SP1 to OES 2018.

NOTE: Post January 2019, if OES is upgraded to OES 2018, the message to import the keys might be displayed during the registration of the server to the customer center. For more information, see [Appendix C, “Importing New Build Keys to the Keyring,” on page 197](#).

5.2 Planning for the Upgrade to OES 2018

- ♦ [Section 5.2.1, “Be Sure to Check the Release Notes,” on page 88](#)
- ♦ [Section 5.2.2, “Understanding the Implications for Other Products Currently Installed on the Server,” on page 88](#)
- ♦ [Section 5.2.3, “Upgrading in Text Mode,” on page 89](#)

5.2.1 Be Sure to Check the Release Notes

The [OES 2018: Release Notes](#) documents issues that Micro Focus 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” on page 88](#)

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

During the upgrade process from OES 11 SP2 and later releases to OES 2018, packages that are not part of the OES 2018 distributions are automatically retained unless you select them for deletion.

This includes third-party products you have installed, as well as other Micro Focus 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.

For Information About This Micro Focus Product	See This Documentation
GroupWise	GroupWise online documentation (http://www.novell.com/documentation/groupwise.html)
ZENworks	ZENworks online documentation (https://www.novell.com/documentation/zenworks11/)
Identity Manager	Identity Management online documentation (https://www.netiq.com/documentation/)
Other products	All Novell online documentation (http://www.novell.com/documentation/)

If you have installed a third-party product, ensure that it is supported on OES 2018 and follow the upgrade instructions that should be included with it.

5.2.3 Upgrading in Text Mode

If you plan to upgrade your OES server to OES 2018 in text mode, before starting the upgrade process, you must change the default runlevel to runlevel 3 in the `/etc/inittab` file. If you fail to do this, you might not be able to continue the upgrade process and complete it at later stages.

5.3 Meeting the Upgrade Requirements

Meet the following requirements before you upgrade and install any OES 2018 components:

- [Section 5.3.1, “Securing Current Data,” on page 89](#)
- [Section 5.3.2, “Ensuring That There Is Adequate Storage Space on the Root Partition,” on page 89](#)
- [Section 5.3.3, “Preparing the Server You Are Upgrading,” on page 90](#)
- [Section 5.3.4, “Checking the Server’s DNS Name,” on page 90](#)
- [Section 5.3.5, “Ensuring That the Server Has a Server Certificate,” on page 90](#)
- [Section 5.3.6, “Changing the Mount Options Before an Upgrade,” on page 91](#)
- [Section 5.3.7, “Preparing an Installation Source,” on page 91](#)
- [Section 5.3.8, “Synchronizing the OES Configuration Information before Starting an Upgrade,” on page 91](#)
- [Section 5.3.9, “Moving to Common Proxy Users Before an Upgrade,” on page 92](#)

5.3.1 Securing Current Data

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

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

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

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

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

For example, if you consider to include all the patterns available before upgrading, you would require approximately 7.5 GB of storage space on the root partition.

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

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

5.3.3 Preparing the Server You Are Upgrading

Ensure that the server meets the hardware requirements for OES 2018. See [Section 2.2.2, “Server Hardware,”](#) on page 14.

Itanium is not a supported platform for OES 2018.

Complete the steps in [Table 5-2](#) for your target server.

Table 5-2 *Preparing the Server You Are Upgrading*

If the Server Is Running	Do This Before Upgrading the Server
OES 2015 SP1	1. Run YaST > Software > Online Update to patch the OES source server to the latest patch level.
OES 2015	2. Ensure that the server and services are still running as desired.
OES 11 SP3	3. Upgrade to OES 2018 using the instructions in this section, then apply all patches and verify services.
OES 11 SP2	

5.3.4 Checking the Server’s DNS Name

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

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

5.3.5 Ensuring That the Server Has a Server Certificate

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

These instructions only apply when that is not the case.

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

To check for or add a certificate:

- 1 Launch YaST.
- 2 Click **Security and Users > CA Management**.
- 3 If no certificate authorities (CAs) are listed, create one by clicking **Create Root CA**.
If a CA is listed, you can use it by selecting the CA and clicking **Enter CA**.
- 4 If you are using a listed CA, you must provide the CA password (generally the root password).

- 5 Click **Certificates > Add**.
- 6 Fill out the forms required for a server certificate. After the last form is complete, a server certificate is created and listed in the certificate list.
- 7 Select the certificate you just created.
- 8 Click the **Export** button, then select **Export as Common Server Certificate**.

5.3.6 Changing the Mount Options Before an Upgrade

Before starting the upgrade, ensure that the mount options for all the partitions are set to **Device ID** or **Device Path**.

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

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

IMPORTANT: If you plan to clone your hard disks in the future, do not select **Device ID** as a mount option. The cloning process will fail. For more information, see [“New default in SLES/SLED 10 SP1: mount “by Device ID””](#).

- 6 Repeat [Step 4](#) and [Step 5 on page 91](#) 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.

5.3.7 Preparing an Installation Source

Review and complete the instructions for [“Setting Up a Network Installation Source” on page 31](#). We recommend using the network installation option, especially if you are upgrading multiple servers.

5.3.8 Synchronizing the OES Configuration Information before Starting an Upgrade

The modifications that you make to an OES server using YaST are stored in the configuration files at `/etc/sysconfig/novell`. This 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 `afp`, `lum`, `edir`, `cifs`, `iprint`, `dhcp`, `ncs`, `netstorage`, `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.

5.3.9 Moving to Common Proxy Users Before an Upgrade

If services are configured with service proxy users, it is recommended to move to common proxy users. Use the `move_to_common_proxy.sh` script to move services (AFP, CIFS, DNS, DHCP, NetStorage, NCS, and LUM) that use a service-specific proxy user to common proxy user. A common proxy user helps you avoid the administrative overhead that occurs with multiple proxy users.

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

- 1 Use the following commands to identify the list of services that use common proxy users and service-specific proxy users:

```
cd /opt/novell/proxymgmt/bin
./retrieve_proxy_list.sh
cat /var/opt/novell/log/proxymgmt/pxylist.txt
```

- 2 Use the following command to move the services that are not using the common proxy user:

```
./move_to_common_proxy.sh -d <LDAP Admin FDN> -w <LDAP Admin Password> -i <LDAP server IP address> -p <LDAP port> -s <service name>
```

Use a comma to separate multiple services. To move all services, use the keyword 'all' in the service name.

For example, to move the LUM service, the command would be:

```
./move_to_common_proxy.sh -d cn=admin,o=novell -w novell -i 192.168.1.255 -p 636 -s novell-lum
```

After moving to common proxy user, verify the value of the field `CONFIG_LDAP_PROXY_CONTEXT` in the file `/etc/sysconfig/novell/oes-ldap`. If the value is empty or not in the format `cn=OESCommonProxy_<short hostname>, <common proxy context>`, you must do the following to avoid any failures during upgrade:

- 1 Run the command `/opt/novell/proxymgmt/bin/cp_retrieve_proxy_cred username`.
- 2 Copy the output received and paste it as the value for the field `CONFIG_LDAP_PROXY_CONTEXT` in the file `/etc/sysconfig/novell/oes-ldap`.

5.4 Upgrading to OES 2018

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 93](#)
- ♦ [Section 5.4.2, “Specifying the Partition to Update,” on page 94](#)
- ♦ [Section 5.4.3, “Reviewing the Previously Used Repositories,” on page 94](#)
- ♦ [Section 5.4.4, “Specifying Customer Center Configuration Settings,” on page 94](#)
- ♦ [Section 5.4.5, “Specifying the Add-On Product Installation Information,” on page 96](#)
- ♦ [Section 5.4.6, “Verifying and Customizing the Update Options in Installation Settings,” on page 96](#)
- ♦ [Section 5.4.7, “Accepting the Installation Settings,” on page 98](#)
- ♦ [Section 5.4.8, “Specifying Configuration Information,” on page 98](#)
- ♦ [Section 5.4.9, “Finishing the Upgrade,” on page 101](#)

5.4.1 Using Physical Media to Upgrade

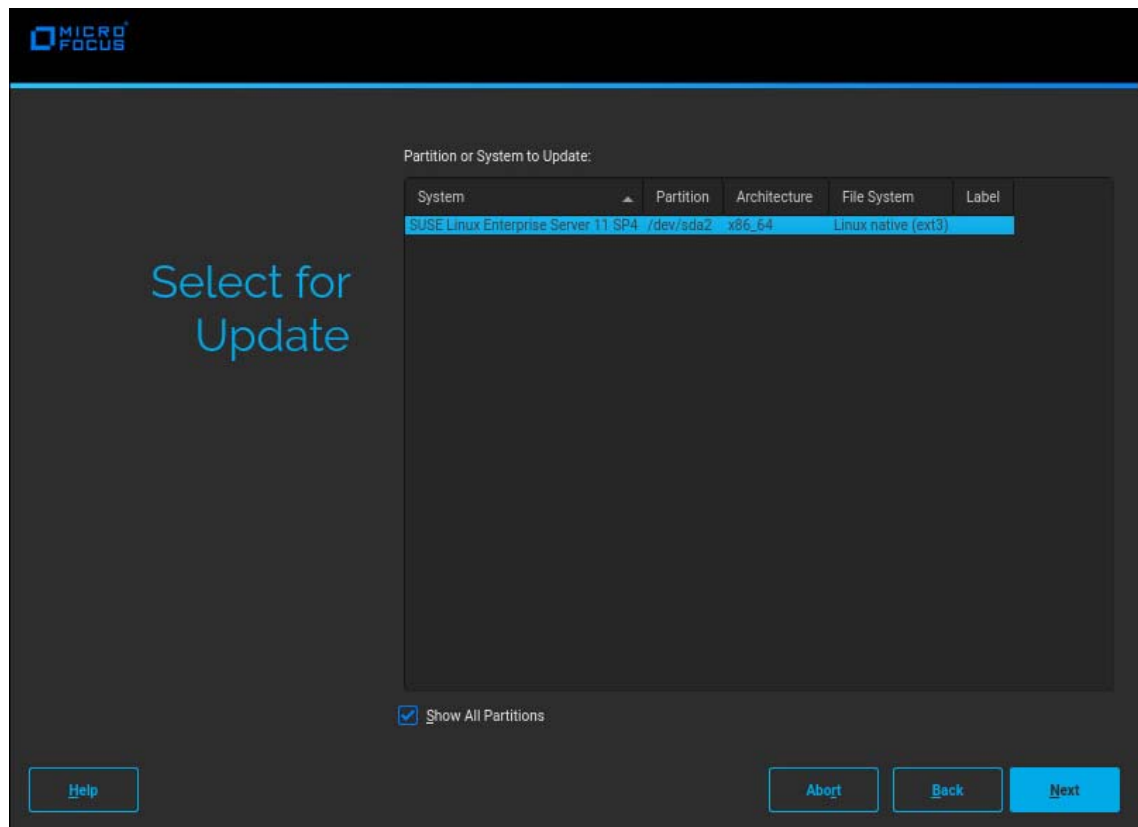
- 1 Ensure that the server meets the upgrade requirements. See [“Meeting the Upgrade Requirements” on page 89](#).
- 2 Insert the OES 2018 Install Media into the DVD drive of the server that you are upgrading to OES 2018, then reboot the machine.
- 3 From the DVD boot menu, select **Upgrade**, then press 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 94](#).
 - 6b [“Reviewing the Previously Used Repositories” on page 94](#)
 - 6c [“Specifying Customer Center Configuration Settings” on page 94](#)
 - 6d [“Specifying the Add-On Product Installation Information” on page 96](#)
 - 6e [“Verifying and Customizing the Update Options in Installation Settings” on page 96](#).
 - 6f [“Accepting the Installation Settings” on page 98](#).
 - 6g [“Specifying Configuration Information” on page 98](#).
 - 6h [“Finishing the Upgrade” on page 101](#).
- 7 Verify that the upgrade was successful. See the procedures in [“Verifying That the Installation Was Successful” on page 81](#).
- 8 Complete the server setup by following the procedures in [“Completing OES Installation or Upgrade Tasks” on page 109](#).

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 OES 2015 and SLES 11 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 2018 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 95](#)
- ♦ [“Registering the Server During the Upgrade” on page 95](#)

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

- 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 96](#).

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 2018. For example, iPrint for OES.

If you do not want to add any add-on products with OES 2018, click **Next** to continue with [“Verifying and Customizing the Update Options in Installation Settings” on page 96](#).

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 **Update Options**.
- 2 In the Update Options page, click **Update with Installation of New Software and Features Based on the Selection > Select Patterns**.
- 3 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 2-5 on page 23](#).

Some OES services, such as Novell CIFS and Novell Samba, are not supported together on the same server.

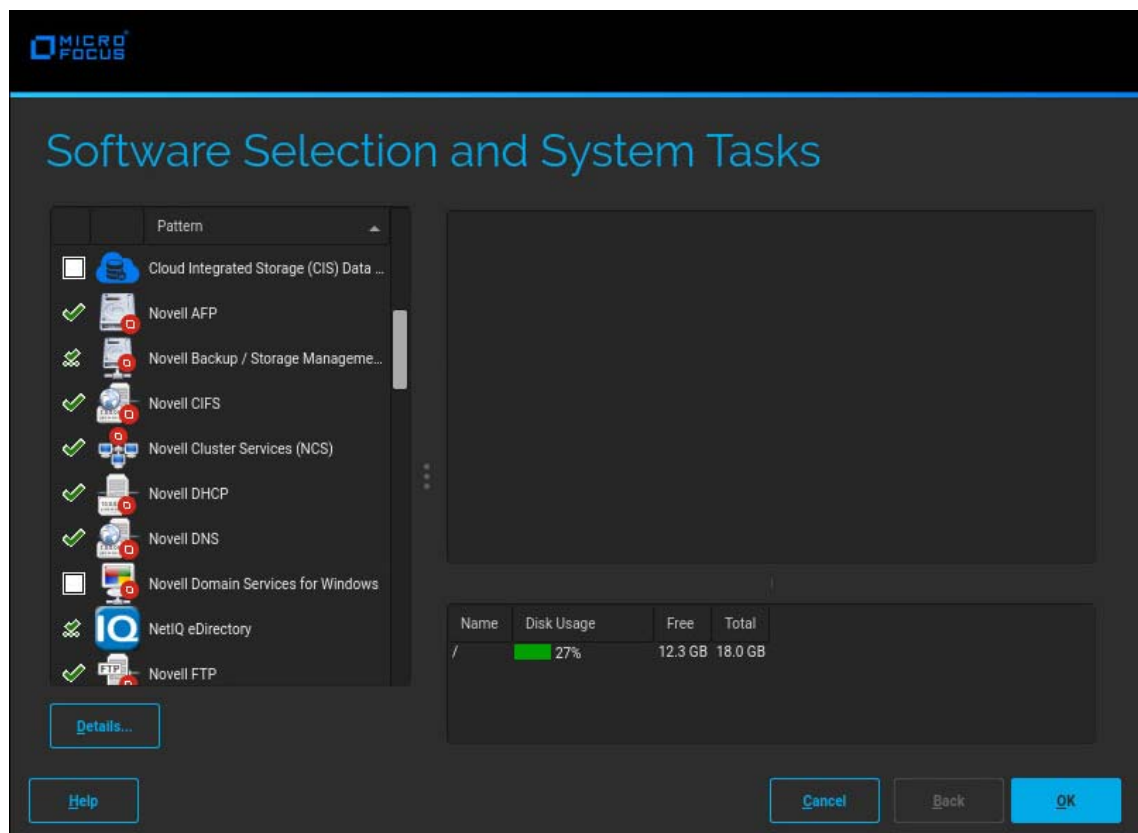
IMPORTANT: If you deselect a pattern after selecting it, you are instructing the installation program to not install that pattern and all of its dependent patterns. Rather than deselecting a pattern, click **Cancel** to cancel your software selections, then click the **Select Patterns** heading again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

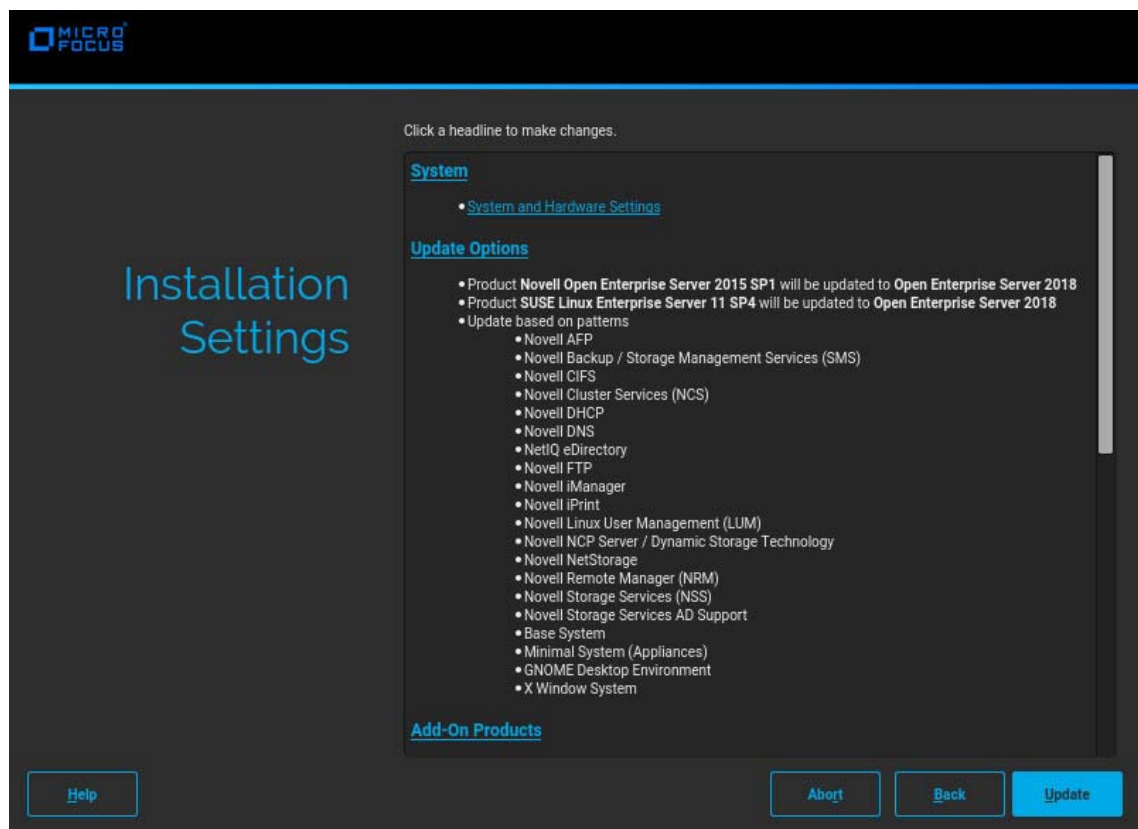
Attempting to uninstall a service by deselecting its pattern is not recommended. For more information, see [Chapter 12, “Disabling OES 2018 Services,” on page 153](#).

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



- 4 If you want to see the details of your selections, click **Details....**
- 5 When you have the software components selected that you want to install, click **Accept**.
- 6 When the notification about deleting unmaintained packages appears, click **OK**.
- 7 (Conditional) If the prompt for **Automatic Changes** displays, click **Continue**.
- 8 (Conditional) If you are prompted to resolve any dependency conflicts, resolve them.
- 9 If the Update Options page displays again, click **OK**.
- 10 On the Installation Settings page, ensure the following are listed under the **Update Options**:
 - ♦ Product **Novell Open Enterprise Server 2015 SP1** will be updated to **Open Enterprise Server 2018**
 - ♦ Product **SUSE Linux Enterprise Server 11 SP4** will be updated to **Open Enterprise Server 2018**

Proceed with [Section 5.4.7, "Accepting the Installation Settings,"](#) on page 98.



- 11 If you see package conflict errors (red text under the **Packages** link), refer to the [OES 2018: Release Notes](#) for resolution instructions.
- 12 Continue with “[Accepting the Installation Settings](#)” on page 98.

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 98.

5.4.8 Specifying Configuration Information

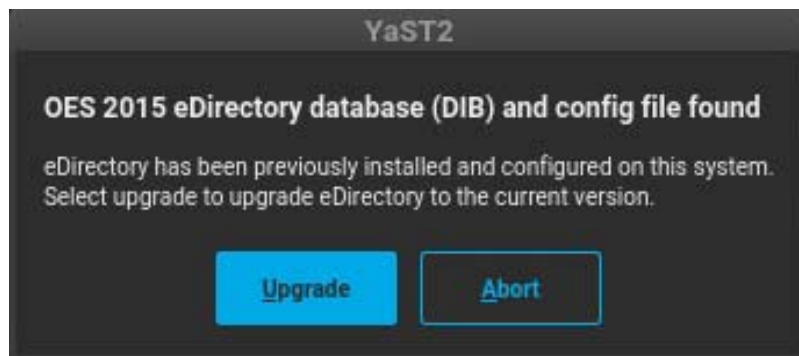
When the server reboots, you are required to complete the following configuration information:

- ♦ “[Upgrading eDirectory](#)” on page 99
- ♦ “[Specifying LDAP Configuration Settings](#)” on page 99
- ♦ “[Configuring Open Enterprise Server Services](#)” on page 100

Upgrading eDirectory

OES 2018 includes eDirectory 9.0.

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



NOTE

- ♦ If you are upgrading from OES 11 SP3, this dialog will show that the OES 11 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 99](#).

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.

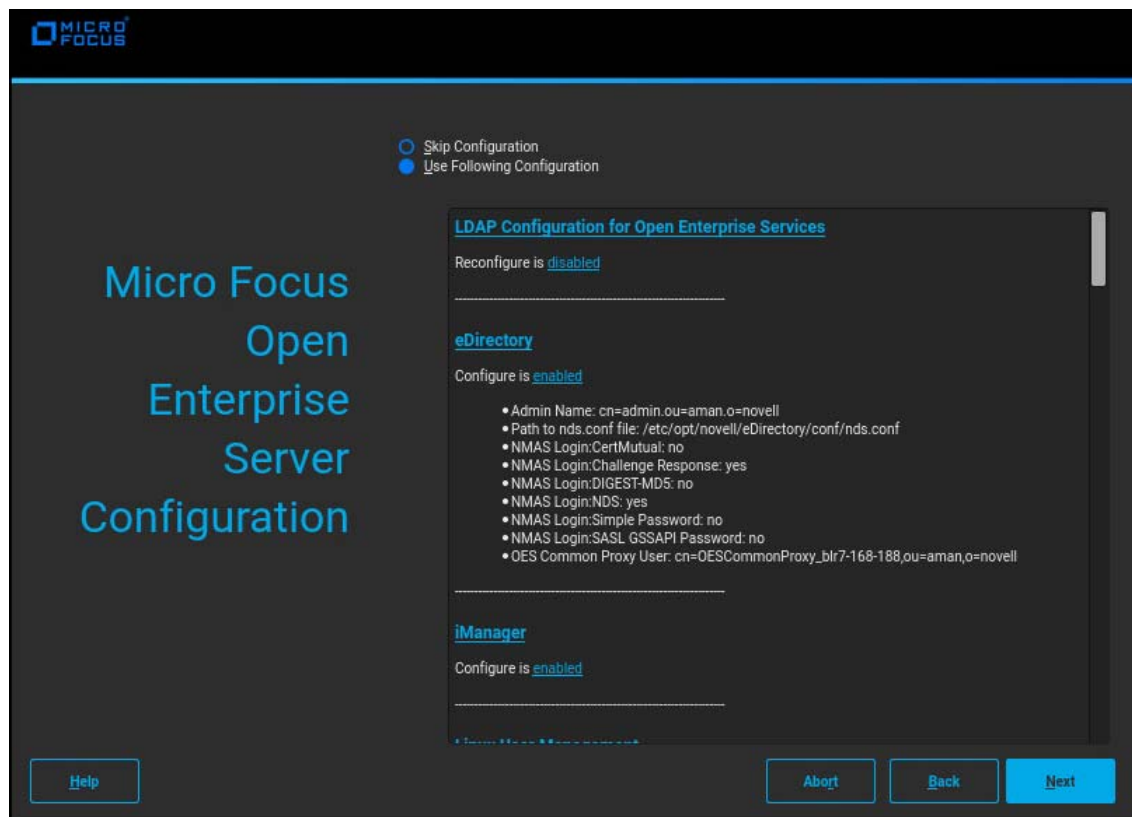
- 1 In the **eDirectory Tree Name** field, specify the name for the existing eDirectory tree that you are installing this server into.
- 2 In the **Admin Name and Context** field, specify the name and context for user Admin on the existing tree.
- 3 In the **Admin Password Name** field, specify a password 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 100](#).

Configuring Open Enterprise Server Services

After you complete the LDAP configuration or eDirectory configuration, the **Micro Focus 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 56](#), or click a link below:

- ◆ [AFP](#)
- ◆ [Backup/Storage Management Services \(SMS\)](#)
- ◆ [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](#)
 - ♦ [NetStorage](#)
 - ♦ [Pre-Migration Server](#)
 - ♦ [Novell Remote Manager \(NRM\)](#)
 - ♦ [Novell Samba](#)
 - ♦ [Novell Storage Services](#)
 - ♦ [NSS Active Directory Support](#)
- 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 56](#).

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 **Enabled** 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 2018 Server” on page 83](#).
 - 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 5.4.9, “Finishing the Upgrade,” on page 101](#).

5.4.9 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.

5.5 Using AutoYaST for an OES 2018 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 OES 2018 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 102](#)
- [Section 5.5.2, “Creating an Answer File to Provide the eDirectory and DSfW Passwords,” on page 102](#)
- [Section 5.5.3, “Upgrading an OES 11 SP2, OES 11 SP3, OES 2015, or OES 2015 SP1 Server to OES 2018,” on page 104](#)
- [Section 5.5.4, “Upgrading an OES 11 SP2, OES 11 SP3, OES 2015, and OES 2015 SP1 XEN Guest Server to OES 2018,” on page 104](#)
- [Section 5.5.5, “Troubleshooting an AutoYaST Upgrade,” on page 105](#)

5.5.1 Prerequisites

- Identify the 64-bit OES 11 SP2, OES 11 SP3, OES 2015 or OES 2015 SP1 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 2018 upgrade requirements specified in [Section 5.3, “Meeting the Upgrade Requirements,” on page 89](#).
- 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 (for OES 11 SP2, the file name is `edir_oes11_sp2`; for OES 11 SP3, it is `edir_oes11_sp3`; for OES 2015, it is `edir_oes2015` and for OES 2015 SP1, it is `edir_oes2015_sp1`) 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 102](#).

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 OES 11 SP2, OES 11 SP3, OES 2015 or OES 2015 SP1 machine as a root user and execute the following command:

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

Using the GUI on OES 11 SP2 and Above

- 1 Using the GUI on OES 11 SP2 and above

- 1a In the terminal window, type the following command:

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

- 1b 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 create-answer-file.ycp --help`.

5.5.3 Upgrading an OES 11 SP2, OES 11 SP3, OES 2015, or OES 2015 SP1 Server to OES 2018

Ensure that you have met all the requirements listed in [Section 5.5.1, "Prerequisites," on page 102](#).

- 1 Use the integrated ISO (OES2018-DVD-x86_64-DVD1.iso) to boot the OES 11 SP2, OES 11 SP3, OES 2015 or OES 2015 SP1 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
```

- 3 Press Enter.

The upgrade proceeds without any user intervention.

5.5.4 Upgrading an OES 11 SP2, OES 11 SP3, OES 2015, and OES 2015 SP1 XEN Guest Server to OES 2018

Ensure that you have met all the requirements listed in [Section 5.5.1, "Prerequisites," on page 102](#).

- 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:

```
os=sles12 vm-install --vm-settings /etc/xen/vm/<guest>.xml --os-type $os --os-  
settings http://<the web server IP>/download/autoupgrade.xml
```

- 5 In the Operating System Installation screen, select the appropriate SLES 12 options as shown in the following image.

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

Operating System Installation

Specify the bootable virtual disk (often labeled as Disk 1) or the network installation source URL. Each CD, DVD, or ISO image required for installation must be added as a virtual disk.

☒ Virtual Disk: 1.0 GB CD-ROM or DVD (file:/root/OES2018-DVD-x86_64-DVD1.iso) + Add
☐ Network URL: ▼
☐ PXE Boot ▼

Some operating systems support automating the installation by specifying a URL or file(s). Select a directory to include multiple files.

AutoYaST file: Find

Some operating systems accept additional arguments, used to customize the installation or boot process.

Additional Arguments:

Select the behavior when the operating system exits with power off, reboot or crash. Settings take effect after installation is complete.

Power Off: preserve ▼
 Reboot: restart ▼
 Crash: coredump-restart ▼

Cancel Apply

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 106
- ♦ “Unattended Upgrade Scenarios That Require User Input” on page 106

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 102](#)

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 11 SP2, the file name is `edir_oes11_sp2`; for OES 11 SP3, it is `edir_oes11_sp3`; for OES 2015, it is `edir_oes2015`; for OES 2015 SP1, it is `edir_oes2015_sp1` and for OES 2018, it is `edir_oes2018`) at `/etc/sysconfig/novell/`, you will be prompted for the same. For more information, see [Section 5.5.1, “Prerequisites,” on page 102](#).

5.6 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.

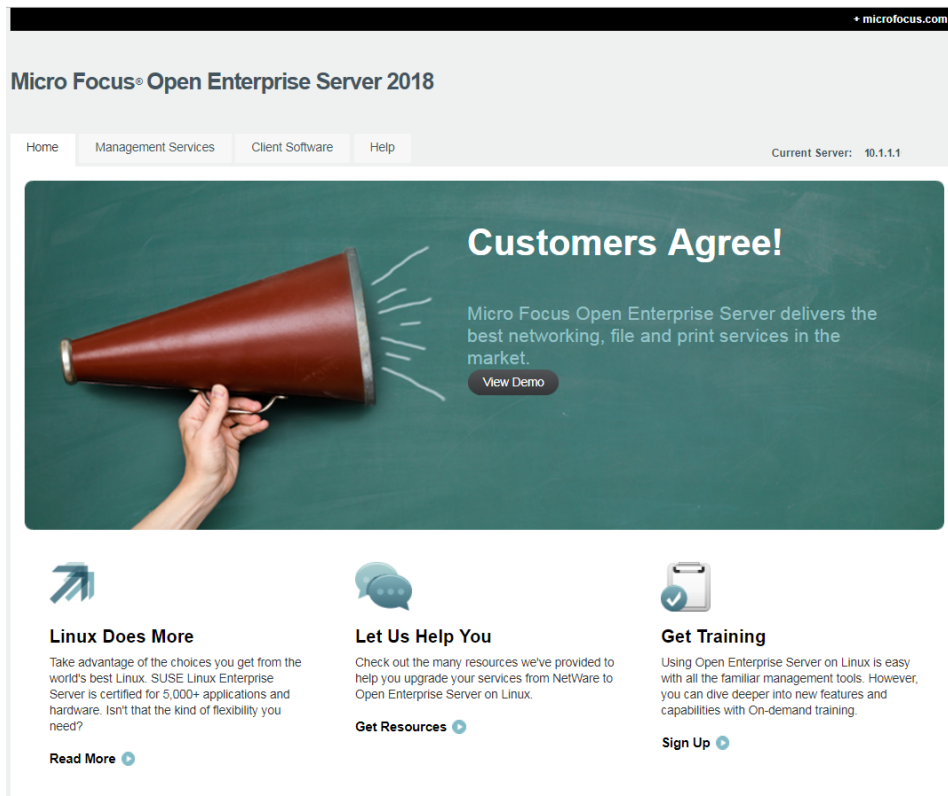
You can also quickly verify a successful installation by accessing the server from your Web browser.

- 1 In the Address field of your Web browser, enter the following URLs:

`http://IP_or_DNS`

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

You should see a Web page similar to the following:



- 2 If you want to look at the eDirectory tree and begin to see how iManager works, click the Management Services home page, click **Management Tools** > **iManager**, and then log in as user Admin (the user you created during product installation).

You can also access iManager by typing the following URL in a browser window and logging in as user Admin:

```
http://IP_or_DNS_name/nps/iManager.html
```

- 3 Verify the version of OES using the following command. It should be OES 2018.

```
cat /etc/*-release
```

- 4 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 2018 or an installation source.

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

- 5 Continue with [“What's Next” on page 107](#).

5.7 What's Next

After you complete the upgrade and verify that it was successful, see [“Completing OES Installation or Upgrade Tasks” on page 109](#).

6 Completing OES Installation or Upgrade Tasks

This section provides information for completing the following tasks:

- ♦ [Section 6.1, “Determining Which Services Need Additional Configuration,” on page 109](#)
- ♦ [Section 6.2, “Rebooting the Server after Installing NSS,” on page 110](#)
- ♦ [Section 6.3, “Restarting Tomcat,” on page 110](#)
- ♦ [Section 6.4, “Implementing Digital Certificates in an OES Environment,” on page 110](#)

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 2.4.4, “Adding/Configuring OES Services as a Different Administrator,” on page 20](#).

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 2018 services.

Table 6-1 OES 2018 Services Additional Installation and Configuration Instructions

OES 2018 Service	For Additional Installation and Configuration Information
Domain Services for Windows	See “ Installing Domain Services for Windows ” in the OES 2018: Domain Services for Windows Administration Guide .
Novell AFP	See “ Installing and Setting Up AFP ” in the OES 2018: Novell AFP for Linux Administration Guide .
Novell Backup/Storage Management Services (SMS)	See “ Installing and Configuring SMS ” in the OES 2018: Storage Management Services Administration Guide for Linux .
Novell CIFS	See “ Installing and Setting Up CIFS ” in the OES 2018: Novell CIFS for Linux Administration Guide .
Novell Cluster Services	See “ Installing, Configuring, and Repairing Novell Cluster Services ” in the OES 2018: Novell Cluster Services for Linux Administration Guide .
Novell DHCP	See “ Installing and Configuring DHCP ” in the OES 2018: DNS/DHCP Services for Linux Administration Guide .
Novell DNS	See “ Installing and Configuring DNS ” in the OES 2018: DNS/DHCP Services for Linux Administration Guide .

OES 2018 Service	For Additional Installation and Configuration Information
NetIQ eDirectory 9.0.3	See “Installing or Upgrading NetIQ eDirectory on Linux” in the NetIQ eDirectory Installation Guide .
Novell iManager 3.0.2	See “Installing iManager Server and Workstation” in the NetIQ iManager Installation Guide .
Novell iPrint	See “Installing and Setting Up iPrint on Your Server” in the OES 2018: iPrint Administration Guide .
Novell Linux User Management	See “Setting Up Linux User Management” in the OES 2018: Linux User Management Administration Guide .
Novell NCP Server	See “Installing and Configuring NCP Server for Linux” in the OES 2018: NCP Server for Linux Administration Guide .
Novell NetStorage	See “Installing NetStorage” in the OES 2018: NetStorage Administration Guide for Linux .
Novell Remote Manager	See “Changing the HTTPSTKD Configuration” in the OES 2018: OES Remote Manager Administration Guide .
Novell Samba	See “Installing the Novell Samba Components” in the OES 2018: Novell Samba Administration Guide .
Novell Storage Services	See “Installing and Configuring Novell Storage Services” in the OES 2018: NSS File System Administration Guide for Linux .
Pre-Migration Server	See “Preparing for Transfer ID” in the OES 2018: Migration Tool 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 be 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 Novell Storage Services Active Directory (NSS AD) support afresh, or after upgrading to OES 2018.

- ♦ [Section 7.1, “Understanding the NSS AD Support,” on page 113](#)
- ♦ [Section 7.2, “NSS AD Support Matrix,” on page 116](#)
- ♦ [Section 7.3, “Prerequisites for Installing and Configuring NSS AD,” on page 117](#)
- ♦ [Section 7.4, “Installing or Upgrading to OES 2018 with NSS AD Support,” on page 118](#)
- ♦ [Section 7.5, “About Novell Identity Translator \(NIT\),” on page 122](#)

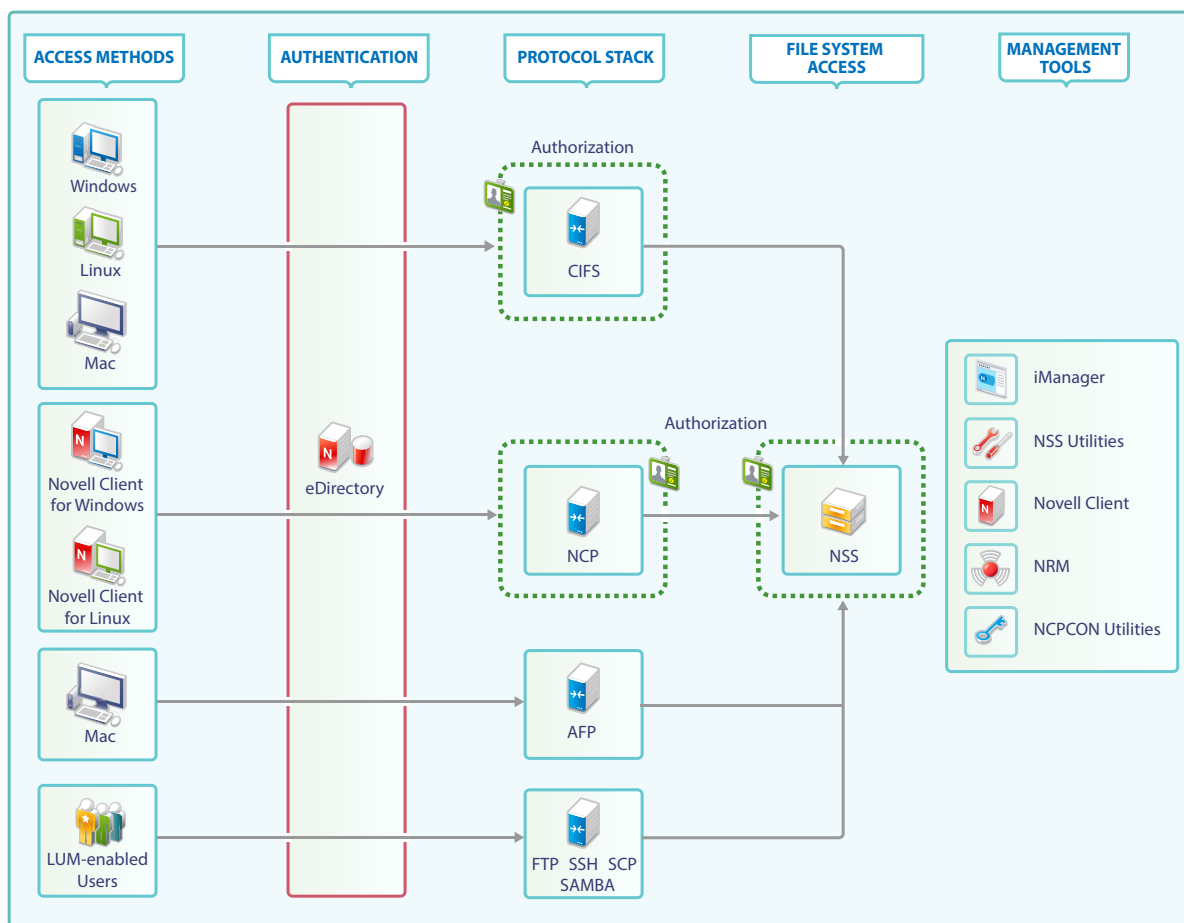
7.1 Understanding the NSS AD Support

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 AFP or CIFS. To access NSS resources using FTP, Samba, 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 AFP, FTP, Samba, 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.

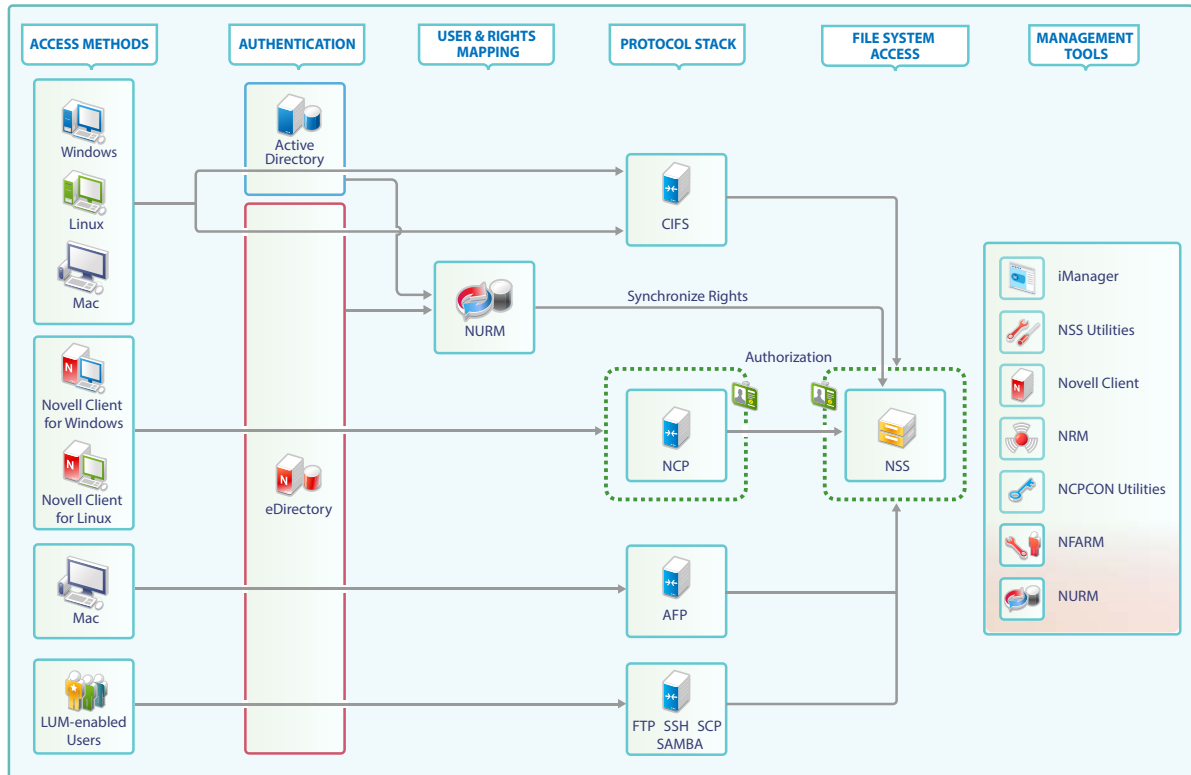
Rights Management: iManager, rights utility, NCPCON utilities, Client for Open Enterprise Server for Windows and Novell Client for Linux

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, AFP, and Samba 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 114](#) under [Section 7.1.1, "NSS Resource Access Until OES 11 SP2," on page 113](#).

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, AFP, FTP, Samba, 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 AFP, FTP, Samba, 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.

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 122](#).

7.2 NSS AD Support Matrix

- ♦ **OES 2018:** SLES 12 SP2
- ♦ **Active Directory:** Active Directory running on Windows 2008, Windows 2008 R2, Windows 2012, and Windows 2012 R2. Beginning with OES 2015 SP1 both single and multiple forests are supported.
- ♦ **OES File Access Rights Management Utility (NFARM):** Windows 10, Windows 8.1, Windows 8, Windows 7 SP1, Windows 7, Windows 2012 R2, Windows 2012, Windows 2008 R2, and Windows 2008.

- ♦ **OES User Rights Map Utility (NURM):** Any web browser that supports, HTML5, CSS3, and Java script.

7.3 Prerequisites for Installing and Configuring NSS AD

- ♦ **Active Directory:** Ensure that you have a working AD server, and the OES 2018 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.
- ♦ **Time Synchronization:** The clocks must be synchronized between OES 2018 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 \(http://support2.microsoft.com/kb/248717\)](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 122](#).

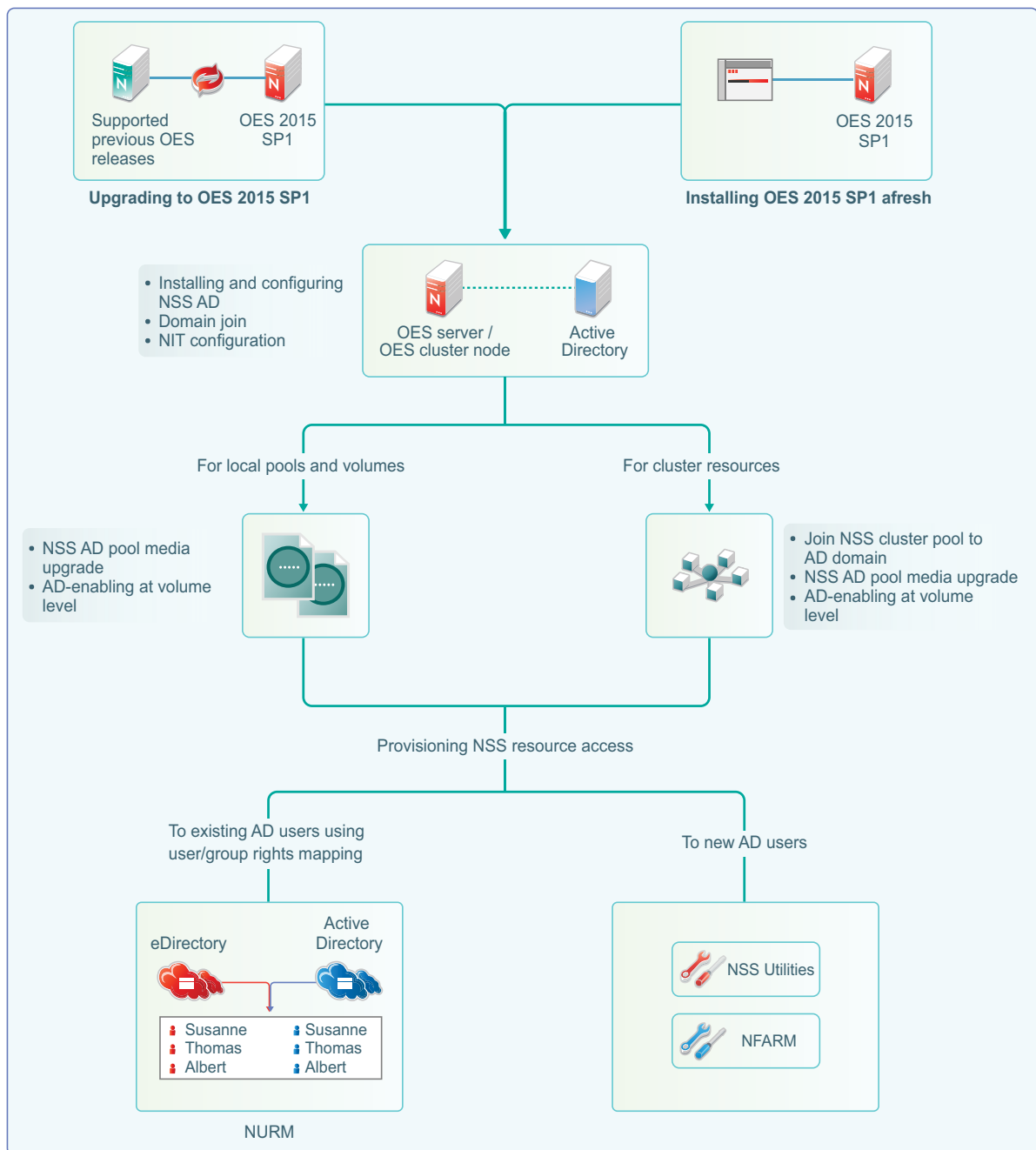
- ♦ **NSS AD Coexistence with Other OES Services:** When you configure and install NSS AD, ensure that you do not opt to install Novell SAMBA and DSfW on the same server where NSS AD will be installed and configured.
- ♦ **NSS AD's Dependency on CIFS Service:** Before installing and configuring NSS AD, ensure that the CIFS service is installed and running.
- ♦ **Cluster Recommendation:** In a cluster environment, if you plan to upgrade to OES 2018 with NSS AD support, it is recommended to upgrade all the cluster nodes to OES 2018. 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 *OES 2018: NSS File System 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 *OES 2018: NSS AD Administration Guide*.

7.4 Installing or Upgrading to OES 2018 with NSS AD Support

Here's how you can install and configure NSS AD afresh or after an upgrade to OES 2018.

- ♦ [Section 7.4.1, “Resolving the AD DNS Name from OES 2018,” on page 120](#)
- ♦ [Section 7.4.2, “Installing and Configuring NSS AD Support,” on page 120](#)
- ♦ [Section 7.4.3, “Validating the NSS AD Configuration,” on page 120](#)



- ♦ For information on installing or upgrading to OES 2018, domain join, and NIT configuration, see [Section 7.4.2, “Installing and Configuring NSS AD Support,”](#) on page 120.
- ♦ 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 *OES 2018: NSS File System 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 *OES 2018: NSS File System 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 *OES 2018: NSS File System 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 Novell Rights Map utility to map users and rights between eDirectory and Active Directory users. For more information, see “[OES User Rights Management \(NURM\)](#)” in the *OES 2018: NSS File System Administration Guide for Linux*.
- ♦ To manage AD users’ rights, user quota, owner information, directory quota and so on, use Novell File Access Rights Management or rights utility. For more information, see “[OES File Access Rights Management \(NFARM\)](#)” and “[rights](#)” in the *OES 2018: NSS File System Administration Guide for Linux*.

There is no change with the way you install or upgrade to OES 2018, except in the Novell Storage Services AD Support Configuration screens.

7.4.1 Resolving the AD DNS Name from OES 2018

To make OES 2018 with NSS AD work properly, ensure that AD server and OES 2018 server 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.

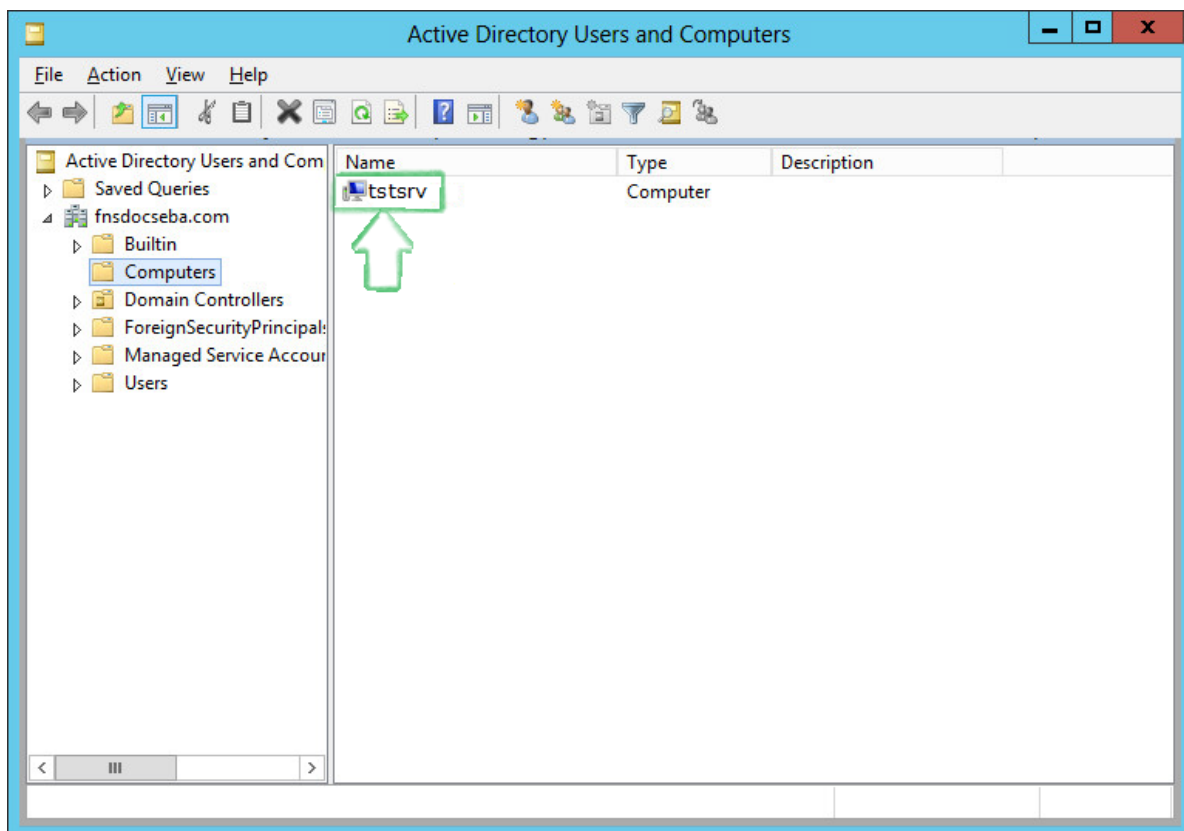
7.4.2 Installing and Configuring NSS AD Support

After resolving the AD DNS Name from the OES 2018 server, under the OES Patterns screen, select Novell 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 2018 computer object will be created. The default container is `cn=computers`. If you have already created a OES 2018 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 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 a new service in OES 2015 as 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 [OES 2018: 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 Novell 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 <code>uidNumber</code> 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 <code>uidNumber</code> attribute in Active Directory is ignored.
	Disabled	Retrieves the <code>uidNumber</code> from Active Directory when available. Users without a <code>uidNumber</code> cannot access NSS.
The <code>uidNumber</code> attribute is not set for any AD users. No AD users have a UID number in Active Directory	Enabled	Generates UIDs within the specified UID range for all AD users needing NSS access.
	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 Novell CIFS, NSS, and SMS.

8

Updating (Patching) an OES 2018 Server

To update your server with the patches released from Micro Focus requires you to perform the following tasks during the installation or upgrade or after the installation or upgrade is complete. The instructions in this section are for patching the server after the installation or upgrade is complete.

- ♦ [Section 8.1, “Overview of Updating \(Patching\),” on page 125](#)
- ♦ [Section 8.2, “Preparing the Server for Updating,” on page 126](#)
- ♦ [Section 8.3, “Registering the Server in the Customer Center,” on page 127](#)
- ♦ [Section 8.4, “Updating the Server,” on page 130](#)
- ♦ [Section 8.5, “GUI Based Patching,” on page 133](#)
- ♦ [Section 8.6, “Frequently Asked Questions about Updating,” on page 133](#)
- ♦ [Section 8.7, “Patching From Behind a Proxy Server,” on page 133](#)
- ♦ [Section 8.8, “Installing the Latest iManager NPMs After Applying OES Patches,” on page 134](#)
- ♦ [Section 8.9, “Restarting the OES Instance of Tomcat After Applying a Tomcat Update,” on page 134](#)

8.1 Overview of Updating (Patching)

- ♦ [Section 8.1.1, “The Patch Process Briefly Explained,” on page 125](#)
- ♦ [Section 8.1.2, “Update Options,” on page 126](#)

8.1.1 The Patch Process Briefly Explained

The OES 2018 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 2018 administrators have three options for updating servers with patches from Micro Focus.

- ♦ **Novell Online Update Servers:** For those who don't require an internal update source, OES 2018 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 (SMT) for SUSE Linux Enterprise:** This product doesn't require a separate license. It lets you host patches from the Novell 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 [Novell Download Site \(http://download.novell.com/Download?buildid=l8FuDkiYOg0~\)](http://download.novell.com/Download?buildid=l8FuDkiYOg0~).

NOTE: OES 2018 patch channels are available through NCC. If you are using SMT for patch update, ensure that it communicates only with NCC and not with SCC.

- ♦ **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 about ZENworks Linux Management, see its [product page on Novell.com \(https://www.novell.com/documentation/zenworks11/zen11_cm_linuxpkg_mgmt/data/bvjhr7p.html\)](https://www.novell.com/documentation/zenworks11/zen11_cm_linuxpkg_mgmt/data/bvjhr7p.html).

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 or ZCM 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.

NOTE: If the OES 2018 server is patched post January 2019, a message to import the new keys found in the repository is displayed. For more information, see [Appendix C, "Importing New Build Keys to the Keyring," on page 197](#).

8.2 Preparing the Server for Updating

Before you apply the patch on the server, review the following information:

- ♦ Make sure you have installed all the services that you need on the server.
- ♦ 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`.

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

In particular, ensure that you have enough space where the update process downloads all the updates to `/var/cache/zypp/`.

Depending on the number of patches that you are going to apply, you might need about 3 GB for OES 2018.

- ♦ 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.

- ♦ If you are planning to create a CA certificate with a 8192 bits RSA public key, ensure that you upgrade all the servers in your eDirectory tree to 9.1 before creating the CA certificate. For more information, see [NetIQ Certificate Server](#) in the [NetIQ eDirectory Administration Guide](#).

8.3 Registering the Server in the Customer Center

Before you can patch an OES 2018 server with updates from Micro Focus, 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 8.3.1, “Prerequisites,” on page 127](#)
- ♦ [Section 8.3.2, “Registering the Server in the Customer Center Using the Command Line,” on page 128](#)
- ♦ [Section 8.3.3, “Registering the Server in the Customer Center Using the GUI,” on page 129](#)

8.3.1 Prerequisites

To complete these procedures, you must have the following:

- ♦ A Customer Center account or access to an account.

This is the same account that you use for Bugzilla. For more information about Customer Center account, see [Micro Focus Customer Center - Frequently Asked Questions \(https://www.novell.com/cchelp/ncc-faq.html\)](#).

- The activation codes for OES that you received when you purchased your product.
- An established connection to the Internet.

8.3.2 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=oes2018_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:

```
Test-Server:~ # zypper ls
# | Alias | Name | Enabled | GPG Check | Refresh | Type
-----+-----+-----+-----+-----+-----+-----
1 | nu_novell_com | nu_novell_com | Yes | ---- | Yes | ris
2 | OES2018-2018-0 | OES2018-2018-0 | No | ---- | ---- | yast2
Test-Server:~ #
```

The URIs you see for the ZYPP type differ based on your installation source.

3b To verify the catalogs, enter

```
zypper lr
```

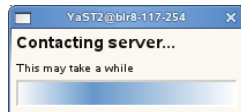
The results should be similar to the following:

```
Test-Server:~ # zypper lr
Repository priorities are without effect. All enabled repositories share the same priority.
# | Alias | Name | Enabled | GPG Check | Refresh
-----+-----+-----+-----+-----+-----
1 | OES2018-2018-0 | OES2018-2018-0 | No | ---- | ----
2 | nu_novell_com:OES2018-Pool | OES2018-Pool | Yes | (r) Yes | Yes
3 | nu_novell_com:OES2018-SLE-Module-Containers-12-SP2-Debuginfo-Pool | OES2018-SLE-Module-Containers-12-SP2-Debuginfo-Pool | No | ---- | ----
4 | nu_novell_com:OES2018-SLE-Module-Containers-12-SP2-Debuginfo-Updates | OES2018-SLE-Module-Containers-12-SP2-Debuginfo-Updates | No | ---- | ----
5 | nu_novell_com:OES2018-SLE-Module-Containers-12-SP2-Pool | OES2018-SLE-Module-Containers-12-SP2-Pool | Yes | (r) Yes | Yes
6 | nu_novell_com:OES2018-SLE-Module-Containers-12-SP2-Updates | OES2018-SLE-Module-Containers-12-SP2-Updates | Yes | (r) Yes | Yes
7 | nu_novell_com:OES2018-SLE-SDK-12-SP2-Debuginfo-Pool | OES2018-SLE-SDK-12-SP2-Debuginfo-Pool | No | ---- | ----
8 | nu_novell_com:OES2018-SLE-SDK-12-SP2-Debuginfo-Updates | OES2018-SLE-SDK-12-SP2-Debuginfo-Updates | No | ---- | ----
9 | nu_novell_com:OES2018-SLE-SDK-12-SP2-Pool | OES2018-SLE-SDK-12-SP2-Pool | No | ---- | ----
10 | nu_novell_com:OES2018-SLE-SDK-12-SP2-Updates | OES2018-SLE-SDK-12-SP2-Updates | No | ---- | ----
11 | nu_novell_com:OES2018-SLES12-SP2-Debuginfo-Pool | OES2018-SLES12-SP2-Debuginfo-Pool | No | ---- | ----
12 | nu_novell_com:OES2018-SLES12-SP2-Debuginfo-Updates | OES2018-SLES12-SP2-Debuginfo-Updates | No | ---- | ----
13 | nu_novell_com:OES2018-SLES12-SP2-Pool | OES2018-SLES12-SP2-Pool | Yes | (r) Yes | Yes
14 | nu_novell_com:OES2018-SLES12-SP2-Updates | OES2018-SLES12-SP2-Updates | Yes | (r) Yes | Yes
15 | nu_novell_com:OES2018-Updates | OES2018-Updates | Yes | (r) Yes | Yes
Test-Server:~ #
```

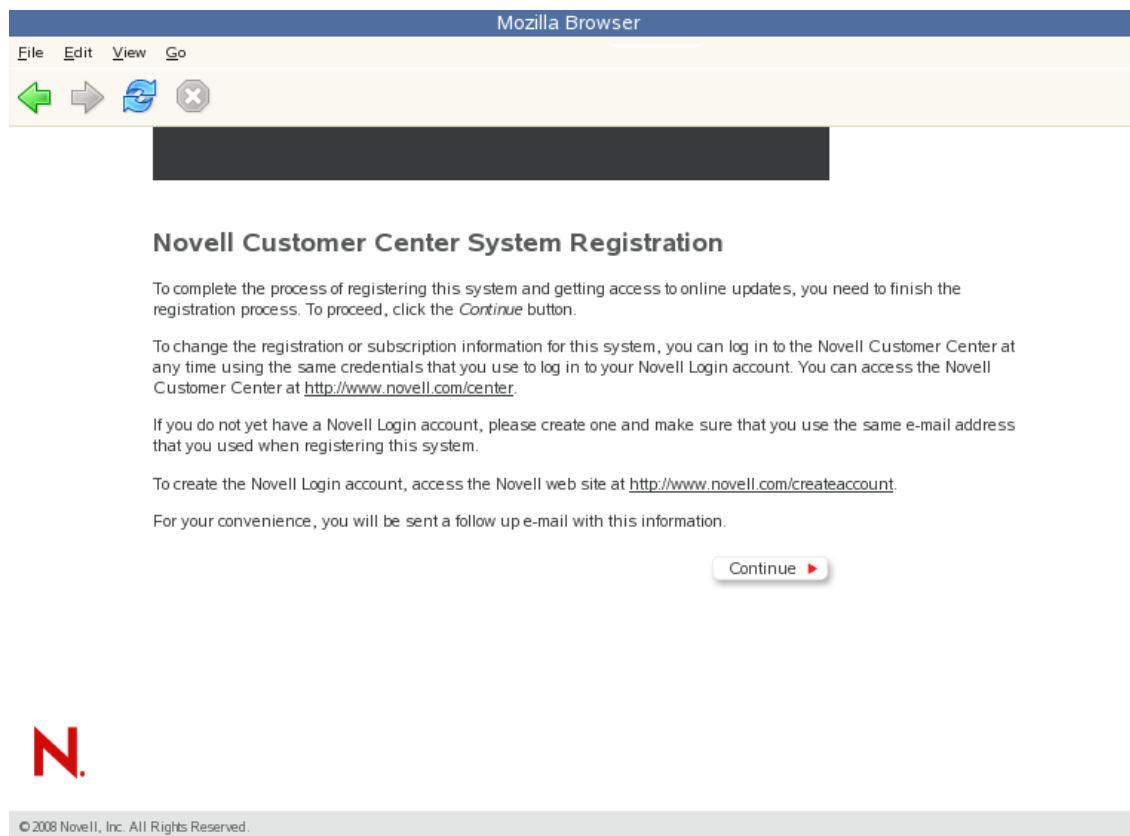

8.3.3 Registering the Server in the Customer Center Using the GUI

- 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.

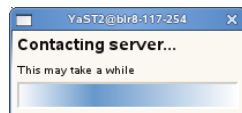
After you click **Next**, the following message is displayed. Wait until this message disappears and the Manual Interaction Required page displays.



- 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 2018 (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 following 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.

8.4 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 8.4.1, “Updating the Server Using the Command Line,” on page 131](#)

You could also patch an OES server using the following methods: [Section 8.5, “GUI Based Patching,” on page 133](#), [Section 8.7, “Patching From Behind a Proxy Server,” on page 133](#), and so on.

8.4.1 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 2018.

- 1 Log in to the server as `root` or `su` to `root`.
- 2 At the command line, enter the following commands. The screen shots show example output.

2a Refresh all services:

```
zypper ref -s
```

The list of repositories should include the following update repositories:

Enabled Repositories

- ♦ OES2018-Pool
- ♦ OES2018-Updates
- ♦ OES2018-SLES12-SP2-pool
- ♦ OES2018-SLES12-SP2-Updates
- ♦ OES2018-SLE-Module-Containers-12-SP2-Pool
- ♦ OES2018-SLE-Module-Containers-12-SP2-Updates

Optional/Disabled Repositories

- ♦ OES2018-SLE-Module-Containers-12-SP2-Debuginfo-Pool
- ♦ OES2018-SLE-Module-Containers-12-SP2-Debuginfo-Updates
- ♦ OES2018-SLES12-SP2-Debuginfo-Pool
- ♦ OES2018-SLES12-SP2-Debuginfo-Updates
- ♦ OES2018-SLE-SDK-12-SP2-Pool
- ♦ OES2018-SLE-SDK-12-SP2-Updates
- ♦ OES2018-SLE-SDK-12-SP2-Debuginfo-Pool
- ♦ OES2018-SLE-SDK-12-SP2-Debuginfo-Updates

2b See whether updates are available for OES 2018:

```
zypper patch-check --repo catalog1 --repo catalog2
```

For example,

```
zypper patch-check --repo OES2018-SLES12-SP2-Updates --repo OES2018-Updates
```

2c Update the server with all available OES 2018 patches:

```
zypper up -t patch -r OES2018-SLES12-SP2-Updates -r OES2018-Updates
```

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: Do not use the `zypper up` command by itself without the `-t` option to update an OES server. Always use the `-t patch` option as described in [Section 8.4.1, “Updating the Server Using the Command Line,” on page 131](#).

If the `-t patch` option is omitted, `zypper` includes SLES packages in the download that can cripple or completely break OES services.

The `-t patch` option also ensures that patch metadata (including script files, etc.) is downloaded so that SLES can correctly update the system.

For more information on zypper, see [SDB:Zypper usage 11.3](http://en.opensuse.org/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 -r OES2018-SLES12-SP2-Updates -r OES2018-Updates
```

2c To list the patches and their status, enter:

```
zypper pch OES2018-SLES12-SP2-Updates OES2018-Updates
```

2d To view specific patch information, enter:

```
zypper patch-info patch_name
```

For example:

```
zypper patch-info slessp4-sax2
```

2e To list all installed patches, enter:

```
zypper search -t pch -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 -r catalog1 -r catalog2 -g category_name
```

Replace *category_name* with `security`, `recommended`, or `optional`.

For example:

```
zypper patch -r OES2018-SLES12-SP2-Updates -r OES2018-Updates -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 slessp4-sax2-12428
```

- ♦ 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 2018 services are restarted.

8.5 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 2018.

- 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**.
 - ♦ OES2018-Pool
 - ♦ OES2018-Updates
 - ♦ OES2018-SLES12-SP2-pool
 - ♦ OES2018-SLES12-SP2-Updates
 - ♦ OES2018-SLE-Module-Containers-12-SP2-Pool
 - ♦ OES2018-SLE-Module-Containers-12-SP2-Updates
- 4 In the YaST Control Center, under **Software**, click **Online Update**.
- 5 Select the patches you want to apply and click **Accept**.
- 6 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.

8.6 Frequently Asked Questions about Updating

This section contains the following information:

- ♦ [Section 8.6.1, “Do I apply all the patches in the catalogs? How do I know which patches to apply?” on page 133](#)

8.6.1 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.

8.7 Patching From Behind a Proxy Server

See [TID 7006845 \(https://www.novell.com/support/kb/doc.php?id=7006845\)](https://www.novell.com/support/kb/doc.php?id=7006845).

8.8 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 3.0.3 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.

8.9 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 2018 servers.

For complete instructions on using AutoYaST2, see *Automatic Linux Installation and Configuration with Yast2* (<http://doc.opensuse.org/projects/YaST/openSUSE11.3/autoinstall/>). 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. This creates `/root/autoinst.xml` that can be used for cloning. For more information, see *SUSE AutoYast Guide* (https://www.suse.com/documentation/sles-12/book_autoyast/data/book_autoyast.html).

This section contains the following information:

- ♦ [Section 9.1, “Prerequisites,” on page 135](#)
- ♦ [Section 9.2, “Setting Up a Control File with OES Components,” on page 136](#)
- ♦ [Section 9.3, “Setting Up an Installation Source,” on page 141](#)
- ♦ [Section 9.4, “Cloning an OES Server Post OES Installation and Configuration,” on page 141](#)

9.1 Prerequisites

You need at least the following components to install an OES 2018 server by using AutoYaST:

- ☐ A server with OES 2018 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 136](#).

- ❑ 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 141](#).

- ❑ A source or server that contains the AutoYaST profile (control file).

For more information, see [“Setting Up an Installation Source” on page 141](#).

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. See [Section 9.2.1, “Fixing an Automatically Created Control File,” on page 136](#).
- ♦ You can create or modify a control file by using the AutoInstallation module in YaST. For procedures, see [Section 9.2.2, “Using the AutoInstallation Module to Create the Control File,” on page 136](#).

This system depends on existing modules that are usually used to configure a computer after OES 2018 is installed on a server.

9.2.1 Fixing an Automatically Created Control File

Review the following issue and solution to fix the automatically created control file.

- ♦ **Issue:** If you did not patch the server during the installation, the OES product is not identified correctly in the control file.

Solution: When creating the profile or control file, change the product line from:

```
<product>Novell Open Enterprise Server 11</product>
```

to

```
<product>OPEN_ENTERPRISE_SERVER</product>
```

9.2.2 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 2018.

- 1 On a server that has OES 2018 installed, 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 22](#). 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 AGFA Monotype Corporation 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](http://doc.opensuse.org/projects/YaST/openSUSE11.3/autoinstall/CreateProfile.Partitioning.html) (<http://doc.opensuse.org/projects/YaST/openSUSE11.3/autoinstall/CreateProfile.Partitioning.html>).
- 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”](http://www.suse.de/~ug/autoyast_doc/configuration.html#createprofile.scripts) (http://www.suse.de/~ug/autoyast_doc/configuration.html#createprofile.scripts) in *Automatic Linux Installation and Configuration with Yast2*.
 - 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 137](#). For more information about which modules are in each pattern, see [“Deciding What Patterns to Install” on page 22](#).

Pattern	Other Module Dependencies
Novell AFP	<ul style="list-style-type: none">◆ Novell Backup / Storage Management Services (SMS)◆ NetIQ eDirectory◆ Novell Storage Services (NSS)◆ Novell Linux User Management (LUM)◆ Novell Remote Manager (NRM)
Novell Backup/Storage Management Services (SMS)	<ul style="list-style-type: none">◆ Novell Linux User Management (LUM)◆ Novell Remote Manager (NRM)
Novell CIFS	<ul style="list-style-type: none">◆ Novell Backup / Storage Management Services (SMS)◆ NetIQ eDirectory◆ Novell Storage Services (NSS)◆ Novell Linux User Management (LUM)◆ Novell Remote Manager (NRM)

Pattern	Other Module Dependencies
Novell Cluster Services (NCS)	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell DHCP	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell DNS	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell Domain Services for Windows	<ul style="list-style-type: none"> ♦ Novell Backup / Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell DNS ♦ Novell iManager ♦ Novell iPrint ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM) ♦ Novell Storage Services (NSS) ♦ Novell NCP Server
NetIQ eDirectory	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell FTP	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell iManager	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell iPrint	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell iManager ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell Linux User Management (LUM)	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ Novell Remote Manager (NRM)

Pattern	Other Module Dependencies
Novell NCP Server / Dynamic Storage Technology	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell NetStorage	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ Novell iManager ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell Pre-Migration Server	<ul style="list-style-type: none"> ♦ Novell Backup / Storage Management Services (SMS) ♦ NetIQ eDirectory (without a replica) ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell Remote Manager (NRM)	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ Novell Linux User Management (LUM)
Novell Samba	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell Storage Services (NSS)	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell NCP Server ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)
Novell Storage Service AD Support	<ul style="list-style-type: none"> ♦ Novell Backup/Storage Management Services (SMS) ♦ NetIQ eDirectory ♦ Novell NCP Server ♦ Novell Storage Services (NSS) ♦ Novell CIFS Services ♦ Novell Linux User Management (LUM) ♦ Novell Remote Manager (NRM)

- 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* (<http://doc.opensuse.org/projects/YaST/openSUSE11.3/autoinstall/>).

13 Exit the configuration management tool by clicking **File** > **Exit**.

14 Proceed with “Setting Up an Installation Source” on page 141.

9.3 Setting Up an Installation Source

For OES 2018, you must set up a separate directory for the SLES 12 SP2 software and the OES 2018 software.

AutoYaST requires an installation source. You have several options. For an explanation of each, see “The Auto-Installation Process” (https://www.suse.com/documentation/sles-12/book_autoyast/data/invoking.html) in the *SUSE AutoYaST Guide* (https://www.suse.com/documentation/sles-12/book_autoyast/data/book_autoyast.html).

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 Reinstall an OES Server

To 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 root password.
 - ♦ Replace “ENTER PASSWORD HERE” with eDirectory password.
 - ♦ 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 \(http://www.novell.com/support/kb/doc.php?id=7006641\)](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 `OES2018-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.

NOTE: Cloud Integrated Storage (CIS) does not work, if autoinst.xml file is copied from already installed and configured OES 2018 server (without CIS) and manually add the CIS tags into autoinst.xml and then install OES 2018 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 server.

For example:

```
<ipv4_forward config:type="boolean">true</ipv4_forward>

<FW_MASQUERADE>yes</FW_MASQUERADE>
```

However, if OES 2018 server is installed using autoinst.xml created from already installed OES 2018 server (with CIS), the CIS works fine.

10 Installing, Upgrading, or Updating OES on a VM

In Open Enterprise Server (OES), you can install OES 2018 as a guest operating system on the following servers:

- ♦ A SUSE Linux Enterprise Server (SLES) 12 SP2 Linux server running KVM.
See the [Introduction to KVM Virtualization \(https://www.suse.com/documentation/sles-12/book_virt/data/cha_kvm_intro.html\)](https://www.suse.com/documentation/sles-12/book_virt/data/cha_kvm_intro.html) in the [Virtualization Guide \(https://www.suse.com/documentation/sles-12/book_virt/data/book_virt.html\)](https://www.suse.com/documentation/sles-12/book_virt/data/book_virt.html).
- ♦ A SUSE Linux Enterprise Server (SLES) 12 SP2 Linux server running Xen.
See [Introduction to Xen Virtualization \(https://www.suse.com/documentation/sles-12/book_virt/data/cha_xen_basics.html\)](https://www.suse.com/documentation/sles-12/book_virt/data/cha_xen_basics.html) in the [Virtualization Guide \(https://www.suse.com/documentation/sles-12/book_virt/data/book_virt.html\)](https://www.suse.com/documentation/sles-12/book_virt/data/book_virt.html).

For general information on the virtualization technology in SLES 12 SP2, see the [SLES 12 documentation \(https://www.suse.com/documentation/sles-12/\)](https://www.suse.com/documentation/sles-12/).

This section documents the system requirements, installation instructions, upgrade and migration instructions, and issues associated with setting up OES 2018 on a Xen-based virtual machine.

- ♦ [Section 10.1, “System Requirements,” on page 145](#)
- ♦ [Section 10.2, “Prerequisites,” on page 146](#)
- ♦ [Section 10.3, “Preparing the Installation Software,” on page 146](#)
- ♦ [Section 10.4, “Installing an OES 2018 VM Guest,” on page 147](#)
- ♦ [Section 10.5, “Upgrading an OES VM Guest to OES 2018,” on page 149](#)
- ♦ [Section 10.6, “Setting Up an OES 2018 VM Guest to Use Novell Storage Services \(NSS\),” on page 150](#)

10.1 System Requirements

To create an OES 2018 VM guest, you need a SLES 12 SP2 server that is set up as a VM host server.

- ♦ [Section 10.1.1, “VM Host Considerations,” on page 145](#)
- ♦ [Section 10.1.2, “Novell Storage Services Considerations,” on page 146](#)
- ♦ [Section 10.1.3, “Setup Instructions,” on page 146](#)

10.1.1 VM Host Considerations

When you set up a virtual machine host for OES 2018 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 2018 virtual machine, you need a minimum of 2 GB of memory (1 GB for the host plus 1GB for the OES 2018 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 2018 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 VM is tested as guest on SLES 11 SP4 and SLES 12 SP2 VM hosts.

10.1.2 Novell 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 *OES 2018: NSS File System Administration Guide for Linux*.

10.1.3 Setup Instructions

For setup procedures, see the *Virtualization Guide* (https://www.suse.com/documentation/sles-12/book_virt/data/book_virt.html).

10.2 Prerequisites

Before creating an OES 2018 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 135.
- ♦ 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 147
- ♦ [Section 10.3.2, “Preparing the Installation Source Files,”](#) on page 147

10.3.1 Downloading the Installation Software

For information on downloading the following ISO image files, see the [Open Enterprise Server 2018 Download Instructions \(https://download.novell.com/\)](https://download.novell.com/).

Table 10-1 OES ISO Images and DVD Labels for x86_64 (64-Bit Installations)

ISO Image File	DVD Label
OES2018-DVD-x86_64-DVD1.iso	Open Enterprise Server 2018 Media

10.3.2 Preparing the Installation Source Files

To create an OES 2018 VM guest, you must make the installation software available in one of the following locations:

- ♦ **A Local Installation Source:** The 64-bit ([Table 10-1](#)) ISO files copied to the host server's local drives.
- ♦ **A Network Installation Source:** The 64-bit ([Table 10-1](#)) 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 2018 VM Guest

Creating an OES 2018 virtual machine requires you to complete the following major tasks.

- ♦ [Section 10.4.1, "Specifying Options for Creating an OES 2018 VM Guest," on page 147](#)

10.4.1 Specifying Options for Creating an OES 2018 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 \(https://www.suse.com/documentation/sles-12/book_virt/data/cha_xen_config.html\)](https://www.suse.com/documentation/sles-12/book_virt/data/cha_xen_config.html)” in the *Virtualization with Xen guide (https://www.suse.com/documentation/sles-12/book_virt/data/book_virt.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 1024 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 2018 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/xen/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 2018 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 **Apply**.

9c To create additional virtual disks, click the Harddisk icon in the Disks wizard.

10 If you are installing SLES 12 SP2 from a downloaded ISO image file, click **DVD, browse to the SLES 12 SP2 image file, then click **Open > OK > Apply**.**

11 If you are installing OES 2018 from a downloaded ISO image file, click **DVD, browse to the OES 2018 image file, then click **Open > OK > Apply**.**

12 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**.

13 Click **Operating System:**

13a If you are installing from a downloaded ISO image, ensure that the SLES 12 SP2 image is specified as the **Virtual Disk** installation source.

13b If you are installing from a network installation source, specify the URL for the SLES 12 SP2 network installation source.

You specify a network installation source for OES 2018 during the install.

13c 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.

13d 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 usesh=1  
sshpassword=password
```

13e Click **Apply**.

14 Click **OK** to start the virtual machine and launch the operating system installation program.

15 Read and accept the license agreement, then continue with [Section 3.4, “Specifying Network Settings,”](#) on page 37.

10.5 Upgrading an OES VM Guest to OES 2018

IMPORTANT: To upgrade an OES VM paravirtualized guest to OES 2018, you must install using files on the network. Physical media upgrades and using ISO image files are not supported methods.

Performing a down-server upgrade on a Xen VM guest is very much like upgrading a physical machine

- ♦ [Section 10.5.1, “Before You Start the Upgrade Process,”](#) on page 149
- ♦ [Section 10.5.2, “Starting the Upgrade,”](#) on page 149

10.5.1 Before You Start the Upgrade Process

- 1 Make sure you follow all of the applicable instructions and guidelines in [Section 5.2, “Planning for the Upgrade to OES 2018,”](#) on page 88 and [Section 5.3, “Meeting the Upgrade Requirements,”](#) on page 89.

10.5.2 Starting the Upgrade

- 1 In Virtual Machine Manager, shut down the OES VM guest that you are upgrading.
- 2 Click the **Create a New Virtual Machine** icon or right-click localhost (Xen) and choose **New**.
- 3 Click **Forward**.
- 4 Select **I Need to Upgrade an Existing Operating System**, then click **Forward**.
- 5 Select **Novell Open Enterprise Server**, then click **Forward**.
- 6 In the Managed Virtual Machines list, select the VM guest you are upgrading.
- 7 In the Network URL field, type the URL to your SLES 12 SP2 network-based installation source, then click **Upgrade**.
- 8 On the Welcome page, agree to the license and click **Next**.
- 9 For instructions on the rest of the upgrade process, go to [Chapter 5, “Upgrading to OES 2018,”](#) on page 87 and continue from there.

10.6 Setting Up an OES 2018 VM Guest to Use Novell Storage Services (NSS)

When you install OES 2018 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 *OES 2018: NSS File System Administration Guide for Linux*.

11

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 11.1, “Configuring SHA-2 Certificate,” on page 151](#)
- ♦ [Section 11.2, “Verifying the Certificates with SHA-2 Signature,” on page 152](#)

11.1 Configuring SHA-2 Certificate

- ♦ [Section 11.1.1, “Prerequisites,” on page 151](#)
- ♦ [Section 11.1.2, “CA Server,” on page 151](#)
- ♦ [Section 11.1.3, “Other Servers,” on page 151](#)
- ♦ [Section 11.1.4, “Servers Running on eDirectory 8.8.7 or OES 11 SP1 or Earlier,” on page 152](#)

11.1.1 Prerequisites

- ♦ eDirectory (January 2016 eDirectory 8.8 SP8 Patch 6 Hot Patch 1)

11.1.2 CA Server

- 1 Apply patch on the OES server where CA is hosted in the tree.
- 2 Restart the eDirectory service.
`rcnstd 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.

```
rcnstd 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.

11.1.3 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.

```
rcnstd 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.

11.1.4 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 SP2, OES 11 SP3 or OES 2015 servers in the tree.

11.2 Verifying the Certificates with SHA-2 Signature

- ♦ On the OES server, run the following command against the LDAP server 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 /var/opt/novell/eDirectory/data/SSCert.der -inform der -text  
-noout"
```


12 Disabling OES 2018 Services

Although you can uninstall Open Enterprise Server (OES) 2018 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` and start YaST.
- 2 Click **System > Services Manager**.
- 3 Select the *applicable_service_name*, then click **Enable/Disable**.
- 4 Click **OK**.

You can also 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 3.0 Administration Guide](#).

13 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 13.1, “Cleaning Up the eDirectory Server,” on page 155](#)
- ♦ [Section 13.2, “Reconfiguring the eDirectory Server through YaST,” on page 157](#)
- ♦ [Section 13.3, “Reconfiguring OES Services,” on page 157](#)

13.1 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 13.1.1, “Before You Clean Up,” on page 155](#)
- ♦ [Section 13.1.2, “Reconfiguring the Replica Server,” on page 156](#)
- ♦ [Section 13.1.3, “Reconfiguring the CA Server,” on page 156](#)
- ♦ [Section 13.1.4, “Cleaning Up eDirectory,” on page 156](#)

13.1.1 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 13.1.2, “Reconfiguring the Replica Server,” on page 156](#).
- ♦ 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 13.1.3, “Reconfiguring the CA Server,” on page 156](#).

13.1.2 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 \(https://www.netiq.com/documentation/edirectory-9/edir_admin/data/a2iiiiik.html\)](https://www.netiq.com/documentation/edirectory-9/edir_admin/data/a2iiiiik.html) in the *NetIQ eDirectory 9.0 Administration Guide*.
- 2 Clean up the replica server.
For more information, see [Section 13.1.4, “Cleaning Up eDirectory,”](#) on page 156.
- 3 Reconfigure the replica server.
For more information, see [Section 13.2, “Reconfiguring the eDirectory Server through YaST,”](#) on page 157.
- 4 On successful reconfiguration of the replica server, continue with [Section 13.3, “Reconfiguring OES Services,”](#) on page 157.

13.1.3 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 \(http://www.novell.com/documentation/crt33/crtadmin/data/a2ebop8.html#acea8nu\)](http://www.novell.com/documentation/crt33/crtadmin/data/a2ebop8.html#acea8nu) and [Creating a Server Certificate Object \(http://www.novell.com/documentation/crt33/crtadmin/data/fbgcdhec.html\)](http://www.novell.com/documentation/crt33/crtadmin/data/fbgcdhec.html) in the *Novell Certificate Server 3.3.2 Administration Guide*.
- 2 Clean up the server.
For more information, see [Section 13.1.4, “Cleaning Up eDirectory,”](#) on page 156.
- 3 Reconfigure the server.
For more information, see [Section 13.2, “Reconfiguring the eDirectory Server through YaST,”](#) on page 157.
- 4 After successfully reconfiguring the server, continue with [Section 13.3, “Reconfiguring OES Services,”](#) on page 157.

13.1.4 Cleaning Up eDirectory

- 1 Use iManager to delete all the objects from the eDirectory tree.
- 2 Stop the ndsd daemon:

```
rcnstd 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 \(https://www.netiq.com/documentation/edirectory-9/edir_admin/data/agm7hq7.html#agwk3ga\)](https://www.netiq.com/documentation/edirectory-9/edir_admin/data/agm7hq7.html#agwk3ga) in the *NetIQ eDirectory 9.0 Administration Guide*.

13.2 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 13.1.1, "Before You Clean Up," on page 155](#):
 - 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**.

13.3 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 13-1 Services

Starts by Default	Start Manually	Re-create Objects	Reconfigure
SMS	Novell AFP	NSS	Novell DNS
LUM	NCS	NCP	Novell CIFS
NRM	Novell DHCP		SLP
Novell FTP	iPrint		NMAS
Groupwise	Novell Samba		
DST	NetStorage		
DFS	iManager		
WBFM	NTP		
Welcome Page			
VLOG Utility			

- ♦ [Section 13.3.1, “Re-creating eDirectory Objects,” on page 158](#)
- ♦ [Section 13.3.2, “Services Requiring Reconfiguration,” on page 159](#)
- ♦ [Section 13.3.3, “Manually Starting Services,” on page 160](#)

13.3.1 Re-creating eDirectory Objects

- ♦ [“Novell Storage Service” on page 158](#)
- ♦ [“NCP Server” on page 159](#)

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 [OES 2018: NSS File System Administration Guide for Linux](#).

- Re-create the eDirectory object for each NSS pool:
 - Start NSSMU by entering the following command at the command prompt:


```
nssmu
```
 - Select **Pools** and press Enter to list all the NSS pools.
 - Select a pool that needs to be re-created and press F4.
 - Select **Yes** when you are prompted to delete and re-create an NDS pool object.
The selected NDS pool object is re-created.
 - Repeat from [Step 1c](#) for each NDS pool object that needs to be re-created.
- Re-create the eDirectory object for each NSS volume:
 - In NSSMU, select **Volumes** and press Enter to list all the NSS volumes.
 - Select a volume and press F4.
 - 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 [OES 2018: 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
```

13.3.2 Services Requiring Reconfiguration

- ♦ [“Novell DNS” on page 159](#)
- ♦ [“Novell CIFS” on page 159](#)
- ♦ [“Novell SLP” on page 160](#)
- ♦ [“NMAS” on page 160](#)

Novell 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 Novell 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 Novell DNS reconfiguration.

Novell 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 Novell 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 **Novell 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.

Novell SLP

The SLP DA IP address is added during eDirectory reconfiguration. See [Step 6e on page 157](#) for more information.

NMAS

The NMAS login method is selected during eDirectory reconfiguration. See [Step 7 on page 157](#) for more information.

13.3.3 Manually Starting Services

Re-create the eDirectory objects of NCP and NSS volumes as directed in the [Section 13.3.1, “Re-creating eDirectory Objects,” on page 158](#), before starting the following services manually:

Table 13-2 *Manually Restarting Services*

Service Name	Starting the Service
Novell AFP	<code>rcnovell-afptcpd start</code> or <code>systemctl start novell-afptcpd.service</code>
Novell Cluster Service (NCS)	<code>rcnovell-ncs start</code> or <code>systemctl start novell-ncs.service</code>
NetStorage	<code>rcnovell-xregd start</code> or <code>systemctl start novell-xregd.service</code>
	<code>rcnovell-xsrvd start</code> or <code>systemctl start novell-xsrvd.service</code>
Samba	Start the Samba service through iManager
Novell DHCP	<code>rcnovell-dhcpd start</code> or <code>systemctl start novell-dhcpd.service</code>
iPrint	<code>rcnovell-ipsmd start</code> or <code>systemctl start novell-ipsmd.service</code>
	<code>rcnovell-idsd start</code> or <code>systemctl start novell-idsd.service</code>

Service Name	Starting the Service
iManager	<p>After completing the OES installation, if iManager is installed without using YaST, Tomcat must be started manually.</p> <pre>systemctl start novell-tomcat6.service</pre> <pre>rcapache2 restart</pre>
NTP	<pre>rcntpd restart</pre>

14 Security Considerations

This section includes issues that you should consider when installing and configuring a Open Enterprise Server (OES) 2018 Linux server.

- ♦ [Section 14.1, “Access to the Server During an Installation or Upgrade,” on page 163](#)
- ♦ [Section 14.2, “Remote Installations Through VNC,” on page 163](#)
- ♦ [Section 14.3, “Improperly Configured LDAP Servers,” on page 163](#)

14.1 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.

14.2 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 12 SP2 Deployment Guide](https://www.suse.com/documentation/sles-12/book_sle_deployment/data/sec_deployment_remoteinst_scenario.html) (https://www.suse.com/documentation/sles-12/book_sle_deployment/data/sec_deployment_remoteinst_scenario.html).

14.3 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](#).

15 Troubleshooting

This section presents information on troubleshooting the OES installation and configuration.

- [Section 15.1, “PID File Unavailable Message,” on page 165](#)
- [Section 15.2, “systemctl kill Not Supported,” on page 166](#)
- [Section 15.3, “Executing kinit Command Fails in .LOCAL Domain,” on page 166](#)
- [Section 15.4, “The OES Service Pattern Icons are not Displayed and OES Patterns are not in the Proper Order,” on page 166](#)
- [Section 15.5, “Package Conflict Occurs During the Add-On Install of Novell FTP Pattern,” on page 166](#)
- [Section 15.6, “The Health Check Option for CA is not Displayed in iManager,” on page 168](#)
- [Section 15.7, “Deleting the Existing eDirectory Objects when Reinstalling the OES Server or Reconfiguring the eDirectory,” on page 169](#)
- [Section 15.8, “Problem In Assigning IP Address For autoinst.xml-based Installations,” on page 169](#)
- [Section 15.9, “eDirectory Restart Results in an Error Message on a Non-DSfW Server,” on page 169](#)
- [Section 15.10, “The DEFAULT SLP Scope Gets added to the slp.conf File During an Upgrade to OES 2018,” on page 170](#)
- [Section 15.11, “The change_proxy_pwd.sh Script Fails to Synchronize Password,” on page 170](#)
- [Section 15.12, “OES Installation Fails Due to Encrypted OES Media URL in the autoinst.xml File,” on page 171](#)
- [Section 15.13, “Installing or Upgrading to OES 2018 using AutoYaST Creates the OES Repository Name Using Random Characters,” on page 171](#)
- [Section 15.14, “Verification of the Container Object Fails During the AD Domain Join Process,” on page 171](#)
- [Section 15.15, “Timing Issues for OES on Xen,” on page 172](#)

15.1 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.

15.2 **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`.

15.3 **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. The mDNS is installed in OES as part of AFP installation. 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]"

15.4 **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.

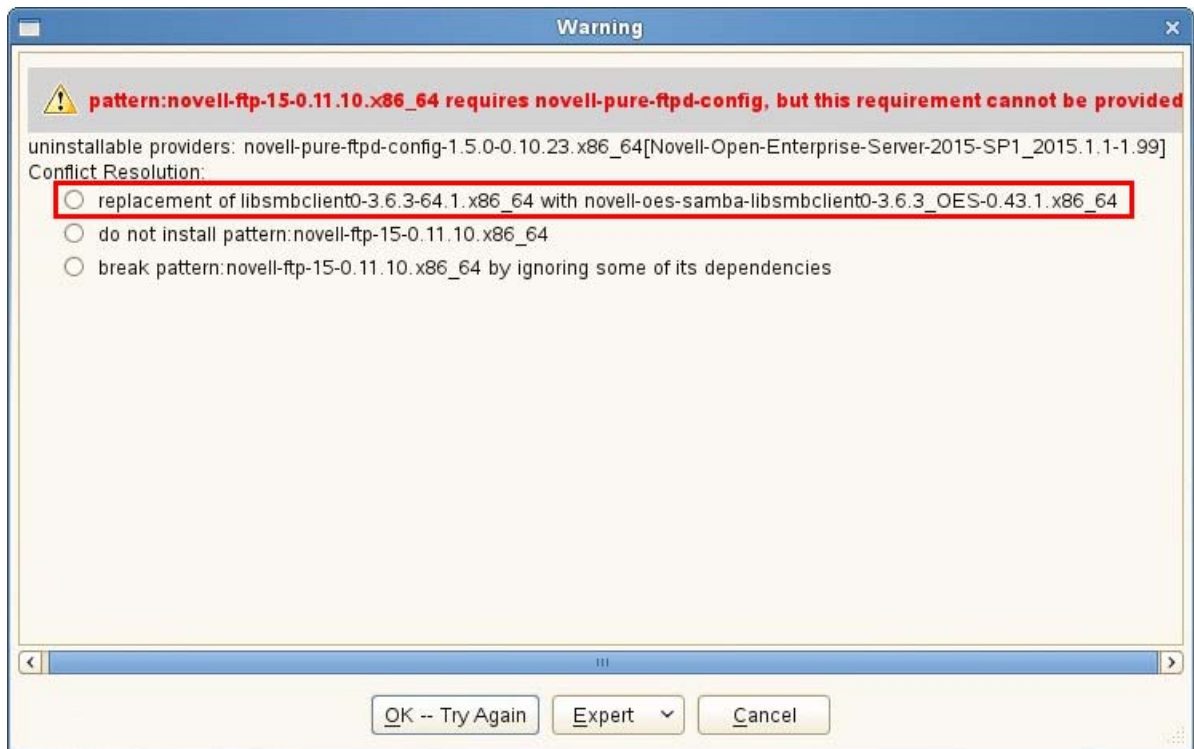
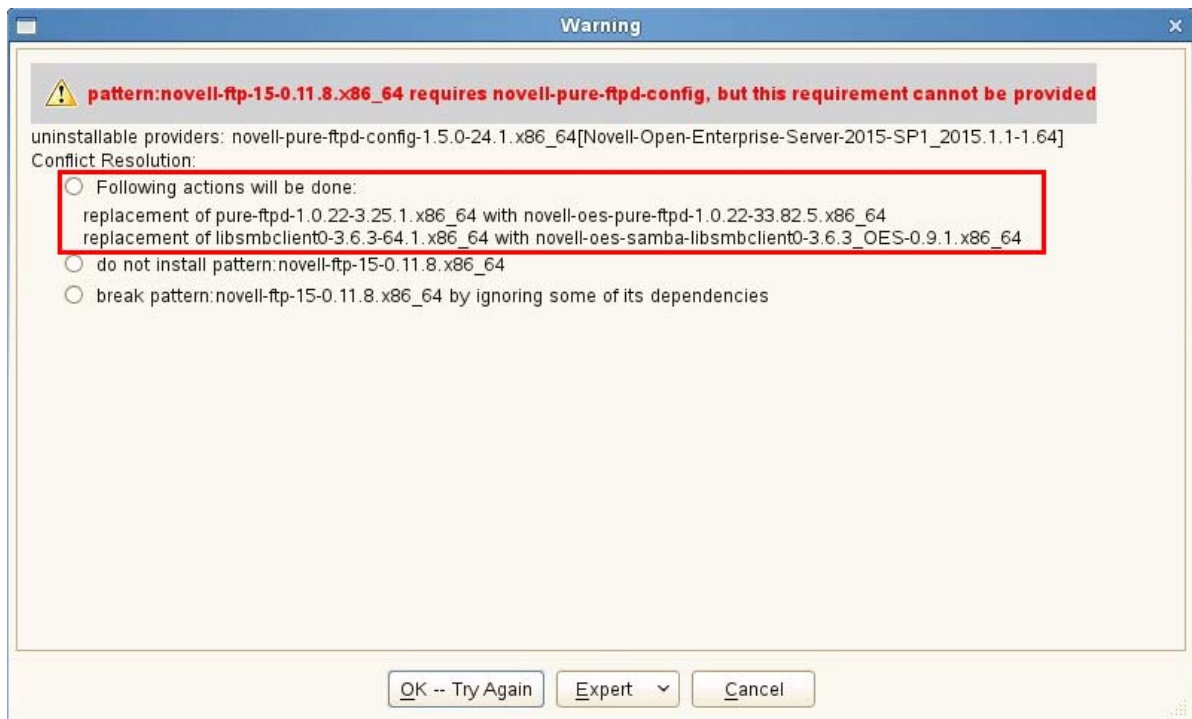
```
zypper mr -p <priority> <OES_medaname>
```

For example, `zypper mr -p 98 OES_media`

15.5 **Package Conflict Occurs During the Add-On Install of Novell FTP Pattern**

If you select **Patterns > OES Services > Novell FTP** during the Add-On installation, a package conflict warning message is displayed.

The following warning messages might be displayed during the Add-On install.

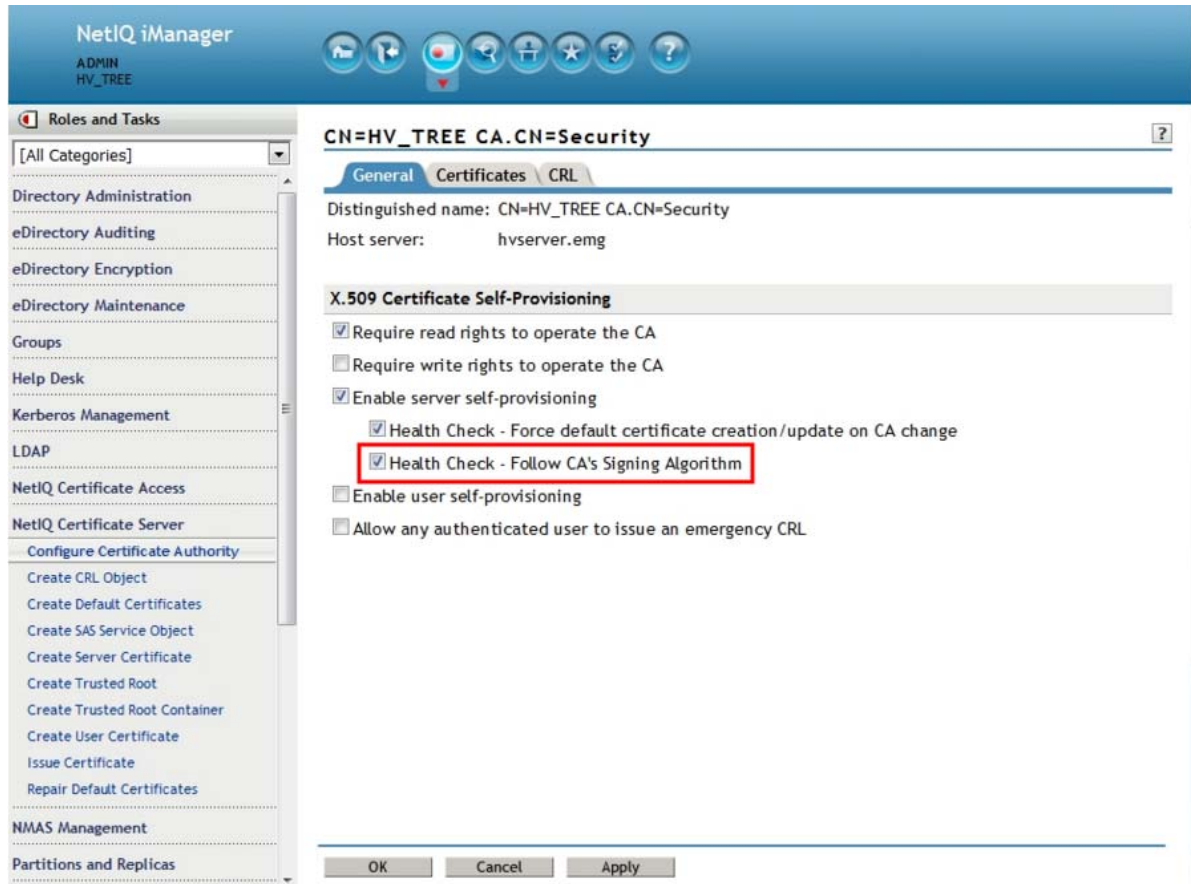


To resolve this issue, do the following:

1. Select the replacement option highlighted in both the warning messages.
2. Click **OK -- Try Again**.

15.6 The Health Check Option for CA is not Displayed in iManager

The **Health Check - Follow CA's Signing Algorithm** check box is not displayed in iManager, **NetIQ Certificate Server > Configure Certificate Authority > General** tab. This might randomly occur on applying the January 2016 patch.



To resolve this issue, do the following:

1. Delete all the contents of the `/var/opt/novell/tomcat6/work/Catalina/localhost/nps` folder.

Ensure to delete the JSPs files that are cached in the `nps` folder.

2. Restart Tomcat.

```
systemctl restart novell-tomcat6.service
```

The option will now be displayed in iManager.

15.7 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)

15.8 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.

15.9 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 (IPCEExternal, 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.

15.10 The DEFAULT SLP Scope Gets added to the slp.conf File During an Upgrade to OES 2018

When you upgrade an OES server that is configured as an SLP DA to OES 2018, 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.

15.11 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.

15.12 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 NCC 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.novell.com/
repo/$RCE/OES11-SP2-Pool/sle-11-x86_64]]></media_url>
    <product>Open_Enterprise_Server</product>
    <product_dir></product_dir>
  </listentry>
</add_on_products>
```

15.13 Installing or Upgrading to OES 2018 using AutoYaST Creates the OES Repository Name Using Random Characters

Before you start the installation of OES 2018, 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/OES2018/GMC/x86_64]]></
media_url>
    <product>Open_Enterprise_Server</product>
    <product_dir></product_dir>
    <name>MyOES_name</name>
    <alias>MyOES_alias</alias>
  </listentry>
</add_on_products>
```

15.14 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.

15.15 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 12 SP2 or OES 2018). Ensure that you understand and follow the instructions in [Xen Virtual Machine Clock Settings](#) in the [Virtualization Guide](#).

A

OES 2018 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) 2018 components follow Linux Standard Base (LSB) requirements regarding file location. Efforts to do this are detailed here.

- ♦ [Section A.1, “General Rules,” on page 173](#)
- ♦ [Section A.2, “Exceptions,” on page 174](#)

A.1 General Rules

Where possible, product design has followed these rules:

- ♦ **/opt/novell:** Contains all static data in the following standard subdirectories.

<code>/opt/novell/bin</code>	Executable files that are used by multiple products or are intended to be executed by an end user.
<code>/opt/novell/service/sbin</code>	Executable files that are used only by a product and are not executed by an end user.
<code>/opt/novell/lib</code>	Shared libraries that are used by multiple products and shared or static libraries that are part of an SDK.
<code>/opt/novell/include</code>	Header files for SDKs, typically in a product subdirectory.
<code>/opt/novell/lib64</code>	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 novell 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 12 SP2 AutoYaST \(https://www.suse.com/documentation/sles-12/book_autoyast/data/book_autoyast.html\)](https://www.suse.com/documentation/sles-12/book_autoyast/data/book_autoyast.html).

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 141](#) section. All the passwords stored in the `autoinst.xml` file will be in clear text.

- [Section B.1, “edirectory,” on page 175](#)
- [Section B.2, “imanager,” on page 181](#)
- [Section B.3, “iprint,” on page 181](#)
- [Section B.4, “ncpserver,” on page 181](#)
- [Section B.5, “ncs,” on page 182](#)
- [Section B.6, “netstorage,” on page 183](#)
- [Section B.7, “novell-afp,” on page 184](#)
- [Section B.8, “novell-cifs,” on page 185](#)
- [Section B.9, “novell-dhcp,” on page 186](#)
- [Section B.10, “novell-dns,” on page 187](#)
- [Section B.11, “novell-lum,” on page 189](#)
- [Section B.12, “novell-samba,” on page 190](#)
- [Section B.13, “nss,” on page 192](#)
- [Section B.14, “oes-cis,” on page 192](#)
- [Section B.15, “oes-ldap,” on page 193](#)
- [Section B.16, “sms,” on page 194](#)
- [Section B.17, “novell-nssad,” on page 195](#)

B.1 edirectory

Attribute Name	Description
<code>ocs_store</code>	Always set this to 'yes' so that the proxy credentials are stored in OCS. Example: <code><ocs_store>yes</ocs_store></code>

Attribute Name	Description
cert_mutual	<p>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.</p> <p>Example: <cert_mutual>no</cert_mutual></p>
challenge_response	<p>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.</p> <p>Example: <challenge_response>yes</challenge_response></p>
create_server_object	<p>Set this to 'Yes' when you want to create a DNS server object.</p> <p>Example: <create_server_object>yes</create_server_object></p>
dib_location	<p>Specify the path of the nds database.</p> <p>Example: <dib_location>/var/opt/novell/eDirectory/data/dib</dib_location></p>
digest_md5	<p>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.</p> <p>Example: <digest_md5>no</digest_md5></p>
domain_name	<p>Specify the DSfW DNS domain name. The value of this tag and xad_domain_name tag should be same.</p> <p>Example: <domain_name>acme.com</domain_name></p>
existing_dns_ip	<p>Specify the existing DNS server IP address.</p> <p>Example: <existing_dns_ip>192.168.1.1</existing_dns_ip></p>
group_context	<p>Specify the DNS DHCP group object context.</p> <p>Example: <group_context>ou=OESystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</group_context></p>
host_name	<p>Specify the host name of the current server where the installation is being done.</p> <p>Example: <host_name>acme-208</host_name></p>
http_port	<p>Specify the HTTP port of the eDirectory server where the installation is being done.</p> <p>Example: <http_port config:type="integer">8028</http_port></p>
https_port	<p>Specify the HTTPS port of the current eDirectory server.</p> <p>Example: <https_port config:type="integer">8030</https_port></p>
install_secretstore	<p>Set to 'yes' when you want to install the secret store.</p> <p>Example: <install_secretstore>yes</install_secretstore></p>

Attribute Name	Description
install_universalstore	<p>Set to 'yes' when you want to install the universal store.</p> <p>Example: <install_universalstore>no</install_universalstore></p>
ldap_basedn	<p>Specify the DNSs server's CN name. This is required only in case of DSfW server.</p> <p>Example: <ldap_basedn>ou=OESSystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</ldap_basedn></p>
ldap_server	<p>Specify the IP address of the DNS LDAP server.</p> <p>Example: <ldap_server>192.168.1.1</ldap_server></p>
locator_context	<p>Specify the DNS locator object context where the DNS servers or zones are present.</p> <p>Example: <locator_context>ou=OESSystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</locator_context></p>
migrate_option	<p>Always set this to 'no' as the migrate NKDC realm to DSfW domain is discontinued.</p> <p>Example: <migrate_option>no</migrate_option></p>
nds	<p>Set to this to 'yes' when you want to use the NDS login method that provides secure password challenge-response user authentication to eDirectory.</p> <p>Example: <nds>yes</nds></p>
ntp_server_list	<p>Specify reliable NTP servers IP addresses.</p> <p>Example: <ntp_server_list config:type="list"> <listentry>192.168.1.5</listentry> </ntp_server_list></p>
overwrite_cert_files	<p>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).</p> <p>Example: <overwrite_cert_files>yes</overwrite_cert_files></p>
replica_server	<p>Specify the IP address of the master eDirectory server.</p> <p>Example: <replica_server>192.168.1.5</replica_server></p>
runtime_admin	<p>Specify the common proxy user context of the DNS.</p> <p>Example: <runtime_admin>cn=OESCommonProxy_host1,ou=OESSystemObjects,dc=acme,dc=com</runtime_admin></p>
runtime_admin_password	<p>Specify the common proxy DNS password.</p> <p>Example: <runtime_admin_password>SAM23#\$</runtime_admin_password></p>

Attribute Name	Description
sasl_gssapi	<p>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.</p> <p>Example: <sasl_gssapi>no</sasl_gssapi></p>
server_context	<p>Specify the eDirectory server context where there eDirectory server object needs to be created.</p> <p>Example: <server_context>ou=wdc,o=acme</server_context></p>
server_object	<p>Specify the eDirectory server object name that has the object name and context.</p> <p>Example: <server_object>cn=DNS_edir-acme-208,ou=OESystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</server_object></p>
simple_password	<p>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.</p> <p>Example: <simple_password>no</simple_password></p>
slp_backup	<p>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).</p> <p>Example: <slp_backup>yes</slp_backup></p>
slp_backup_interval	<p>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.</p> <p>Example: <slp_backup_interval>900</slp_backup_interval></p>
slp_da	<p>Specify the list of IP addresses of the SLP Directory Agents.</p> <p>Example:</p> <pre><slp_da config:type="list"> <listentry>198.162.1.1</listentry> </slp_da></pre>
slp_dasync	<p>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.</p> <p>Example: <slp_dasync>no</slp_dasync></p>
Slp_mode	<p>Specify the SLP mode to multicast, da, or da_server. By default, it is set to multicast.</p> <p>Example: <slp_mode>da</slp_mode></p>

Attribute Name	Description
slp_scopes	<p>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.</p> <p>Example: <slp_scopes>DEFAULT</slp_scopes></p>
tls_for_simple_binds	<p>Set this to 'yes' when you require TLS for SIMPLE binds with passwords.</p> <p>Example: <tls_for_simple_binds>yes</tls_for_simple_binds></p>
tree_type	<p>Specify the type of eDirectory tree: new or existing.</p> <p>Example: <tree_type>new</tree_type></p>
use_secure_port	<p>Set this to 'yes' when you want the DNS to use the secure port for communication in an DSfW environment.</p> <p>Example: <use_secure_port>yes</use_secure_port></p>
xad_admin_password	<p>Specify the DSfW domain administrator password.</p> <p>Example: <xad_admin_password>SAM23#\$</xad_admin_password></p>
xad_config_dns	<p>Set this to 'yes' when you want to configure this domain controller also as a DNS server.</p> <p>Example: <xad_config_dns>yes</xad_config_dns></p>
xad_convert_existing_container	<p>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.</p> <p>Example: <xad_convert_existing_container>no</xad_convert_existing_container></p>
xad_domain_name	<p>Specify the DSfW DNS domain name. The value of this tag and domain_name tag should be same.</p> <p>Example: <xad_domain_name>acme.com</xad_domain_name></p>
xad_domain_type	<p>Specify the DSfW domain type: forest, domain or controller.</p> <ul style="list-style-type: none"> ♦ 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. <p>Exmple: <xad_domain_type>forest</xad_domain_type></p>
xad_existing_container	<p>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'.</p> <p>Example: <xad_existing_container>ou=OESSystemObjects, o=acme</xad_existing_container></p>
xad_forest_root	<p>Specify the forest root domain name in the DSfW forest.</p> <p>Example: <xad_forest_root>acme.com</xad_forest_root></p>

Attribute Name	Description
xad_ldap_admin_context	<p>Specify the eDirectory tree admin context.</p> <p>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.</p> <pre><xad_ldap_admin_context>cn=admin,ou=admins,o=acme</xad_ldap_admin_context></pre> <p>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></p> <p>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></p>
xad_ldap_admin_password	<p>Specify the eDirectory tree administrator password.</p> <p>Example: <xad_ldap_admin_password>SAM23#\$</xad_ldap_admin_password></p>
xad_netbios	<p>Specify the NetBIOS name of the DSfW domain.</p> <p>Example: <xad_netbios>EXAMPLE</xad_netbios></p>
xad_parent_domain	<p>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></p>
xad_parent_domain_address	<p>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></p>
xad_parent_domain_admin_context	<p>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></p>
xad_parent_domain_admin_password	<p>Specify the immediate DSfW parent domain's administrator password.</p> <p>Example: <xad_parent_domain_admin_password>SAM23#\$</xad_parent_domain_admin_password></p>
xad_replicate_partitions	<p>Always set this to 'yes'. This indicates that the replicas of the configuration and schema partitions will be added to the local domain controller.</p> <p>Example: <xad_replicate_partitions>yes</xad_replicate_partitions></p>
xad_retain_policies	<p>Set this to 'yes' when you want to retain the existing NMA universal password policies.</p> <p>Example: <xad_retain_policies>yes</xad_retain_policies></p> <p>NOTE: If set to 'no', the DSfW configuration will override the existing password policies if any.</p>

Attribute Name	Description
xad_service_configured	<p>Always specify this value to 'yes' when you want to configure DSfW.</p> <p>Example: <xad_service_configured>yes</xad_service_configured></p>
xad_site_name	<p>Specify the site name to which this domain controller should be associated with. Otherwise the default value should be 'Default-First-Site-Name'.</p> <p>Example: <xad_site_name>Default-First-Site-Name</xad_site_name></p>
xad_wins_server	<p>Specify 'yes' when you want to configure the DSfW domain controller as WINS server.</p> <p>Example: <xad_wins_server></xad_wins_server></p> <p>NOTE: Only one domain controller in a DSfW domain should be designated as WINS server.</p>

B.2 imanager

Attribute Name	Description
configure_now	<p>Set this to 'true' always in AutoYaST based installations.</p> <p>Example: <configure_now config:type="boolean">true</configure_now></p>
install_plugins	<p>Set to 'yes' to install all the iManager npms.</p> <p>Example: <install_plugins>yes</install_plugins></p>

B.3 iprint

Attribute Name	Description
ldap_server	<p>Specify the IP or DNS name of the LDAP server that is used for authentication by iPrint during secure printing and management operations.</p> <p>Example: <ldap_server>192.168.1.2</ldap_server></p>
top_context	<p>Specify the context (and its entire subtree) that is used to find the user during authentication.</p> <p>Example: <top_context>o=acme</top_context></p>

B.4 ncpserver

Attribute Name	Description
configure_now	<p>Set this to 'true' always as NCP is a must for OES to work.</p> <p>Example: <configure_now config:type="boolean">true</configure_now></p>

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	<p>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.</p> <p>Example: <cluster_dn>cn=clus134,ou=ncs,o=acme</cluster_dn></p>
cluster_ip	<p>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.</p> <p>Example: <cluster_ip>192.168.1.1</cluster_ip></p>
config_type	<p>Specify whether the node is being configured for a "New Cluster" or an "Existing Cluster".</p> <p>Example: <config_type>Existing Cluster</config_type></p>
ldap_servers	<p>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.</p> <p>Example: <ldap_servers>192.168.1.1,192.168.1.2</ldap_servers></p>
proxy_user	<p>Specify the NCS proxy user credentials--the username and password. The NCS proxy user is the user identity used by the NCS daemon to communicate with eDirectory (the LDAP server). In the proxy_user tag, specify the Fully Distinguished name of the NCS proxy user in comma-delimited typeful format. This might be one of the following users:</p> <ul style="list-style-type: none">♦ OES Common Proxy User: This requires that the OES Common Proxy User is enabled in eDirectory for this server. This is the default choice. The OES Common Proxy user for each server has a different identity in eDirectory. If you specify the OES Common Proxy User, each nodes' OES Common Proxy User is automatically added to the NCS Management group for the cluster <clustername>_MGT_GRP in the cluster container.♦ LDAP Admin User: The LDAP Admin user that you used when you configured NCS on this server. This is the secondary default choice.♦ Another Admin User: An existing LUM-enabled administrator user that you created to use as the NCS proxy user. <p>Example: <proxy_user>cn=OESCommonProxy_avalon,o=acme</proxy_user></p>

Attribute Name	Description
proxy_user_password	<p>Specify the password for the specified user. If you specify the OES Common Proxy User, you should use the same password that you used in the eDirectory settings for this user.</p> <p>Example: <proxy_user_password>SAM23#\$</proxy_user_password></p>
sbd_dev	<p>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.</p> <p>Example: <sbd_dev>sdc</sbd_dev></p>
sbd_dev2	<p>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.</p> <p>Example: <sbd_dev2>sdd</sbd_dev2></p>
sbd_size	<p>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.</p> <p>Example:</p> <ul style="list-style-type: none"> ♦ 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	<p>Specify the hostname of the server where you are configuring.</p> <p>Example: NCS.<server_name>avalon</server_name></p>
start	<p>Specify whether to start NCS automatically after the configuration completes by specifying a start value of "Now". To start the NCS manually, specify "Later".</p> <p>Example: <start>Now</start></p>

B.6 netstorage

Attribute Name	Description
xtier_proxy_context	<p>Specify the LDAP context for xtier proxy user.</p> <p>Example: <xtier_proxy_context>cn=OESCommonProxy_wdc34,o=acme</xtier_proxy_context></p>
xtier_proxy_password	<p>Specify the password for xtier proxy user.</p> <p>Example: <xtier_proxy_password>SAM23#\$</xtier_proxy_password></p>

Attribute Name	Description
xtier_server	Specify the IP address of the xtier server. Example: <xtier_server>192.168.1.1</xtier_server>
xtier_users_context	Specify the LDAP context for the xtier users. Example: <xtier_users_context>o=acme</xtier_users_context>

B.7 novell-afp

Attribute Name	Description
afp_ldap_server	Specify the IP address of the eDirectory LDAP server that AFP connects to at install time. Example: <afp_ldap_server>192.168.1.2</afp_ldap_server>
afp_proxy_user	Specify the AFP proxy user FQDN in LDAP format used for searching AFP users in eDirectory at login time. Example: <afp_proxy_user>cn=afpproxy,o=acme</afp_proxy_user> If you are using common proxy for AFP, mention the user FQDN of the common proxy as shown below. <afp_proxy_user>cn=OESCommonProxy_localhostname,o=acme</afp_proxy_user>
afp_proxy_user_password	Specify the password for the AFP proxy user. Example: <proxy_user_password>SAM23#\$</proxy_user_password>
afp_edir_contexts	Specify a list of AFP User contexts that are searched when the AFP user enters a user name for authentication. The server searches through each context in the list until it finds the user object. Example: <afp_edir_contexts config:type="list"> <listentry>ou=wdc,o=acme</listentry> <listentry>ou=prv,o=acme</listentry> </afp_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 AFP proxy user to grant search rights over user contexts. This is required for subtree search feature. Example: <usercontext_rights>yes</usercontext_rights>

B.8 novell-cifs

Attribute Name	Description
ldap_server	<p>Specify the IP address of the eDirectory LDAP server that AFP connects to at install time.</p> <p>Example: <code><ldap_server>192.168.1.2</ldap_server></code></p>
cifs_ldap_port	<p>Specify the LDAP port of the server specified in the ldap_server tag.</p> <p>Example: <code><cifs_ldap_port config:type="integer">636</cifs_ldap_port></code></p>
use_secure_port	<p>Set this to 'yes' if the LDAP port is mentioned in cifs_ldap_port tag is a secure port, else no.</p> <p>Example: <code><use_secure_port>yes</use_secure_port></code></p>
proxy_user	<p>Specify the CIFS proxy user FQDN in LDAP format used for searching CIFS users in eDirectory at log time.</p> <p>Example: <code><proxy_user>cn=cifsproxy,o=acme</proxy_user></code></p> <p>If you are using common proxy for AFP, mention the user FQDN of the common proxy as shown below.</p> <p><code><proxy_user>cn=OESCommonProxy_localhostname,o=acme</proxy_user></code></p>
create_new_user	<p>Set this value to 'yes' when you want to create a CIFS proxy user at install time.</p> <p>Example: <code><create_new_user>no</create_new_user></code></p>
proxy_user_password	<p>Specify the password for the CIFS proxy user.</p> <p>Example: <code><proxy_user_password>SAM23#\$</proxy_user_password></code></p>
use_ocs_for_credentials	<p>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.</p> <p>Example: <code><use_ocs_for_credentials>yes</use_ocs_for_credentials></code></p>
server_context	<p>Specify the context of the local NCP server.</p> <p>Example: <code><server_context>ou=wdc,o=acme</server_context></code></p>
cifs_edir_contexts	<p>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.</p> <p>Example:</p> <pre><cifs_edir_contexts config:type="list"> <listentry>ou=wdc,o=acme</listentry> <listentry>ou=prv,o=acme</listentry> </cifs_edir_contexts></pre>
subtree_search	<p>Set this value to 'yes' when you want to enable the subtree search feature.</p> <p>Example: <code><subtree_search>no</subtree_search></code></p>

Attribute Name	Description
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.9 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: <ul style="list-style-type: none"> ◆ 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 config:type="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	<p>Specify static or dynamic.</p> <ul style="list-style-type: none"> ♦ 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. <p>Example: <ldap_method>static</ldap_method></p>
ldap_referrals	<p>Set this to 'yes' when you want to enable LDAP referral.</p> <p>Example: <ldap_referrals>yes</ldap_referrals></p>
ldap_server	<p>Specify the IP address of the LDAP server.</p> <p>Example: <ldap_server>192.168.1.2</ldap_server></p>
ldap_user	<p>Specify the DHCP common proxy user context.</p> <p>Example: <ldap_user>cn=OESCommonProxy_host1,ou=OESystemObjects,dc=sales,dc=wdc,dc=acme,dc=com</ldap_user></p>
ldap_user_password	<p>Specify the common proxy DHCP password.</p> <p>Example: <ldap_user_password>SAM23#\$</ldap_user_password></p>
locator_context	<p>Specify the DHCP locator context.</p> <p>Example: <locator_context>ou=OESystemObjects.dc=sales.dc=wdc.dc=acme.dc=com</locator_context></p>
server_context	<p>Specify the DHCP server context.</p> <p>Example: <server_context>ou=OESystemObjects.dc=sales.dc=wdc.dc=acme.dc=com</server_context></p>
server_object_name	<p>Specify the DHCP server object name.</p> <p>Example: <server_object_name>DHCP_acme-208</server_object_name></p>
use_secure_port	<p>Set it to 'yes' when you want to use a secure port for communicating with the LDAP server.</p> <p>Example: <use_secure_port>yes</use_secure_port></p>
use_secure_port_config	<p>Set this to 'yes' when you want to use a secure port for DHCP configuration.</p> <p>Example: <use_secure_port_config>yes</use_secure_port_config></p>

B.10 novell-dns

Attribute Name	Description
ocs_store	<p>Set this to 'yes' when you want to store the DNS proxy credentials in OCS.</p> <p>Example: <ocs_store>yes</ocs_store></p>

Attribute Name	Description
create_server_object	Set this to 'yes' when you want to create DNS server object. Example: <create_server_object>no</create_server_object>
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>
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>
runtime_admin_password	Specify the common proxy DNS password. Example: <runtime_admin_password>SAM23#\$</runtime_admin_password>
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.11 novell-lum

Attribute Name	Description
admin_group	<p>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.</p> <p>Example: <admin_group>cn=admingroup,o=acme</admin_group></p>
alternate_ldap_servers_list1	<p>Specify a list of the IP addresses of the local eDirectory servers that you are connecting to.</p> <p>Example:</p> <pre><alternate_ldap_servers_list1 config:type="list"> <listentry>192.168.1.1</listentry> <listentry>192.168.1.2</listentry> </alternate_ldap_servers_list1></pre>
alternate_ldap_servers_list2	<p>Specify one or more external LDAP servers. Ensure to specify the IP address of a valid LDAP server that is up and running.</p> <p>Example:</p> <pre><alternate_ldap_servers_list2 config:type="list"> <listentry>192.168.1.3</listentry> <listentry>192.168.1.4</listentry> </alternate_ldap_servers_list2></pre>
ldap_server	<p>Specify the IP address of the LDAP server.</p> <p>Example: <ldap_server>164.99.100.38</ldap_server></p>

Attribute Name	Description
lum_enabled_services	<p>If you want the LUM-enabled users to access the following services, set the value of those tags to 'yes': FTP, GDM, Gnome Screensaver, Gnomesu pam, Login, SFCB, SSHD and SU.</p> <p>Example:</p> <pre> <lum_enabled_services> <ftp>no</ftp> <gdm>no</gdm> <gnome-screensaver>no</gnome-screensaver> <gnomesu-pam>no</gnomesu-pam> <login>no</login> <sfcg>yes</sfcg> <sshd>no</sshd> <su>no</su> </lum_enabled_services> </pre>
partition_root	<p>Specify the context where UNIX Config Object will be created.</p> <p>Example: <partition_root>o=acme</partition_root></p>
proxy_user	<p>Specify the LUM proxy user FQDN, in LDAP format, used for searching LUM users in eDirectory at login time.</p> <p>Example: <proxy_user>cn=ldapsproxy,o=acme</proxy_user></p> <p>If you are using common proxy for LUM, mention the user FQDN of the common proxy as shown below.</p> <pre> <proxy_user>cn=OESCommonProxy_localhostname,o=acme</ proxy_user> </pre>
proxy_user_password	<p>Specify the password for the LUM proxy user.</p> <p>Example: <proxy_user_password>SAM23#\$</proxy_user_password></p>
restrict_access	<p>Set it to 'yes' if you want to restrict read and write access for users other than the owners of the home directories.</p> <p>Example: <restrict_access>yes</restrict_access></p>
ws_context	<p>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.</p> <p>Example: <ws_context>o=novell</ws_context></p>

B.12 novell-samba

NOTE: Novell Samba must not be installed on the same server as Novell CIFS.

Attribute Name	Description
ldap_server	<p>Specify the IP address (in IPv4 format) of the LDAP server in the tree that you want Novell Samba to use for LDAP (eDirectory) communications.</p> <p>Example: <ldap_server>192.168.1.1</ldap_server></p>
netbios_name	<p>Specify the NetBIOS name to use for the virtual Samba server. Use the hostname and append "-W" to it. The total length of the NetBIOS name can be up to 15 characters (this is a NetBIOS restriction). This means the hostname of the server should be limited to 13 characters. If you specify a longer hostname, it is truncated from the left to create the NetBIOS name. As a result, iManager won't be able to find the associated server and group objects.</p> <p>Example: <netbios_name>avalon-W</netbios_name></p>
proxy_user_context	<p>Specify the credentials of an eDirectory user that has rights to search the tree for Samba users. Specify the Fully Distinguished name of the Samba Proxy User in comma-delimited typeful format. (Typeful format means that the FDN uses the abbreviations of the LDAP object types (such as cn=, ou=, o=, dc= and so on).) Each of the intermediate containers must already exist. The proxy user name must be unique in that path. If the user identity does not yet exist, specify that it is new by specifying "Yes" as the value for the <proxy_user_is_new> tag.</p> <ul style="list-style-type: none"> ♦ If you specify a new user that does not already exist in eDirectory, the user is created, LUM-enabled, and assigned the necessary rights and the password you specify here. ♦ If you specify an existing eDirectory user, it is assumed that you have already LUM-enabled the user and assigned the user the necessary rights, and no modification is made to the user. Specify the user's password. <p>Example (new user):</p> <ul style="list-style-type: none"> ♦ <proxy_user_context>cn=acme-208-sambaProxy,cn=Users,dc=labs,dc=wdc,dc=acme,dc=com</proxy_user_context> ♦ <proxy_user_is_new>yes</proxy_user_is_new> ♦ <proxy_user_password>SAM23#\$</proxy_user_password>
proxy_user_is_new	
proxy_user_password	
user_context	<p>Specify the Base Context of the Samba users who are accessing data on this server via Samba/CIFS. Specify the context in dot-delimited typeful format. This Base Context is usually set to the eDirectory container where the tree admin user is created. Typically, this is the Organization (O) container, and users are created in Organizational Unit (OU) containers beneath the O container. If your Samba users are (or will be) located in the same container as admin or in a subcontainer of that container, you should specify the o= container. Otherwise, specify a container in your tree that is at the same level or above the container where the Samba users will be created.</p> <p>Example: <user_context>cn=Users,dc=labs,dc=wdc,dc=acme,dc=com</user_context></p>

B.13 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 config:type="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 config:type="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.14 oes-cis

Attribute Name	Description
admin_context	Specify the LDAP distinguished name of the CIS server administrator. Example: <admin_context>cn=admin,o=acme</admin_context>
admin_password	Specify the CIS administrator password. Example: <admin_password>SAM23#\$</admin_password>
ca_certificate	Specify the path of the eDirectory Certificate Authority (CA) file. Example: <ca_certificate>/etc/opt/novell/certs/SScert.pem</ca_certificate>
cluster_enable	Set this to 'yes' to allow the CIS server to be part of a cluster resource. Example: <cluster_enable>yes</cluster_enable>
context	Specify the LDAP distinguished name (DN) of the container object under which the NCP server objects of the OES server reside that can connect to the CIS server. Example: <context>o=acme</context>
database_password	Specify the MariaDB password. Example: <database_password>SAM23#\$</database_password>
database_uri	Specify the IP address of the database server. Example: <database_uri>192.168.1.2:3306</database_uri>

Attribute Name	Description
database_username	Specify the MariaDB username. Example: <database_username>User</database_username>
elastic_search_secure_mode	Set this to 'yes' to enable secure communication. Example: <elastic_search_secure_mode>yes</elastic_search_secure_mode>
elastic_search_uri	Specify the IP address of the Elasticsearch server. Example: <elastic_search_uri>192.168.1.2:9400</elastic_search_uri>
gateway_address	Specify the IP address of the local host where CIS server is configured. Example: <gateway_address>192.168.1.2</gateway_address>
kafka_secure_mode	Set this to 'yes' to enable secure communication. Example: <kafka_secure_mode>yes</kafka_secure_mode>
kafka_uri	Specify the IP address of the Kafka server. Example: <kafka_uri>192.168.1.2:9092</kafka_uri>
ldap_server	Specify the IP address of the LDAP server. Example: <ldap_server>192.168.1.2:636</ldap_server>
server_certificate	Specify the path of the server certificate file issued by the eDirectory CA. Example: <server_certificate>/etc/ssl/servercerts/servercert.pem</server_certificate>
server_key	Specify the path of the key file associated with the server certificate Example: <server_key>/etc/ssl/servercerts/serverkey.pem</server_key>
zookeeper_uri	Specify the IP address of ZooKeeper. Example: <zookeeper_uri>192.168.1.2:2181</zookeeper_uri>

B.15 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 Administrator password. Example: <admin_password>SAM23#\$</admin_password>

Attribute Name	Description
ldap_servers	<p>Specify the details of the list of LDAP servers in a particular tree.</p> <ul style="list-style-type: none"> ♦ 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. <p>Example:</p> <pre><ldap_servers config:type="list"> <listentry> <ip_address>164.99.100.38</ip_address> <ldap_port config:type="integer">389</ldap_port> <ldaps_port config:type="integer">636</ldaps_port> </listentry> </ldap_servers></pre>
proxy_context	<p>Specify the FQDN of the default common proxy user.</p> <p>Example: <proxy_context>cn=OESCommonProxy_wdcsales34,o=acme</proxy_context></p>
proxy_password	<p>Specify the common proxy user password.</p> <p>Example: <proxy_password>SAM23#\$</proxy_password></p>
tree_name	<p>Specify the eDirectory tree name.</p> <p>Example: <tree_name>sales_wdc_acme</tree_name></p>
use_common_proxy	<p>Set it to 'yes' when you want to use the default common proxy.</p> <p>Example: <use_common_proxy>yes</use_common_proxy></p>
xad_tree_admin_context	<p>Specify domain tree admin FQDN context.</p> <p>Example: <xad_tree_admin_context></xad_tree_admin_context></p>
xad_tree_admin_password	<p>Specify domain tree admin password.</p> <p>Example: <xad_tree_admin_password>SAM23#\$</xad_tree_admin_password></p>

B.16 sms

Attribute Name	Description
ldap_server	<p>Specify the IP address of the eDirectory LDAP server that SMS connects to at install time.</p> <p>Example: <ldap_server>192.168.1.2</ldap_server></p>

B.17 novell-nssad

Attribute Name	Description
ad_context	<p>Specify Active Directory Context.</p> <p>Example: <ad_context>CN=Computers</ad_context></p>
ad_uid_generate_mode	<p>If you want NIT to generate UIDs specify this to 'yes'.</p> <p>Example: <ad_uid_generate_mode>no</ad_uid_generate_mode></p>
admin_name	<p>Specify the Active Directory administrator user name or an equivalent user that can be used for the AD domain join operation.</p> <p>Example: <admin_name>Administrator</admin_name></p>
admin_password	<p>Specify the administrator password.</p> <p>Example: <admin_password>pa55word</admin_password></p>
domain_admin_group	<p>Specify the Active Directory domain admin group name.</p> <p>Example: <domain_admin_group>Domain Admins</domain_admin_group></p>
domain_name	<p>Specify the Active Directory domain name.</p> <p>Example: <domain_name>ACME.COM</domain_name></p>
nit_end_range	<p>Specify the UID end range. This value has to be an integer always.</p> <p>Example: <nit_end_range config:type="integer">200000</nit_end_range></p>
nit_start_range	<p>Specify the UID start range. This value has to be an integer always.</p> <p>Example: <nit_start_range config:type="integer">100000</nit_start_range></p>
pre_created_object	<p>If you want to use any pre-created objects, set this to 'yes'.</p> <p>Example: <pre_created_object>no</pre_created_object></p>



Importing New Build Keys to the Keyring

Beginning with January 2019, the OES update repository and OES packages are signed with 4096 bit key. The **oes-build-key** patch adds the 4096-bit key to the rpm keyring of the OES server. When this patch is applied, it displays a message to import the new keys to the keyring in the following scenarios:

New Installation of OES 2018

Post January 2019, if a new OES 2018 server is installed, the message to import the keys is displayed during the registration of the server to the customer center or to the patch update server.

Upgrading to OES 2018

Post January 2019, if an earlier version of OES is upgraded to the OES 2018 server, the message to import the keys is displayed during the registration of the server to the customer center or to the patch update server.

Updating the OES 2018 server

On patching the OES 2018 server post January 2019, the message to import the keys is displayed.

NOTE: If a message to import the keys with the following details is displayed in any other scenario, you can go ahead and accept it to continue with the process:

Key ID: 044ADAE04881839
Key Fingerprint: F5E39B083E1A8D7CEFF584C4044ADAE04881839

To import the new keys to the keyring and continue with the process:

- ♦ **In zypper method:** When New repository or package signing key received: is displayed, choose the option **trust** always by entering "a" in the command line.

Figure C-1 Sample prompt in zypper

```
Retrieving repository 'OES2018-Updates' metadata -----[\\]

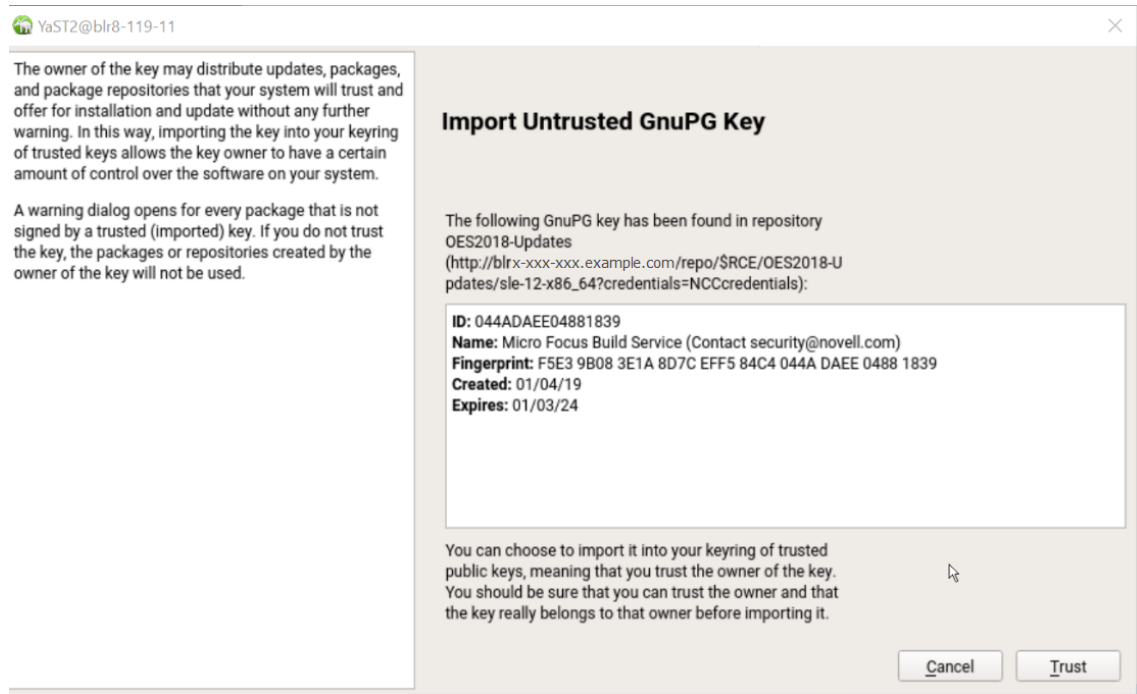
New repository or package signing key received:

Repository:      OES2018-Updates
Key Name:        Micro Focus Build Service (Contact security@novell.com) <OESBuild@novell.com>
Key Fingerprint: F5E39B08 3E1A8D7C EFF584C4 044ADAE0 4881839
Key Created:     Fri Jan  4 17:56:53 2019
Key Expires:     Wed Jan  3 17:56:53 2024
Rpm Name:        gpg-pubkey-04881839-5c2f510d

Do you want to reject the key, trust temporarily, or trust always? [r/t/a/? shows all options] (r): a
```

- ♦ **In YaST method:** Click **Trust**.

Figure C-2 Sample prompt in YaST



- ♦ If SUSE manager is used for managing OES patches, to avoid errors while mirroring, you must perform the following:
 1. Run the command `spacewalk-repo-sync -c <any-OES-channels>`.
For example, `spacewalk-repo-sync -c oes2018-pool-x86_64`.
 2. When prompted to import the keys, import the keys and continue.

See also, [TID 7023680 \(https://support.microfocus.com/kb/doc.php?id=7023680\)](https://support.microfocus.com/kb/doc.php?id=7023680)