Open Enterprise Server 11 SP3

Installation Guide

July 2016

Novell.

Legal Notices

Contents

About This Guide

This guide describes how to install, upgrade, and update Novell Open Enterprise Server (OES) 11 SP3. 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.

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 Novell 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 11 SP3: Installation Guide* is available at the Open Enterprise Server 11 documentation website.

Additional Documentation

For more information about	See
Planning and implementing OES 11 SP3	*OES 11 SP3: Planning and Implementation Guide*
Migration from and coexistence with other products	"Different Migration Tools" in the *OES 11 SP3: Migration Tool Administration Guide*
Installing OES 11 SP3 on a Xen Virtual Host Server	Chapter 10, "Installing, Upgrading, or Updating OES on a VM," on page 191
SLES 11 SP4 Deployment details	*SUSE LINUX Enterprise Server 11 SP4 Deployment* Guide (https://www.suse.com/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html)
SLES 11 SP4 Administration details	*SUSE LINUX Enterprise Server 11 SP4 Administration Guide* (https://www.suse.com/documentation/sles11/book_sle_admin/data/book_sle_admin.html)

1 What’s New or Changed in the OES Install

This section describes enhancements to Install for Novell Open Enterprise Server (OES) 11:

- Section 1.1, “What’s New (OES 11 SP3),” on page 11
- Section 1.2, “What’s New (January 2016 eDirectory 8.8 SP8 Patch 6 Hot Patch 1),” on page 11
- Section 1.3, “What’s New (OES 11 SP2),” on page 11
- Section 1.4, “What’s New or Changed in OES 11 SP1 Install,” on page 12
- Section 1.5, “What’s New or Changed in OES 11 Install,” on page 12

1.1 What’s New (OES 11 SP3)

In addition to bug fixes, the following enhancement or change is provided in OES 11 SP3:

Upgrade from OES 11 SP3 to OES 2015 SP1 can be done remotely using `zypper` command. For more information, see Manual Upgrade from OES 11 SP3 to OES 2015 SP1 Using Zypper in OES 11 SP3: Installation Guide.

1.2 What’s New (January 2016 eDirectory 8.8 SP8 Patch 6 Hot Patch 1)

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. This hot patch contains bug fixes that enables the servers to easily switch to SHA-2 signed certificates.

1.3 What’s New (OES 11 SP2)

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

Express Install

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

Cloning Post Install or Upgrade

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

NCPFS Package Dependency Replaced with Novell Client for Linux

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

Reconfiguring iManager

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

Interoperability with Partnering Vendors

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

1.4 What's New or Changed in OES 11 SP1 Install

- Unattended upgrade from OES 2 or OES 11 to OES 11 SP1 has been enhanced and has undergone some changes. For more information, see "Using AutoYaST for an OES 11 SP3 Upgrade" in the *OES 11 SP3: Installation Guide*.
- A single integrated ISO to install or upgrade OES 11 SP1 is now available. This ISO contains both SLES 11 SP2 and OES 11 SP1.
- Channel upgrade support is added in OES 11 SP1. It supports upgrade from OES 11 to OES 11 SP1.

1.5 What's New or Changed in OES 11 Install

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

2 Preparing to Install OES 11 SP3

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 11 SP3,” on page 20
- Section 2.6, “Deciding What Patterns to Install,” on page 25
- Section 2.7, “Obtaining OES 11 SP3 Software,” on page 35
- Section 2.8, “Preparing Physical Media for a New Server Installation or an Upgrade,” on page 35
- Section 2.9, “Setting Up a Network Installation Source,” on page 36
- Section 2.10, “Always Install OES as an Add-On Product,” on page 40
- Section 2.11, “Install Only One Server at a Time,” on page 40
- Section 2.12, “What's Next,” on page 41

2.1 Before You Install

Before you install Novell Open Enterprise Server 11 SP3 (OES 11 SP3), review the following information:

- ❐ “Planning Your OES 11 SP3 Implementation” in the *OES 11 SP3: Planning and Implementation Guide*
- ❐ “Before You Install” in the *OES 11 SP3: Readme*

2.2 Meeting All Server Software and Hardware Requirements

Before installing OES 11 SP3, 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 part of the OES 11 SP3 installation, you install SUSE Linux Enterprise Server 11 SP4.

IMPORTANT: OES 11 SP3 services were developed and tested on a default and fully-patched SLES 11 SP4 server base.

As you install OES 11 SP3, do not change any of the SLES 11 SP4 Base Technologies package selections, such as Java support. Doing so can cause various problems, such as the installation failing or one or more OES 11 SP3 services not working properly.

If you are installing on an existing SLES 11 SP4 server, be sure to verify that all of the default SLES 11 SP4 components are installed before attempting to install OES 11 SP3 services.

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 11 SP3 is an add-on product to SLES 11 SP4; it only runs on x86_64. Other processors that are supported by SLES 11 SP4, such as Itanium (IA64) and Intel x86(IA32), are not supported for running OES services. **NOTE:** Services such as iManager, SMS, and NRM run in 32-bit mode on a 64-bit platform.
Memory	2 GB of RAM	2 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	7 GB of available, unpartitioned disk space	10 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
Hard Drive	20 GB	
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 11 SP3: 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 2.5.4, "Extending the Schema," on page 23.

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

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

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

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

2.4 Installing and Configuring OES as a Subcontainer Administrator

IMPORTANT: The information explained in Section 2.3, "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	1. In iManager, click **View Objects** > the **Browse** tab, then browse to and select the subcontainer administrator. 2. Click the administrator object, then select **Modify Trustees**. 3. Click the **Assigned Rights** link for the administrator object. 4. For the [All Attributes Rights] property, select **Supervisor**, then click **Done > OK**.
Supervisor right to the container where the server will be installed	1. Browse to the container where the subcontainer administrator will install the server. 2. Click the container object and select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] and [Entry rights] properties, select **Supervisor**, then click **Done > OK > OK**.
Supervisor right to the W0 object located inside the KAP object in the Security container	1. Browse to **Security > KAP**. 2. In KAP, click **W0** and select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] and [Entry rights] properties, select **Supervisor**, then click **Done > OK > OK**.
Supervisor right to the Security container when installing the NMAS login methods	If the subcontainer administrator will install the NMAS login methods: 1. Browse to and select **Security**. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] and [Entry rights] properties, select **Supervisor**, then click **Done > OK > OK**.

Rights Needed	Sample Steps to Follow
Create right to its own container (context)	1. Browse to and select the container where you created the subcontainer administrator. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [Entry Rights] property, select **Create**, then click **Done > OK > OK**.
Create right to the container where the UNIX Config object is located	1. Browse to and select the container where the UNIX Config object is located. By default, this is the Organization object. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [Entry Rights] property, select **Create**, then click **Done > OK > OK**.
Read right to the Security container object for the eDirectory tree	This is not needed if the Supervisor right was assigned because of NMAS. If the subcontainer administrator won't install the NMAS login methods, do the following: 1. Browse to and select **Security**. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] property, select **Read**, then click **Done > OK > OK**.
Read right to the NDSPKI:Private Key attribute on the Organizational CA object (located in the Security container)	1. Browse to **Security** and select the Organizational CA object. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. Click the **Add Property** button. 6. Select **NDSPKI:Private Key**, then click **OK**. The Read right should be automatically assigned. 7. Click **Done > OK > OK**.
Read and Write rights to the UNIX Config object	1. Browse to and select the UNIX Config object. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] property, select **Write** (**Read** is already selected), then click **Done > OK > OK**.

Rights Needed	Sample Steps to Follow
Write right to the [All Attribute Rights] property for the admingroup object	1. Browse to and select the admingroup object. 2. Select **Modify Trustees**. 3. Click **Add Trustee**, browse to and select the subcontainer administrator, then click **OK**. 4. Click the **Assigned Rights** link for the administrator object. 5. For the [All Attributes Rights] property, select **Write** (**Compare and Read** are already selected), then click **Done > OK > OK**.

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

- For DNS, see “eDirectory Permissions ” in the *OES 11 SP3: Novell DNS/DHCP Services for Linux Administration Guide*.
- For DHCP, see “eDirectory Permissions ” in the *OES 11 SP3: Novell 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	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	1. On the Novell 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	1. On the Novell 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	1. On the Novell 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 114.

2.5 Preparing eDirectory for OES 11 SP3

- Section 2.5.1, "If Your Directory Tree Is Earlier than eDirectory 8.6," on page 20
- Section 2.5.2, "If Your LDAP Server Is Running NetWare 6.5 SP2 or Earlier," on page 21
- Section 2.5.3, "If Your Tree Has Ever Contained an OES 1 Linux Server with LUM and NSS Installed," on page 21
- Section 2.5.4, "Extending the Schema," on page 23

2.5.1 If Your Directory Tree Is Earlier than eDirectory 8.6

If you are installing an OES 11 SP3 server into an eDirectory tree that is earlier than eDirectory 8.6, do the following before installing your first OES server in an existing NetWare tree:

1 Extend the schema by using Deployment Manager. See "Schema Update" in the *NW65 SP8: Installation Guide*.

2 Ensure that the schema is synchronized throughout the tree from root:

2a Enter the following commands at the System Console prompt of the NetWare server with the Master of root:

```
set DSTRACE=on
set DSTRACE=nodebug
set DSTRACE=+Schema
set DSTRACE=*SSD
set DSTRACE=*SSA
```

2b Toggle to the Directory Services screen and look for the message `All Processed = YES`.

2c On each server that holds a Master of a partition, enter the following commands at the System Console prompt:

```
set DSTRACE=off
set DSTRACE=nodebug
set DSTRACE=+Schema
set DSTRACE=*SS
```

2d Toggle to the Directory Services screen and look for the message `All Processed = YES`.

2.5.2 If Your LDAP Server Is Running NetWare 6.5 SP2 or Earlier

If you are installing into an eDirectory tree that is using a NetWare server to supply LDAP, you should upgrade the LDAP server that the OES installation will communicate with to NetWare 6.5 SP3 or later. A server running NetWare 6.5 SP2 or earlier will probably abend.

2.5.3 If Your Tree Has Ever Contained an OES 1 Linux Server with LUM and NSS Installed

Having NSS volumes on OES servers requires certain system-level modifications, most of which are automatic. For more information, see "System User and Group Management in OES 11 SP3" in the *OES 11 SP3: Planning and Implementation Guide*.

- "NetStorage, X-Tier, and Their System Users" on page 21
- "An NSS Complication" on page 21
- "eDirectory Solves the Basic Problem" on page 22
- "The OES 2 Solution: Standardizing the UIDs on all OES servers" on page 22

NetStorage, X-Tier, and Their System Users

By default, certain OES services, such as NetStorage, rely on a background Novell service named X-Tier.

To run on an OES server, X-Tier requires two system-created users (named `novlxsrvd` and `novlxregd`) and one system-created group that the users belong to (named `novlxtier`).

An NSS Complication

The two X-Tier users mentioned above, and their group, are created on the local system when X-Tier is installed. For example, they are created when you install NetStorage, and their respective UIDs and GID are used to establish ownership of the service's directories and files.

For NetStorage to run, these X-Tier users and group must be able to read data on all volume types that exist on the OES server.

As long as the server has only Linux traditional file systems, such as Ext3 and Reiser, NetStorage runs well.

However, if the server has NSS volumes, an additional requirement is introduced. NSS data can only be accessed by eDirectory users. Consequently, the local X-Tier users can't access NSS data, and NetStorage can't run properly.

eDirectory Solves the Basic Problem

When NSS volumes are created on the server, the two X-Tier system users and their group are moved to eDirectory and enabled for Linux User Management (LUM). See “Linux User Management: Access to Linux for eDirectory Users” in the *OES 11 SP3: Planning and Implementation Guide*.

After the move to eDirectory, they can function as both eDirectory and POSIX users, and they no longer exist on the local system.

The OES 2 Solution: Standardizing the UIDs on all OES servers

If your eDirectory tree has ever contained an OES 1 Linux server with NSS and LUM installed, do the following on each server (including OES 2) that has NSS and LUM installed:

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

```
id novlxregd
```

```
id novlxsrvd
```

The standardized X-Tier IDs are UID 81 for `novlxregd`, UID 82 for `novlxsrvd`, and GID 81 for `novlxtier`.

2 If you see the following ID information, the X-Tier IDs are standardized and you can move to the next server:

```
uid=81(novlxregd) gid=81(novlxtier) groups=81(novlxtier)
uid=82(novlxsrvd) gid=81(novlxtier) groups=81(novlxtier),8(www)
```

If you see different IDs than those listed above, such as 101, 102, 103, etc., record the numbers for both X-Tier users and the novlxtier group. You need these IDs to standardize the IDs on the server.

3 Download the following script file:

- fix_xtier_ids.sh (http://www.novell.com/documentation/oes2/scripts/fix_xtier_ids.sh)

4 Customize the template file by replacing the variables in angle brackets (<>) as follows:

- **<server_name>:** The name of the server object in eDirectory.

  Replace this variable with the server name.

  For example, if the server name is myserver, replace <server_name> with myserver so that the line in the settings section of the script reads

  ```
  server=myserver
  ```

- **<context>:** The context of the X-Tier user and group objects.

  Replace this variable with the fully distinguished name of the context where the objects reside.

  For example, if the objects are an Organizational Unit object named servers, replace ou=servers,o=company.

- **<admin fdn>:** The full context of an eDirectory admin user, such as the Tree Admin, who has rights to modify the X-Tier user and group objects.

  Replace this variable with the admin name and context, specified with comma-delimited syntax.

  For example, if the tree admin is in an Organization container named company, the full context is cn=admin,o=company and the line in the settings section of the script reads

  ```
  admin_fdn="cn=admin,o=company"
  ```

- **<novlxregd_uid>:** The UID that the system assigned to the local novlxregd user. It might or might not be the same on each server, depending on whether the `nssid.sh` script ran successfully.

  Replace this variable with the UID reported for the novlxregd user on this server as listed when you ran the commands in Step 1 on page 22.

  In the example script, the original UID is 101. It is changed to 81 in the third line of the script. The sixth line changes the UID on all of the files and directories on the server that are owned by the novlxregd user from 101 to 81.
- **<novlxsrvd_uid>:** The UID that the system assigned to the local novlxsrvd user. It might not be the same on each server, depending on whether the `nssid.sh` script ran successfully.

  Replace this variable with the UID reported for the novlxsrvd user on this server as listed when you ran the commands in Step 1 on page 22.

  In the example script, the original UID is 103. It is changed to 82 in the fourth line of the script. The seventh line changes the UID on all of the files and directories on the server that are owned by the `novlxsrvd` user from 103 to 82.
- **<novlxtier_gid>:** The GID that the system assigned to the local novlxtier group. It might not be the same on each server, depending on whether the `nssid.sh` script ran successfully.

  Replace this variable with the GID reported for the novlxtier group on this server as listed when you ran the commands in Step 1 on page 22.

  In the example script, the original GID is 101. It is changed to 81 in the second line of the script. The sixth and seventh lines change the GID from 101 to 81 for all of the files and directories on the server that are owned by the `novlxtier` group.

5 Make the script executable and run it on the server.

IMPORTANT: Changes to the X-Tier files are not reported on the terminal.

Error messages are reported, but you can safely ignore them. The script scans the entire file system, and some files are locked because the system is running.

6 Repeat from Step 1 for each of the other servers in the same context.

2.5.4 Extending the Schema

An eDirectory tree must have its schema extended to accommodate OES 11 servers and services as explained in the following sections:

- “Who Can Extend the Schema?” on page 23
- “Which OES 11 SP3 Services Require a Schema Extension?” on page 24
- “Extending the Schema While Installing OES 11 SP3” on page 24
- “Using the YaST Plug-In to Extend the Schema” on page 25
- “Extending the Schema for Novell Cluster Services” on page 25

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 11 SP3 Services Require a Schema Extension?

The following service schema extensions are included with OES 11 SP3.

A single asterisk (*) indicates a service that is either required for OES 11 SP3 servers or for the default services that are installed on every OES 11 SP3 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 25).

- 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 iFolder
- Novell Domain Services for Windows
- NetIQ NMAS*
- Novell CIFS
- Novell Clustering

  Novell Cluster Services requires you to extend the schema manually. Follow the instructions in "Installing, Configuring, and Repairing Novell Cluster Services" in the *OES 11 SP3: Novell Cluster Services for Linux Administration Guide*.
- Novell Remote Manager
- Novell Samba

Extending the Schema While Installing OES 11 SP3

The simplest way to extend the schema for OES 11 SP3 servers is to have a tree admin install the first OES 11 SP3 server and the first instance of each OES 11 SP3 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 11 SP3 server or the first instance of an OES 11 SP3 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 11 SP3 server running in another tree
- Install a fully patched SLES 11 SP4 server, then install OES 11 SP3 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 11 SP3 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 11 SP3 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 11 SP3: Novell Cluster Services for Linux Administration Guide*.

2.6 Deciding What Patterns to Install

A default SLES 11 SP4 installation has the following base technology, graphical environment, and primary function patterns selected for installation. With the exception explained in the two Important notes below, you can accept or deselect these patterns and install additional patterns as desired.

Table 2-4 *Standard SLES 11 SP4 Installation Patterns*

Pattern	Description
Server Base System	Consists of all packages that are common to all Novell SUSE Linux Enterprise products. Also provides a Linux Standard Base 3.0 compliant runtime environment. This pattern is selected for installation by default. **IMPORTANT:** You must either install this pattern or the Common Code Base pattern.
Common Code Base	The largest system. It includes all packages available with SUSE Linux, except those that would result in dependency conflicts. **IMPORTANT:** You must either install this pattern or the Server Base System pattern.
Novell AppArmor	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 `root`) to thwart attempted exploits and even zero-day attacks. AppArmor offers an advanced tool set that largely automates the development of per-program application security so that no new expertise is required. This pattern is selected for installation by default.
GNOME Desktop Environment	The GNOME desktop environment is an intuitive and attractive desktop for users. The GNOME development platform is an extensive framework for building applications that integrate into the rest of the desktop. This pattern is selected for installation by default.
X Window System	In continuous use for over 20 years, the X Window System provides the only standard platform-independent networked graphical window system bridging the heterogeneous platforms in today's enterprise: from network servers to desktops, thin clients, laptops, and handhelds, independent of operating system and hardware. This pattern is selected for installation by default.
Print Server	Sets up a print server to host print queues so that they can be accessed by other computers on the same network, including machines running Microsoft Windows operating systems. The print server can accept print jobs from client computers and direct them to locally attached printers or to network printers. LPD, CUPS, and SMB print servers and queues are supported. This pattern is selected for installation by default.

The OES add-on installation includes the following OES Services patterns:

Table 2-5 *OES Services Pattern Descriptions*

Pattern	Description
Novell AFP	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. This pattern selects and installs these services: ◆ Novell Backup / Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Storage Services (NSS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) ◆ Novell NCP Server This pattern cannot be installed on the same server as these services: ◆ Novell Domain Services for Windows
Novell Archive and Version Services	Novell Archive and Version Services systematically captures and stores versions of your network files in an archive database, on a schedule that you determine. Users can search for a previous version of a file and quickly restore it. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) ◆ Novell Storage Services (NSS) ◆ Novell NCP Server This pattern cannot be installed on the same server as these services: ◆ Novell Domain Services for Windows
Novell Backup/Storage Management Services (SMS)	The Novell backup infrastructure (called Storage Management Services or SMS) provides backup applications with the framework to develop a complete backup and restore solution. SMS helps back up file systems (such as NSS) or application data (such as data from GroupWise) on NetWare and SUSE Linux Enterprise Server (SLES) to removable tape media or other media for off-site storage. It provides a single consistent interface for all file systems and applications across NetWare and SLES. This pattern selects and installs these services: ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)

Pattern	Description
Novell CIFS	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 11 SP3 server. CIFS allows read and write access from multiple client systems simultaneously. This pattern selects and installs these services: ◆ Novell Backup / Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Storage Services (NSS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) ◆ Novell NCP Server This pattern cannot be installed on the same server as these services: ◆ Novell Domain Services for Windows ◆ Novell Samba
Novell Cluster Services (NCS)	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. 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. 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. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) This pattern cannot be installed on the same server with these services: ◆ High Availability

Pattern	Description
Novell DHCP	Novell DHCP (Dynamic Host Configuration Protocol) uses eDirectory to provide configuration parameters to client computers and integrate them into a network. The eDirectory integration lets you have centralized administration and management of DHCP servers across the enterprise and lets you set up DHCP subnet replication via NetIQ eDirectory. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell DNS	Novell DNS uses NetIQ eDirectory to deliver information associated with domain names, in particular the IP address. This eDirectory integration lets you have centralized administration and management of DNS servers across the enterprise and lets you set up a DNS zone via NetIQ eDirectory. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)

Pattern	Description
Novell Domain Services for Windows	Novell Domain Services for Windows provides seamless cross-authentication capabilities between Windows/Active Directory and Novell OES 11 SP3 servers. It is a suite of integrated technologies that removes the need for the Novell Client 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. This pattern selects and installs these services: ◆ 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 This pattern cannot be installed on the same server as these services: ◆ Novell Samba ◆ Novell CIFS ◆ Novell AFP ◆ Novell Archive and Version Services ◆ Novell FTP ◆ Novell iFolder ◆ Novell NetStorage ◆ Novell Pre-Migration Server ◆ Novell QuickFinder
NetIQ eDirectory	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. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ OpenLDAP

Pattern	Description
Novell FTP	Novell FTP (File Transfer Protocol) is integrated with NetIQ eDirectory so that users can securely transfer files to and from OES volumes. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ Novell Domain Services for Windows
Novell iFolder	Novell iFolder 3.9 is a simple and secure storage solution that increases user productivity by enabling users to back up, access, and manage their personal files from anywhere, at any time. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ Novell Domain Services for Windows
Novell iManager	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. iManager provides the following benefits: ◆ 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 This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)

Pattern	Description
Novell iPrint	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. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ CUPS
Novell Linux User Management (LUM)	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. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Remote Manager (NRM)
Novell NCP Server / Dynamic Storage Technology	Novell NCP Server for Linux enables support for login scripts, mapping drives to OES servers, and other services commonly associated with Novell Client access. This means that Windows users with the Novell Client installed can be seamlessly transitioned to file services on OES. 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. Services included with NCP (NetWare Core Protocol) are file access, file locking, security, tracking of resource allocation, event notification, synchronization with other servers, connection and communication, print services and queue management, and network management. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)

Pattern	Description
Novell NetStorage	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. 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. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell iManager ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ Novell Domain Services for Windows
Novell Pre-Migration Server	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. 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 11 SP3: Migration Tool Administration Guide*. You should also select and install all the services that you plan to migrate from the other server. Services that are not installed on this server prior to the migration cannot be migrated. This pattern selects and installs these services: ◆ Novell Backup / Storage Management Services (SMS) ◆ NetIQ eDirectory (without a replica) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ Novell Domain Services for Windows

Pattern	Description
Novell QuickFinder	QuickFinder lets your users find the information they're looking for on any of your public and private Web sites, your partners' sites, and any number of additional Web sites across the Internet or internal file servers, all from a single search form on your Web page. You can easily modify the look and feel of any of the sample search results pages to match your corporate design. You can create full-text indexes of HTML, XML, PDF, Word, OpenOffice.org, and many other document formats in almost any language with the QuickFinder Unicode indexing engine. You can configure and maintain your indexes remotely from anywhere on the network with the QuickFinder Web-based administration module. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ Novell Domain Services for Windows
Novell Remote Manager (NRM)	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. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM)
Novell Samba	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. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ Novell CIFS ◆ Novell Domain Services for Windows

Pattern	Description
Novell Storage Services (NSS)	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. Unique features include visibility, trustee access control model, multiple simultaneous namespace support, native Unicode, user and directory quotas, rich file attributes, multiple data stream support, event file lists, and a file salvage subsystem. NSS volumes are cross-compatible between kernels. You can mount a non-encrypted NSS data volume on either the Linux or NetWare kernel and move it between them. In a clustered SAN, volumes can fail over between kernels, allowing for full data and file system feature preservation when migrating data to Linux. This pattern selects and installs these services: ◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell NCP Server ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) This pattern cannot be installed on the same server as these services: ◆ Xen Virtual Machine Host Server

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 52 and “Installing or Configuring OES 11 SP3 on an Existing Server” on page 109.

2.7 Obtaining OES 11 SP3 Software

For information on obtaining OES software, see “Getting and Preparing OES 11 SP3 Software” in the *OES 11 SP3: 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 11 SP3 Software” in the *OES 11 SP3: 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	◆ SLES 11 SP4 DVD ISO (SLES-11-SP4-DVD-x86_64-GM-DVD1.iso) ◆ OES 11 SP3 DVD ISO (OES11-SP3-addon-x86_64-DVD1.iso) ◆ Integrated ISO that has SLES 11 SP4 and OES 11 SP3 (OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso) These ISO files can be downloaded from the OES 11 SP3 download page (http://download.novell.com/Download?buildid=f0yiBfaHAZM~).

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 36
- Section 2.9.2, “NetWare as a Network Installation Source Server,” on page 38
- Section 2.9.3, “Windows as a Network Installation Source Server,” on page 40

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 11 SP4 Deployment Guide*
- The instructions in the following sections:
  - “Requirements” on page 37
  - “Procedure” on page 37
  - “NFS Protocol Configuration” on page 37
  - “FTP Protocol Configuration” on page 38
  - “HTTP Protocol Configuration” on page 38

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, Windows, or NetWare 6.5.

- ❒ 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 11 SP3 Software" in the *OES 11 SP3: 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 37
   - "FTP Protocol Configuration" on page 38
   - "HTTP Protocol Configuration" on page 38

   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 11 SP4 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 35.

   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 11 SP3 Installation" on page 44 or "Upgrading to OES 11 SP3" on page 115.

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 11 SP4.

If you choose to use this protocol:

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

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

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

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

   For example,

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

3. Restart Apache.

2.9.2 NetWare as a Network Installation Source Server

Complete the instructions in this section to set up an Open Enterprise Server (OES) 11 SP3 installation source on an existing NetWare 6.5 SP8 server.

- “Prerequisites” on page 39
- “Copy the Files and Mount Them as NSS Volumes” on page 39
- “Create the Boot DVDs” on page 40

Prerequisites

You need the following:

- ❒ A NetWare 6.5 SP8 server accessible on the network where you plan to install the OES 11 SP3 servers with the following:
  - 6 GB free disk space on the server
  - The Apache Web Server for NetWare installed and running
- ❒ The following ISO image files from Novell:

Image File	Purpose
`SLES-11-SP4-DVD-x86_64-GM-DVD1.iso`	Boot DVD for x86_64 (64-bit) SLES 11 SP4 installations
`OES11-SP3-addon-x86_64-DVD1.iso`	Install source for x86_64 (64-bit) OES 11 SP3 services
`OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso`	Integrated ISO has the install source for x86_64 (64-bit) SLES 11 SP4 and OES 11 SP3. It is also acts as the boot DVD using SLES 11 SP4.

For information on downloading these image files, see the Novell Open Enterprise Server 11 Download Instructions (http://www.novell.com/documentation/oes11/esd/di_oes11.html).

Copy the Files and Mount Them as NSS Volumes

The following instructions create unrestricted access to OES 11 SP3 installation files on a NetWare server on your network. Restricting access to the installation files requires additional configuration through Apache Manager or requires manual editing of the Apache configuration files.

For more information on restricting access, see information about the Options, Order, Deny, Allow, and other directives on the Apache.org Web Site (http://httpd.apache.org/docs-2.0/mod/directives.html).

To provide unrestricted access to the OES 11 SP3 image files:

1 Create a directory at the root of a server volume with at least 6 GB of free disk space.

For example, you might create a directory named `OES11_INSTALL` in a volume named `TOOLS`.

2 Restrict access to the directory to only those administrators who copy image files to the directory.

This is important because if someone attempts to access these files after they are mounted as NSS volumes, the volumes are immediately dismounted and are no longer available.

3 Copy the DVD image files listed in "Prerequisites" on page 39 to the directory you just created.

4 At the server console, mount each image file as an NSS volume:

4a Enter the following command:

```
nss /MountImageVolume=volume:directory/filename.iso
```

Replace *volume* with the NSS volume name, *directory* with the directory you created in Step 1, and *filename* with the name of the ISO file.

For example:

```
nss /MountImageVolume=TOOLS:OES11_INSTALL/SLES-11-SP4-DVD-x86_64-GM-
DVD1.iso
```

4b Note the assigned volume name.

For the first SLES DVD you mount, the name is `SLES11SP_3`, which is the actual volume name in the image file. For the second image you mount, the assigned name is DVD_*followed by a four-digit number*, starting with 0000.

The same principle applies to the OES 11 image files. The first file mounted is the actual OES 11 volume name, but the second image is assigned a *DVD_xxxx* name.

Knowing which volume is for which platform is critical as you create an access URL to the volume in Apache Manager.

5. In a supported browser, start Apache Manager by entering the following URL:

   https://*server_ip_address*:2200/apacheadmin/login.jsp

   Replace *server_ip_address* with the IP address of the NetWare server.
6. Log in as the Admin user or a user with administrative rights to the Apache server.
7. Click the **Content Manager** icon.
8. Click **Additional Document Directories**.
9. In the **URL Prefix** field, specify an alias name you want people to use to access one of the mounted volumes.
10. Click the **Search** icon next to the **File Path** field.
11. Click the volume name that matches the alias name you specified in Step 9, then click **Finish**.
12. Click **Save > Save and Apply > OK**.

    The path to the volume is added as an additional document.
13. Repeat from Step 9 for the other three volumes.

All of the ISO files are now available for access through the Apache Web Server running on the NetWare server.

Create the Boot DVDs

See Section 2.8, “Preparing Physical Media for a New Server Installation or an Upgrade,” on page 35.

2.9.3 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 11 SP4 Deployment Guide*.

2.10 Always Install OES as an Add-On Product

You must always install OES by adding it as an add-on product while running the YaST install. This is not the same as adding the OES installation media as an installation source.

Failure to do this will prevent the server from registering as an OES 11 SP3 server with the Novell Customer Center.

2.11 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.

2.12 What's Next

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

- “Installing OES 11 SP3 as a New Installation” on page 43
- “Upgrading to OES 11 SP3” on page 115
- “Using AutoYaST to Install and Configure Multiple OES Servers” on page 177
- “Installing, Upgrading, or Updating OES on a VM” on page 191
- “Installing or Configuring OES 11 SP3 on an Existing Server” on page 109

3 Installing OES 11 SP3 as a New Installation

Novell Open Enterprise Server (OES) 11 SP3 is an add-on product to SUSE Linux Enterprise Server (SLES) 11 SP4. When you install and configure OES, you can also install and configure SLES 11 SP4. Therefore, it is helpful to understand how to perform a SLES 11 SP4 installation. This section provides information on the integrated installation of SLES 11 SP4 and OES 11 SP3.

For detailed information on performing a SLES installation, see the *SLES 11 SP4 Deployment Guide (https://www.suse.com/documentation/sles11/book_sle_deployment/?page=/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html)*.

TIP: You can also use the integrated iso (`OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso`) for OES 11 SP3 installation. This ISO has both OES 11 SP3 and SLES 11 SP4. When you use this ISO, you are not require to select OES as an add-on product in the Installation Mode screen.

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.

3.1 Linux Software RAIDs Are Not Cluster Aware

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

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

3.2 Linux Software RAIDs

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

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

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

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

3.3 Starting the OES 11 SP3 Installation

1 Insert the *SUSE Linux Enterprise Server 11 SP4* installation 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 44
- Section 3.3.2, “Installing from a Network Source with DHCP,” on page 45
- Section 3.3.3, “Installing from a Network Source without DHCP,” on page 46

3.3.1 Installing from Physical Media

1 From the DVD boot menu, select the second option (**Installation**), then press Enter.

2 Select the language that you want to use, then click **Next**.

3 Read and accept the license agreement, then click **Next**.

4 (Conditional) If you haven’t already verified that the media you burned is valid, you can check it by using the **Media Check** option; otherwise, click **Next** to continue with the installation.

5 Follow the prompts, using the information contained in the following sections:

5a “Specifying the Installation Mode” on page 47.

5b “Specifying the Add-On Product Installation Information” on page 48.

5c “Setting Up the Clock and Time Zone” on page 48.

5d “Specifying the Installation Settings for the SLES Base and OES Installation” on page 48.

5e “Specifying Configuration Information” on page 55.

5f “Finishing the Installation” on page 106.

6 Complete the server setup by following the procedures in “Completing OES Installation or Upgrade Tasks” on page 159.

3.3.2 Installing from a Network Source with DHCP

1. From the DVD boot menu, select one of the following Installation options that matches your environment, but do not press Enter.

   - **Installation:** The normal installation mode. All modern hardware functions are enabled.
   - **Installation—ACPI Disabled:** If the normal installation fails, it might be because the system hardware does not support ACPI (advanced configuration and power interface). If this seems to be the case, use this option to install without ACPI support.
   - **Installation—Local APIC Disabled:** If the normal installation fails, it might be because the system hardware does not support local APIC (advanced programmable interrupt controllers). If this seems to be the case, use this option to install without local APIC support.

     If you are not sure, try **Installation—ACPI Disabled** or **Installation—Safe Settings** first.
   - **Installation—Safe Settings:** Boots the system with the DMA mode (for DVD drives) and power management functions disabled. Experts can also use the command line to enter or change kernel parameters.

   At this point you can either

   - Skip to with Step 4 and input everything as the install prompts you.

     or
   - Pre-specify the IP address information and/or the boot options parameters on the **Boot Options** line (see “Using Custom Boot Options” in the *SUSE Linux Enterprise Server Installation and Administration Guide* (http://www.suse.com/documentation/sles11/book_sle_deployment/data/sec_deployment_remoteinst_bootinst.html)).

2. (Optional) If you want to specify the IP address information, do it now.

   Otherwise, continue with Step 3.

3. (Optional) If you want to specify boot options parameters, do it now. Then press Enter and continue with Step 7.

   Otherwise, continue with Step 4.

4. Press F4, and 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 37 of the SUSE Linux as a Network Installation Source Server procedure.

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

6. Press Enter to begin the installation.

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

   7a “Specifying the Installation Mode” on page 47.

   7b “Specifying the Add-On Product Installation Information” on page 48.

   7c “Setting Up the Clock and Time Zone” on page 48.

   7d “Specifying the Installation Settings for the SLES Base and OES Installation” on page 48.

   7e “Specifying Configuration Information” on page 55.

   7f “Finishing the Installation” on page 106.

8. Complete the server setup by following the procedures in “Completing OES Installation or Upgrade Tasks” on page 159.

3.3.3 Installing from a Network Source without DHCP

1 From the DVD boot menu, select one of the following Installation options that matches your environment.

- **Installation:** The normal installation mode. All modern hardware functions are enabled.
- **Installation—ACPI Disabled:** If the normal installation fails, this might be because of the system hardware not supporting ACPI (advanced configuration and power interface). If this seems to be the case, use this option to install without ACPI support.
- **Installation—Local APIC Disabled:** If the normal installation fails, this might be because of the system hardware not supporting local APIC (advanced programmable interrupt controllers). If this seems to be the case, use this option to install without local APIC support.

  If you are not sure, try **Installation—ACPI Disabled** or **Installation—Safe Settings** first.
- **Installation—Safe Settings:** Boots the system with the DMA mode (for DVD drives) and power management functions disabled. Experts can also use the command line to enter or change kernel parameters.

2 At this point you can pre-specify the IP address information, and so forth, on the **Boot Options** line (see "Booting the Target System for Installation" in the *SUSE Linux Enterprise Server Deployment Guide* (http://www.suse.com/documentation/sles11/book_sle_deployment/data/sec_deployment_remoteinst_bootinst.html)

If you want to specify the IP address information, and so forth, do it now. Then press Enter and continue with Step 19 on page 47.

Otherwise, press Enter, continue with Step 3, and input everything as the install prompts you.

3 When you receive the following error, select **OK** and press Enter:

```
Could not find the SUSE Linux Enterprise Server 11 SP4 Installation source.
Activating manual set up program.
```

4 Select the language, then select **OK** and press Enter.

5 Select a keyboard map, then select **OK** and press Enter.

6 Select **Start Installation or System**, then select **OK** and press Enter.

7 Select **Start Installation or Update**, then select **OK** and press Enter.

8 Select **Network**, press Enter, then select **OK** and press Enter.

9 Select the network protocol that matches the configured protocol on your network installation server, then press Enter.

10 (Conditional) If you have more than one network interface card, select one of the cards, then press Enter.

We recommend eth0.

11 When prompted whether you want to use DHCP, select **No**, then press Enter.

12 Specify the IP address for the server, then press Enter.

13 Specify the subnet mask, then press Enter.

14 Specify the gateway, then press Enter.

15 Specify the IP address of a name server, then press Enter.

16 Specify the IP address of the network installation server, then press Enter.

17 (Conditional) Depending on the protocol you specified, you might see additional screens for FTP or HTTP. Select the options that are appropriate for your network, then continue with Step 18.

18 Specify the path to your installation source on the network installation server, then press Enter.

19 Follow the prompts, using the information contained in the following sections:

19a "Specifying the Installation Mode" on page 47.

19b "Specifying the Add-On Product Installation Information" on page 48.

19c "Setting Up the Clock and Time Zone" on page 48.

19d "Specifying the Installation Settings for the SLES Base and OES Installation" on page 48.

19e "Specifying Configuration Information" on page 55.

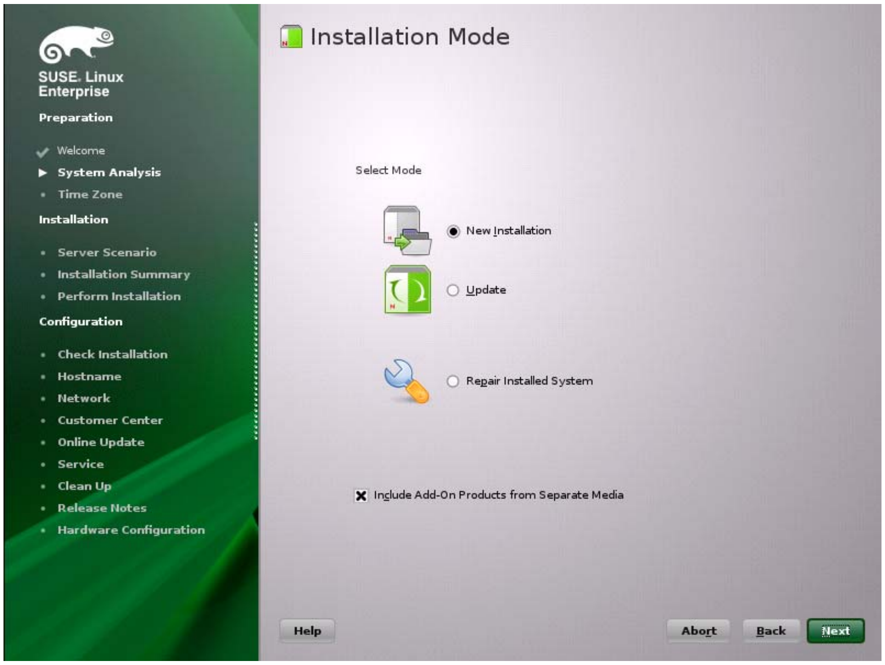
19f "Finishing the Installation" on page 106.

20 Complete the server setup by following the procedures in "Completing OES Installation or Upgrade Tasks" on page 159.

3.4 Specifying the Installation Mode

1 When the Installation Mode page displays, select the following two menu options, then click **Next**:

- **New Installation**
- **Include Add-On Products from Separate Media**



Installation Mode

Select Mode

● New Installation

○ Update

○ Repair Installed System

☒ Include Add-On Products from Separate Media

NOTE: If you have used the integrated iso (`OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso`) for the OES 11 SP3 installation, do not select **Include Add-On Products from Separate Media**.

---

2 Continue with Section 3.5, "Specifying the Add-On Product Installation Information," on page 48.

3.5 Specifying the Add-On Product Installation Information

1 When the Add-On Product Installation page displays, click **Add**.

2 If you are installing OES 11 SP3 from a DVD, do the following:

  2a On the Add-On Product Media page, click **DVD**, then click **Next**.

  2b On the Insert the Add-On Product DVD page, select the appropriate drive where you want to insert the OES 11 SP3 DVD.

  2c Click **Eject**.

  2d Insert the DVD labeled *Novell Open Enterprise Server 11 DVD 1*, then click **Continue**.

3 If you are using an alternate installation source, such as a network installation source, click the appropriate option for your situation, then click Next and supply the required information.

4 Read and accept the Novell Open Enterprise Server 11 SP3 license agreement, then click **Next**.

5 Confirm that the Add-On Product Installation page shows the correct path to the OES media, then click **Next**.

6 Continue with Section 3.6, "Setting Up the Clock and Time Zone," on page 48.

NOTE: During this add-on method of OES installation, the Import Untrusted GnuPG Key pop-up is displayed. Import the key and then proceed.

3.6 Setting Up the Clock and Time Zone

1 Ensure the **Clock**, **Region**, **Timezone**, and **Time and Date** settings are what you want, 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 3.7, "Specifying the Installation Settings for the SLES Base and OES Installation," on page 48.

3.7 Specifying the Installation Settings for the SLES Base and OES Installation

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

- **Overview tab:** This lets you specify everything that is normally required for an OES installation.
- **Expert tab:** This lets you fully customize your SLES installation settings. For detailed information, see "Deployment" in the *SLES 11 SP4 Deployment Guide* (http://www.suse.com/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html). Keep in mind, however, that the SLES guide does not contain instructions for OES-specific components or configurations.

IMPORTANT: If you accept the defaults at this point in the installation process, only the base OES components are installed.

You can add OES services later, but you should at least read the guidelines and follow the applicable procedures in the following sections:

- "Setting Up Disk Partitions" on page 49
- "Customizing the Software Selections" on page 52
- "Accepting the Installation Settings" on page 54

3.7.1 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.

- "Guidelines" on page 49
- "NSS on the System Disk" on page 50
- "Security Flag Recommendations" on page 50
- "Partitioning X86 Machines" on page 51
- "Disk Partition Statistics" on page 51
- "Combining Hard Disk Partitions" on page 52

Guidelines

Table 3-1 presents guidelines for setting up disk partitions on your OES server. For more information, see "Installation Settings" in the *SLES 11 SP4 Deployment Guide* (https://www.suse.com/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html).

Table 3-1 *Partition Guidelines*

Partition to Create	Other Considerations
/boot	Depending on the hardware, it might be useful to create a boot partition (/boot) to hold the boot mechanism and the Linux kernel. You should create this partition at the start of the disk and make it at least 8 MB or 1 cylinder. As a rule of thumb, always create such a partition if it was included in the YaST original proposal. If you are unsure about this, create a boot partition to be on the safe side. **IMPORTANT:** In a Xen VM installation, format the /boot partition using **Ext2** as the file system. For a technical explanation of why this is necessary, see "Paravirtual Mode and Journaling File System" in the *Virtualization with Xen (http://www.suse.com/documentation/sles11/book_xen/data/book_xen.html)* guide.
swap	This should normally be twice the size of the RAM installed on your server. If you create a /boot partition, create the swap partition second. Otherwise, create the swap partition first.
/	Define this partition as 3 GB or more. In all cases, create this partition after you create the swap partition. Keep in mind that this root (/) partition contains all of the partitions listed below that you don't specifically create.
/var	This contains system logs and should therefore be a separate partition to avoid impacting system and service stability because of a disk-full condition. Define this partition as 4 GB or more.

Partition to Create	Other Considerations
/opt	Some (mostly commercial) programs install their data in /opt. Define this partition as 4 GB or more.
/usr	Creating this as a separate partition makes updating the server easier if you need to reinstall the system from the beginning because you can keep the partition intact. Define this partition as 4 GB or more.
/srv	This contains the web and FTP servers. Consider making this a separate partition to avoid having someone flood the disk by accident or on purpose, which impacts system and service stability.
/home	User Home directories go here. Consider making this a separate partition to avoid having someone flood the disk by accident or on purpose, which impacts system and service stability. You can allocate the rest of the disk space to this partition.
/tmp	Creating this as a separate partition is optional. However, because it is writable by everyone, best practices suggest creating a separate partition to avoid having someone flood the disk by accident or on purpose, which impacts system and service stability.
	Place application-specific files on a separate partition.
	If you are building a mail server, note where the mail spools reside because they can grow quite large, and you need to anticipate this when you are defining partition sizes.

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).

Security Flag Recommendations

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

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

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

Disk Partition Statistics

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

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

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.

3.7.2 Customizing the Software Selections

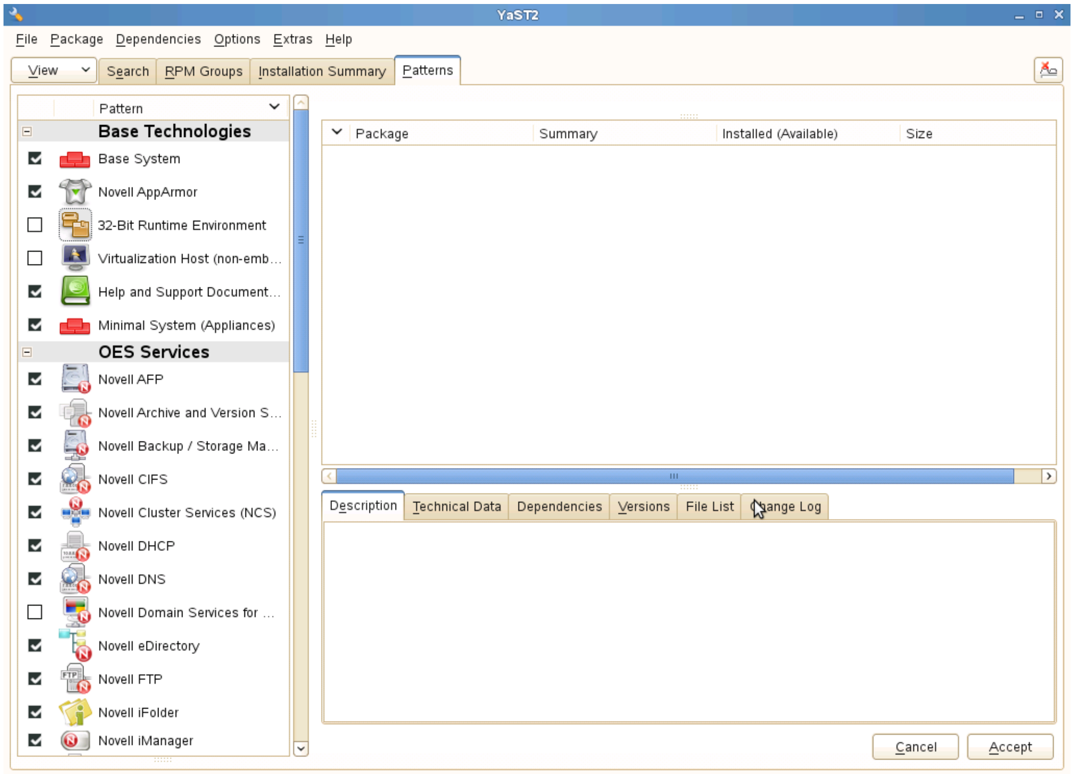
IMPORTANT: To install any of the OES patterns, you must customize the software selections. If you don’t make any selections, only the base SLES 11 SP4 and the base OES packages are installed. However, you can install any of the patterns after the base SLES 11 SP4 installation is complete. See “Installing or Configuring OES 11 SP3 on an Existing Server” on page 109.

To customize which software packages are installed on the server:

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

   The Open Enterprise Server add-on adds the OES Services category of patterns to the base software selection categories offered by the SLES 11 SP4 installation. OES Services include patterns that contain Novell services or products such as Novell DNS and DHCP services, iPrint, or iManager.

   None of the OES Services is selected by default. This lets you fully customize your OES server.
2. At this point, 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 (see “Unsupported Service Combinations” in the *OES 11 SP3: Planning and Implementation Guide*).



Base Technologies

☑ Base System
☑ Novell AppArmor
□ 32-Bit Runtime Environment
□ Virtualization Host (non-emb…
☑ Help and Support Document…
☑ Minimal System (Appliances)

OES Services

☑ Novell AFP
☑ Novell Archive and Version S…
☑ Novell Backup / Storage Ma…
☑ Novell CIFS
☑ Novell Cluster Services (NCS)
☑ Novell DHCP
☑ Novell DNS
□ Novell Domain Services for …
☑ Novell eDirectory
☑ Novell FTP
☑ Novell iFolder
☑ Novell iManager

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 27.

You can manually change the default SLES selections by changing the install status and selecting the patterns offered in each category.

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

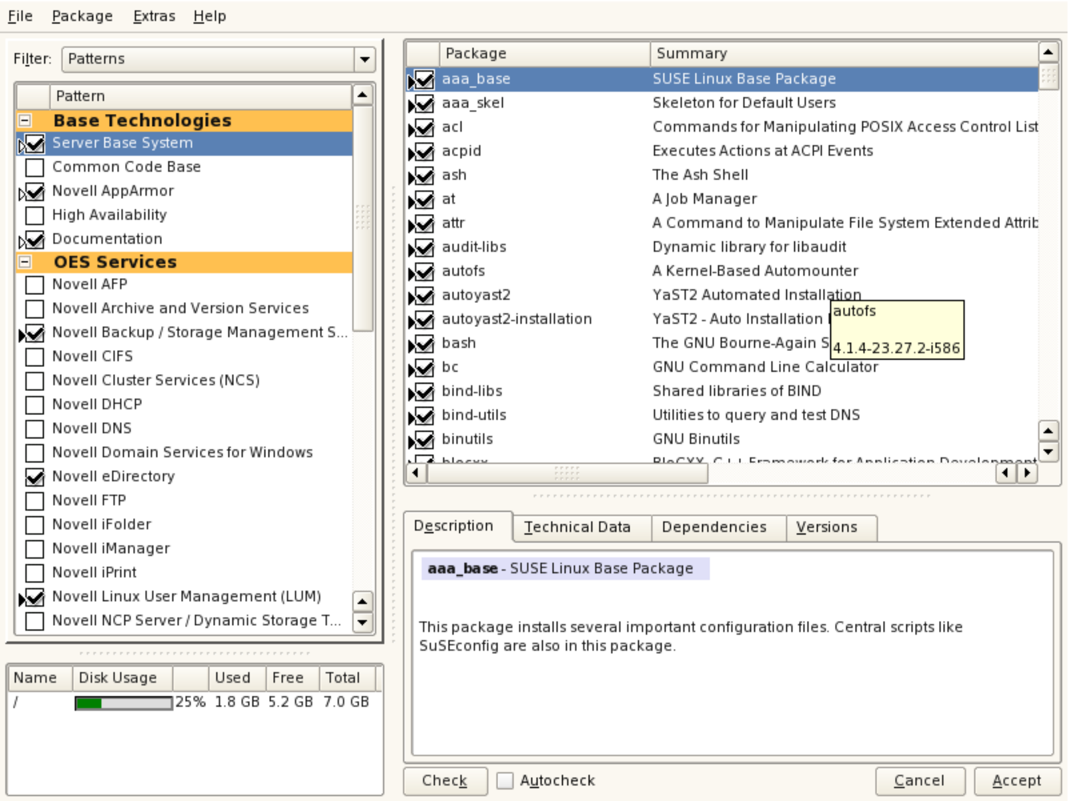
Selecting only the patterns that you want to install ensures that the patterns and their dependent patterns and packages are installed.

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

You must install at least one of the SLES Base Technologies patterns.

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**.



Pattern
Base Technologies
☑ Server Base System
□ Common Code Base
☑ Novell AppArmor
□ High Availability
☑ Documentation
OES Services
□ Novell AFP
□ Novell Archive and Version Services
☑ Novell Backup / Storage Management S...
□ Novell CIFS
□ Novell Cluster Services (NCS)
□ Novell DHCP
□ Novell DNS
□ Novell Domain Services for Windows
☑ Novell eDirectory
□ Novell FTP
□ Novell iFolder
□ Novell iManager
□ Novell iPrint
☑ Novell Linux User Management (LUM)
□ Novell NCP Server / Dynamic Storage T...

Name	Disk Usage	Used	Free	Total
/	25%	1.8 GB	5.2 GB	7.0 GB

Package	Summary
☑ aaa_base	SUSE Linux Base Package
☑ aaa_skel	Skeleton for Default Users
☑ acl	Commands for Manipulating POSIX Access Control List
☑ acpid	Executes Actions at ACPI Events
☑ ash	The Ash Shell
☑ at	A Job Manager
☑ attr	A Command to Manipulate File System Extended Attrib
☑ audit-libs	Dynamic library for libaudit
☑ autofs	A Kernel-Based Automounter
☑ autoyast2	YaST2 Automated Installation
☑ autoyast2-installation	YaST2 - Auto Installation
☑ bash	The GNU Bourne-Again S
☑ bc	GNU Command Line Calculator
☑ bind-libs	Shared libraries of BIND
☑ bind-utils	Utilities to query and test DNS
☑ binutils	GNU Binutils
☑ blocxx	BlocXX C++ Framework for Application Development

autofs
4.1.4-23.27.2-i586

aaa_base - SUSE Linux Base Package

This package installs several important configuration files. Central scripts like SuSEconfig are also in this package.

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

4 If you are prompted with the license agreement for **Professional TrueType Fonts**, click **Accept**.

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

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

3.7.3 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 **Accept**.

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

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

4 For installations using a network installation source, you can remove the network boot DVD (*SLES 11 SP4 DVD 1*) from the DVD drive.

or

For installations using a DVD installation source, leave the DVD in the DVD drive.

5 After the server reboot, proceed with "Specifying Configuration Information" on page 55.

3.8 Specifying Configuration Information

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

- Section 3.8.1, “Specifying the Password for the System Administrator “root”,” on page 55
- Section 3.8.2, “Specifying the Hostname and Domain Name,” on page 55
- Section 3.8.3, “Specifying Network Configuration Settings,” on page 56
- Section 3.8.4, “Testing the Connection to the Internet,” on page 59
- Section 3.8.5, “Specifying Novell Customer Center Configuration Settings,” on page 59
- Section 3.8.6, “Updating the Server Software,” on page 61
- Section 3.8.7, “Specifying Service Configuration Settings,” on page 63
- Section 3.8.8, “Typical and Custom OES Configuration,” on page 65
- Section 3.8.9, “Specifying LDAP Configuration Settings,” on page 67
- Section 3.8.10, “Specifying eDirectory Configuration Settings,” on page 69
- Section 3.8.11, “Configuring OES Services,” on page 77
- Section 3.8.12, “Configuration Guidelines for OES Services,” on page 78

3.8.1 Specifying the 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. If you have a password longer than eight characters, click **Expert Options** > **Blowfish** > **OK**.
2. Confirm the password.
3. Click **Next**.

3.8.2 Specifying the Hostname and Domain Name

On the Hostname and Domain Name page:

1. Specify the hostname associated with the IP address you have or will assign to the server.
2. Specify the domain name for the server.
3. Deselect **Change Hostname via DHCP**.
4. Click **Next**.

3.8.3 Specifying Network Configuration Settings

On the Network Configuration page, you can change the configuration for the following, most of which do not apply in an OES server installation scenario:

- Network Mode
- Firewall
- IPv6
- Network Interfaces
- DSL Connections
- ISDN Adapters
- Modems
- VNC Remote Administration
- Proxy

In this section, we provide details only for the components that apply to OES servers.

- "Network Interface" on page 56
- "Firewall" on page 57

Network Interface

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.

Specify the setting for each network board on the server:

1. On the Network Configuration page, click **Network Interfaces.**
2. On the Network Card Configuration Overview page, select the network card you want to configure, then click **Edit**.
3. Select **Static Address Setup**, then specify the IP address and the subnet mask for the interface.

   OES requires a static IP address.
4. In the **Detailed Settings** list, select **Hostname and Name Server**.

   4a In the **Name Servers and Domain Search List** panel, specify from one to three DNS server IP addresses.

   4b Click **OK** to return to the **Detailed Settings** list.
5. In the **Detailed Settings** list, select **Routing**.

   5a Specify the IP address of the default gateway on the subnet where you are installing the OES server.

   5b Click **OK** to return to the **Detailed Settings** list.
6. Click **Next** to return to the Network Card Configuration Overview page.
7. Complete Step 2 through Step 6 for each network board, then click **Next** to return to the main Network Configuration page.

Firewall

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

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

Table 3-2 *Open Enterprise Server Services and Ports*

Service	Default Ports
Domain Services for Windows	◆ 1636 (LDAPS) ◆ 1389 (LDAP) ◆ 88 (Kerberos TCP and UDP) ◆ 135 (RPC Endpoint Manager TCP and UDP) ◆ 1024 - 65535 (RPC Dynamic Assignments TCP) ◆ 3268 (Global Catalog LDAP TCP) ◆ 3269 (Global Catalog LDAP over SSL TCP) ◆ 123 (Network Time Protocol UDP) ◆ 137 (NetBIOS Name Service TCP and UDP) ◆ 138 (NetBIOS Datagram Service TCP and UDP) ◆ 139 (NetBIOS Session Service TCP and UDP) ◆ 8025 (Domain Service Daemon TCP) ◆ 445 (Microsoft-DS traffic TCP and UDP)
NetIQ eDirectory	◆ 389 (LDAP) ◆ 636 (secure LDAP) **IMPORTANT:** The scripts that manage the common proxy user require port 636 for secure LDAP communications. ◆ 8028 (HTTP for iMonitor) ◆ 8030 (secure HTTP for iMonitor) ◆ 524 (NCP)
iManager	◆ 80 (HTTP) ◆ 443 (secure HTTP)
iPrint	◆ 80 (HTTP) ◆ 443 (secure HTTP) ◆ 631 (IPP)
Novell AFP	◆ 548
Novell Archive and Version Services	◆ 26029
Novell CIFS	◆ 636 (secure LDAP) **IMPORTANT:** The scripts that manage the common proxy user require port 636 for secure LDAP communications.

Service	Default Ports
Novell DHCP	◆ 67
Novell DNS	◆ 953 (secure HTTP) ◆ 53 (TCP) ◆ 53 (UDP)
Novell FTP	◆ 21
Novell Information Portal	◆ 80 (HTTP) ◆ 443 (secure HTTP)
Novell NetWare Core Protocol (NCP)	◆ 524
Novell Remote Manager	◆ 8008 (HTTP) ◆ 8009 (secure HTTP)
SFCB	◆ 5988 (HTTP) ◆ 5989 (secure HTTP)
QuickFinder	◆ 80 (HTTP) ◆ 443 (secure HTTP)
Samba	◆ 139 (Netbios) ◆ 445 (Microsoft-ds)
Secure Shell	◆ 22
Storage Management Services (Backup)	◆ 40193 (smdr daemon)
Time Synchronization	◆ 123 (Network Time Protocol UDP)

To adapt the automatic settings to your own preferences:

1. Click **Change > Firewall**.
2. In the left panel, select the settings you want to change, then make the changes in the right panel.
3. When you are finished, click **Accept**.

For more information about the firewall, see "Configuring the Firewall with YaST" in the *SUSE Linux Enterprise Server 11 Security Guide* (http://www.suse.com/documentation/sles11/book_security/data/sec_fire_suse.html).

To disable the firewall:

1. On the Network Configuration page, under **Firewall**, click **enabled** on the **Firewall is enabled** status line.

   When the firewall is disabled, the status for Firewall should read **Firewall is disabled**.
2. Verify that the settings on the Network Configuration page are set as desired, then click **Next** to save the configuration. Continue with "Testing the Connection to the Internet" on page 59.

3.8.4 Testing the Connection to the Internet

On the Test Internet Connection page:

1 Select **Yes**, **Test Connection to the Internet**, then click **Next**.

Obtaining the latest SUSE release notes might fail at this point. If it does, view the log to verify that the network configuration is correct, then click **Next**.

If the network configuration is not correct, click **Back** > **Back** and fix your network configuration. See "Network Interface" on page 56.

IMPORTANT: Do not skip this test. For a successful install, you must configure the Novell Customer Center and update SLES 11 SP4 from the patch repository before configuring OES services.

2 Continue with "Specifying Novell Customer Center Configuration Settings" on page 59.

3.8.5 Specifying Novell Customer Center Configuration Settings

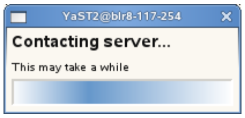
OES 11 SP3 requires that the SLES 11 SP4 base be updated prior to installing and configuring OES 11 SP3 services. If not, some OES services, such as Novell FTP, will not function properly after the installation and will need to be configured again after the SLES patches are applied.

Therefore, when you are entering the Novell Customer Center configuration information, it is critical that you enter either your purchased SLES 11 SP4 code or the 60-day evaluation code available with your SLES 11 SP4 download.

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

Option	What it Does
Configure Now	Proceeds with registering this server and the SLES 11 SP4 and OES 11 SP3 product in the Novell Customer center.
Hardware Profile	Sends the information to the Novell Customer Center about the hardware that you are installing SLES 11 SP4 and OES 11 SP3 on.
Optional Information	Sends optional information to the Novell 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 following message is displayed.



Contacting server...

This may take a while

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

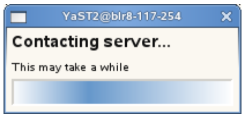
3 On the Manual Interaction Required page, note the information that you will be required to specify, then click **Continue**.

4 On the Novell 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 Novell Login account.
Confirm Email Address	The same email address for your Novell Login account
SUSE Linux Enterprise Server 11 SP4 (optional)	Specify your purchased or 60-day evaluation registration code for the SLES 11 SP4 product. If you don’t specify a code, the server cannot receive any updates or patches.
Open Enterprise Server 11 SP3 (optional)	Specify your purchased or 60-day evaluation registration code for the OES 11 SP3 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.

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

6 After you click **Continue**, the following message is displayed with the Manual Interaction Required screen.

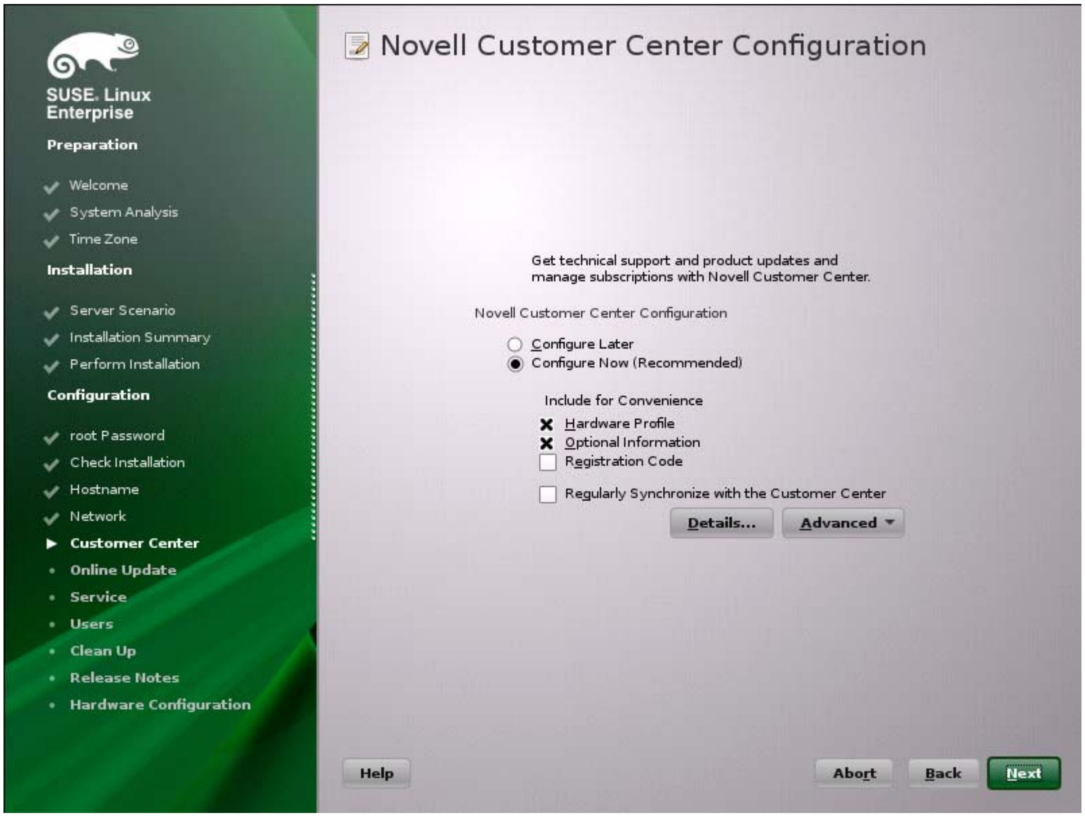


Contacting server...

This may take a while

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

7 Select **Configure Now** to download any updates that are available for the server, then click **Next**.



Novell Customer Center Configuration

Get technical support and product updates and manage subscriptions with Novell Customer Center.

Novell Customer Center Configuration

○ Configure Later
● Configure Now (Recommended)

Include for Convenience

☒ Hardware Profile
☒ Optional Information
□ Registration Code

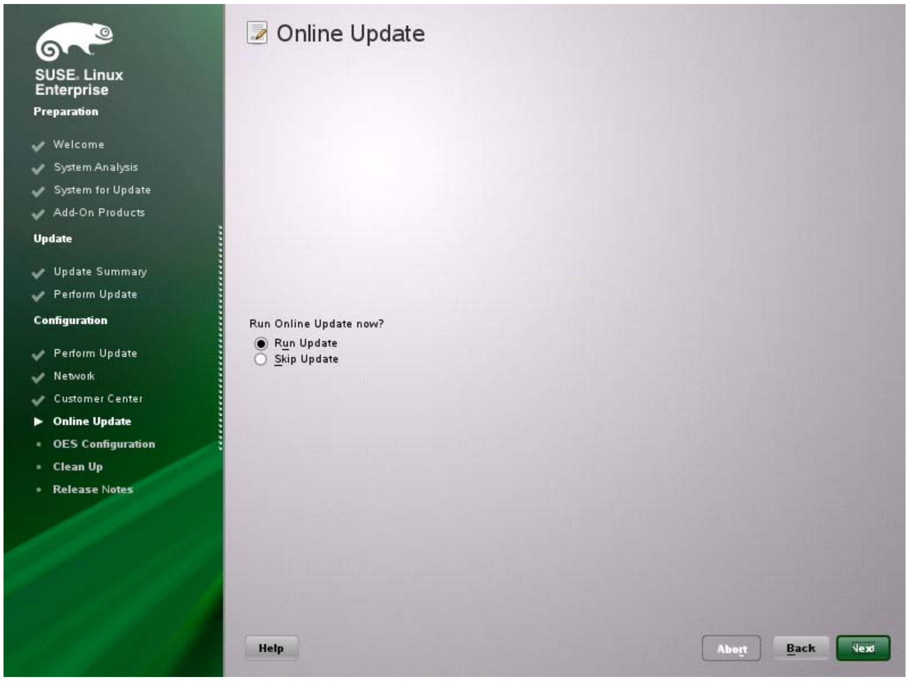
□ Regularly Synchronize with the Customer Center

8 Continue with “Updating the Server Software” on page 61.

3.8.6 Updating the Server Software

When you have a successful connection to the Internet and have registered the server in the Novell Customer Center, the server displays the Online Update page. You must run the online update now for a successful OES installation.

1 On the Online Updates page, click **Run Update > Next**.



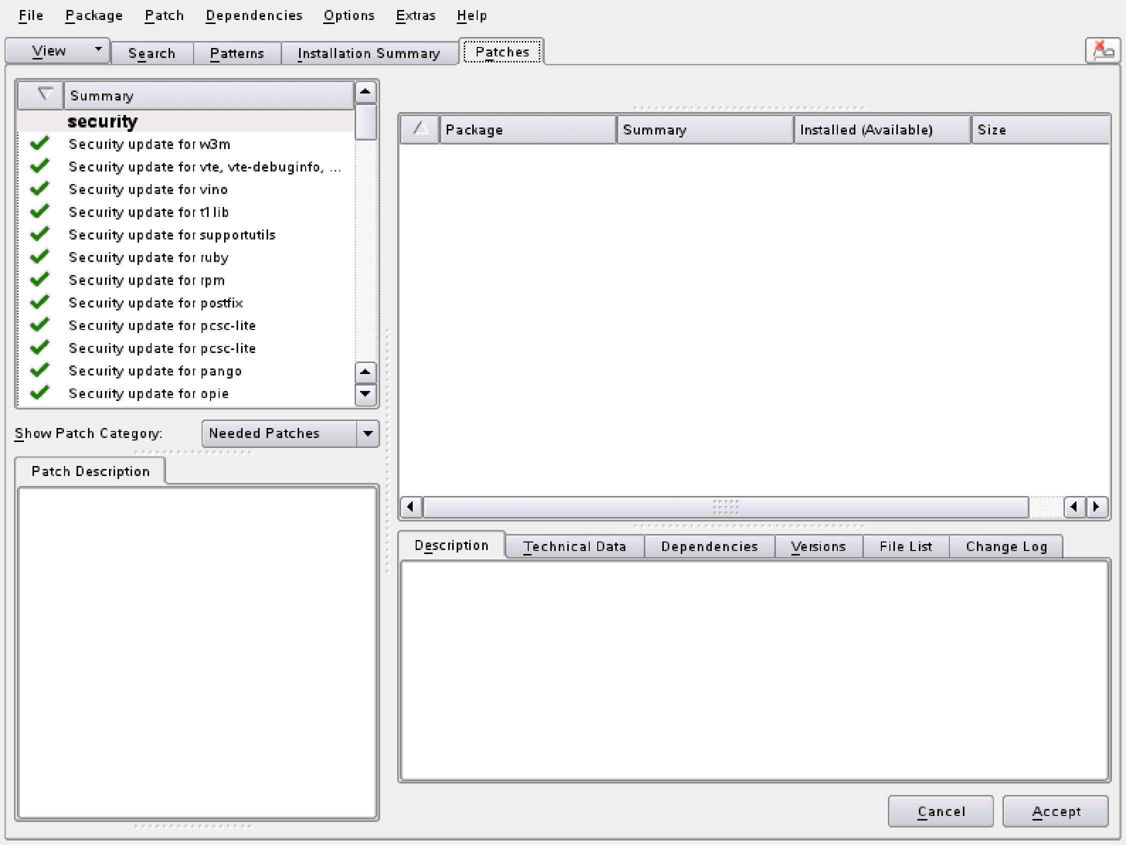
Run Online Update now?

● Run Update

○ Skip Update

2 On the page that shows that updates are available, click **Accept**.

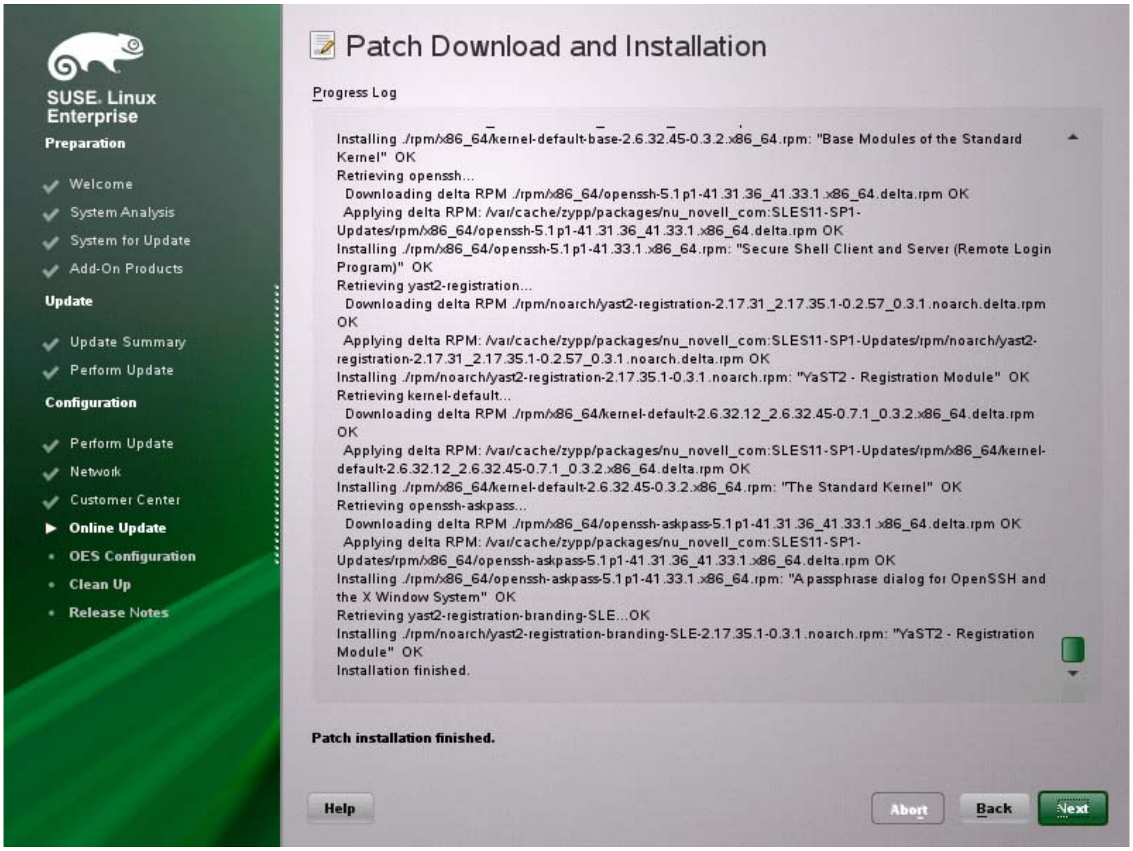
The check marks that are shown on the summary portion of the page are the patches that will be installed on your system after clicking **Accept**.



security

- ✓ Security update for w3m
- ✓ Security update for vte, vte-debuginfo, ...
- ✓ Security update for vino
- ✓ Security update for t1lib
- ✓ Security update for supportutils
- ✓ Security update for ruby
- ✓ Security update for rpm
- ✓ Security update for postfix
- ✓ Security update for pcsc-lite
- ✓ Security update for pcsc-lite
- ✓ Security update for pango
- ✓ Security update for opie

3 When you see the following message, click **Next**.



Patch Download and Installation

Progress Log

```
Installing ./rpm/x86_64/kernel-default-base-2.6.32.45-0.3.2.x86_64.rpm: "Base Modules of the Standard
Kernel"  OK
Retrieving openssh...
  Downloading delta RPM ./rpm/x86_64/openssh-5.1p1-41.31.36_41.33.1.x86_64.delta.rpm OK
  Applying delta RPM: /var/cache/zypp/packages/nu_novell_com:SLES11-SP1-
Updates/rpm/x86_64/openssh-5.1p1-41.31.36_41.33.1.x86_64.delta.rpm OK
Installing ./rpm/x86_64/openssh-5.1p1-41.33.1.x86_64.rpm: "Secure Shell Client and Server (Remote Login
Program)"  OK
Retrieving yast2-registration...
  Downloading delta RPM ./rpm/noarch/yast2-registration-2.17.31_2.17.35.1-0.2.57_0.3.1.noarch.delta.rpm
OK
  Applying delta RPM: /var/cache/zypp/packages/nu_novell_com:SLES11-SP1-Updates/rpm/noarch/yast2-
registration-2.17.31_2.17.35.1-0.2.57_0.3.1.noarch.delta.rpm OK
Installing ./rpm/noarch/yast2-registration-2.17.35.1-0.3.1.noarch.rpm: "YaST2 - Registration Module"  OK
Retrieving kernel-default...
  Downloading delta RPM ./rpm/x86_64/kernel-default-2.6.32.12_2.6.32.45-0.7.1_0.3.2.x86_64.delta.rpm
OK
  Applying delta RPM: /var/cache/zypp/packages/nu_novell_com:SLES11-SP1-Updates/rpm/x86_64/kernel-
default-2.6.32.12_2.6.32.45-0.7.1_0.3.2.x86_64.delta.rpm OK
Installing ./rpm/x86_64/kernel-default-2.6.32.45-0.3.2.x86_64.rpm: "The Standard Kernel"  OK
Retrieving openssh-askpass...
  Downloading delta RPM ./rpm/x86_64/openssh-askpass-5.1p1-41.31.36_41.33.1.x86_64.delta.rpm OK
  Applying delta RPM: /var/cache/zypp/packages/nu_novell_com:SLES11-SP1-
Updates/rpm/x86_64/openssh-askpass-5.1p1-41.31.36_41.33.1.x86_64.delta.rpm OK
Installing ./rpm/x86_64/openssh-askpass-5.1p1-41.33.1.x86_64.rpm: "A passphrase dialog for OpenSSH and
the X Window System"  OK
Retrieving yast2-registration-branding-SLE...OK
Installing ./rpm/noarch/yast2-registration-branding-SLE-2.17.35.1-0.3.1.noarch.rpm: "YaST2 - Registration
Module"  OK
Installation finished.
```

Patch installation finished.

4 In the pop-up that informs you about the kernel update, click **OK**.

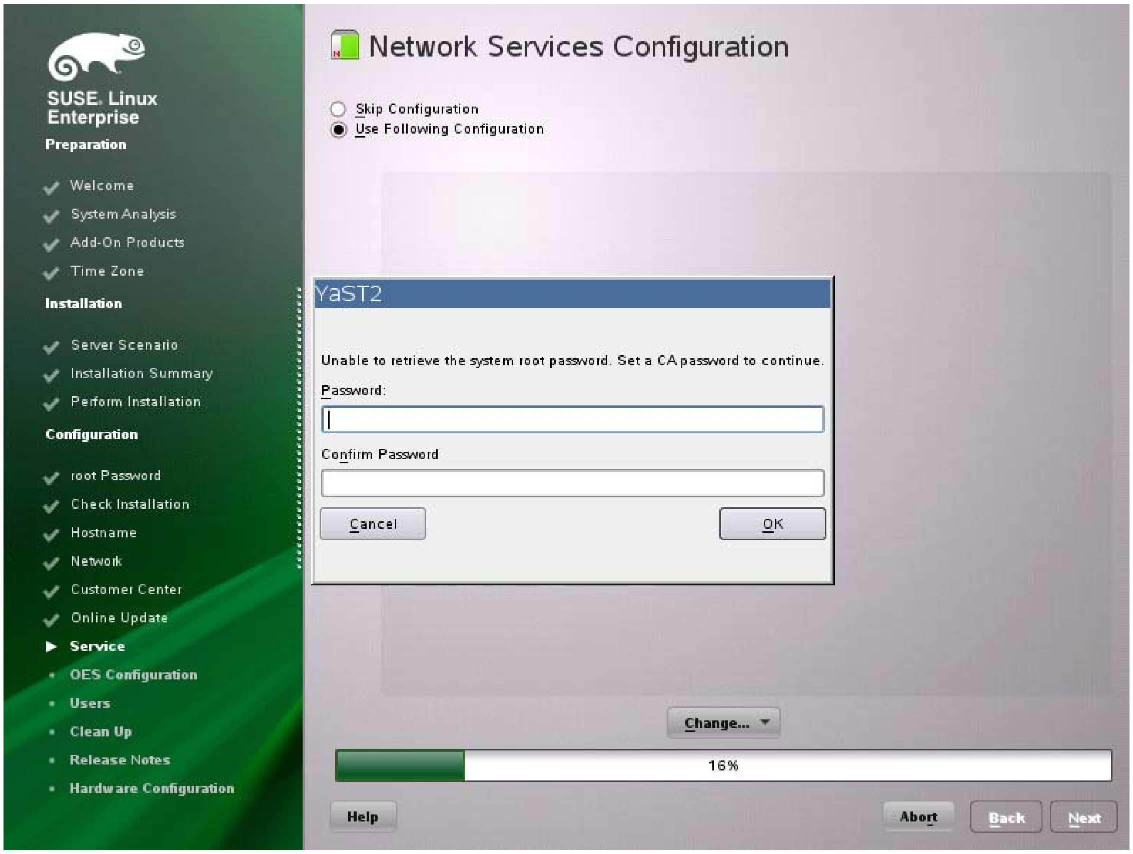
The system reboots before continuing the installation.

5 Continue with "Specifying Service Configuration Settings" on page 63.

3.8.7 Specifying Service Configuration Settings

Because the server was rebooted during the installation, the default settings for CA management lost the root password as indicated by the red text under **CA Management**.

1 Reset the password for `root`.



Network Services Configuration

○ Skip Configuration
● Use Following Configuration

YaST2

Unable to retrieve the system root password. Set a CA password to continue.

Password:

Confirm Password

2 Observe the settings on the Installation Settings page.

- **CA Management:** This indicates the certificate that is used by the Apache web server if another certificate is not specified.

  By default, OES creates and installs a replacement eDirectory certificate later in the installation process. We recommend that you accept the eDirectory certificate option because it is much more secure than the certificate that is proposed.

  Alternatively, you can install a third-party certificate.

  In all cases, do not disable the configuration at this point because the services that use Apache will not work if you do.

  For more information about OES certificate management, see “Certificate Management” in the *OES 11 SP3: Planning and Implementation Guide*.

- **OpenLDAP Server:** Do not enable this option. On OES servers, NetIQ eDirectory LDAP server replaces the SLES 11 SP4 OpenLDAP server.

3 If you are not installing a third-party certificate, click **Next**.

or

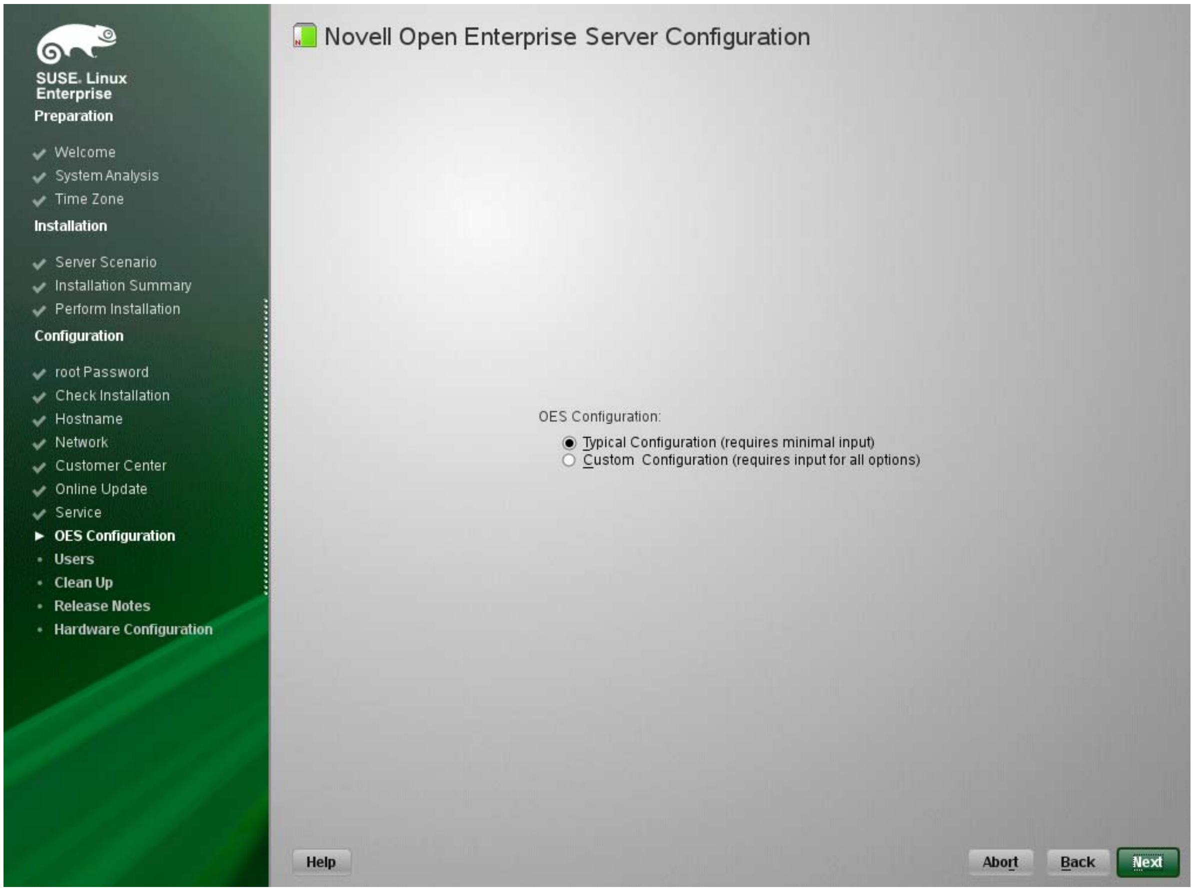
If you are installing a third-party certificate, click **CA Management** and refer to the information about Certificate Authority Management on SLES. See in the “Managing X.509 Certification” in the *SUSE LINUX Enterprise Server 11 Security Guide* (http://www.suse.com/documentation/sles11/book_security/data/cha_security_yast_ca.html). Then return to these instructions to continue your OES installation.

4 If you did not select the NetIQ eDirectory pattern for this server, continue with "Specifying LDAP Configuration Settings" on page 67.

Otherwise, skip the next section and continue with "Specifying eDirectory Configuration Settings" on page 69.

3.8.8 Typical and Custom OES Configuration

Beginning with OES 11 SP3, 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 11 SP3 with minimal user intervention and the Custom Configuration is the detailed usual method to configure OES.



Novell Open Enterprise Server Configuration

OES Configuration:

● Typical Configuration (requires minimal input)
○ Custom Configuration (requires input for all options)

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:

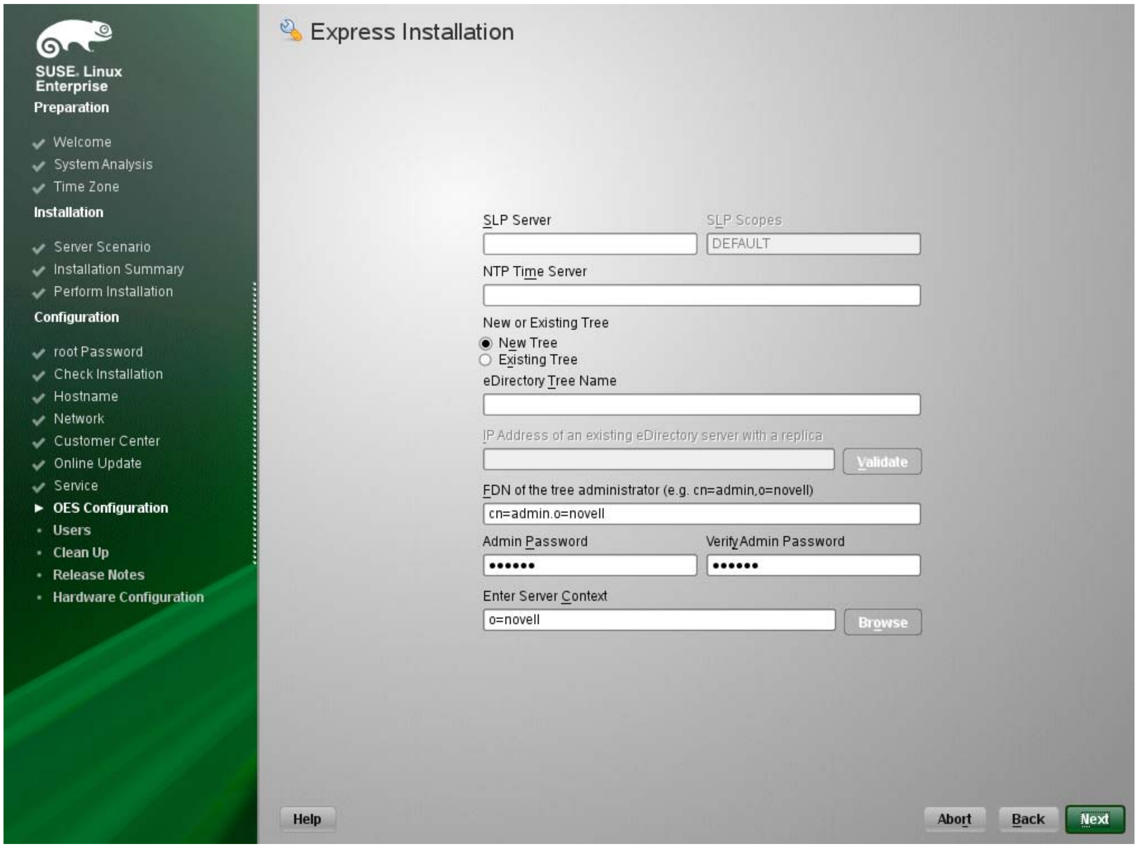
- **SLP Server and SLP Scopes:** In these fields, specify the host name or the IP address of the server where the SLP agent is running and the SLP scopes. If you don't enter any SLP details, multicast SLP mode is chosen by default.

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 serer.

  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 the 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.
- After providing all these details, click **Next**. OES will be installed and configured without any user intervention.



Express Installation

SLP Server

SLP Scopes: DEFAULT

NTP Time Server

New or Existing Tree
● New Tree
○ Existing Tree

eDirectory Tree Name

IP Address of an existing eDirectory server with a replica

FDN of the tree administrator (e.g. cn=admin,o=novell): cn=admin.o=novell

Admin Password: ●●●●●●   Verify Admin Password: ●●●●●●

Enter Server Context: o=novell

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 3.8.9, “Specifying LDAP Configuration Settings,” on page 67, Section 3.8.10, “Specifying eDirectory Configuration Settings,” on page 69, Section 3.8.11, “Configuring OES Services,” on page 77, and Section 3.8.12, “Configuration Guidelines for OES Services,” on page 78.

3.8.9 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.

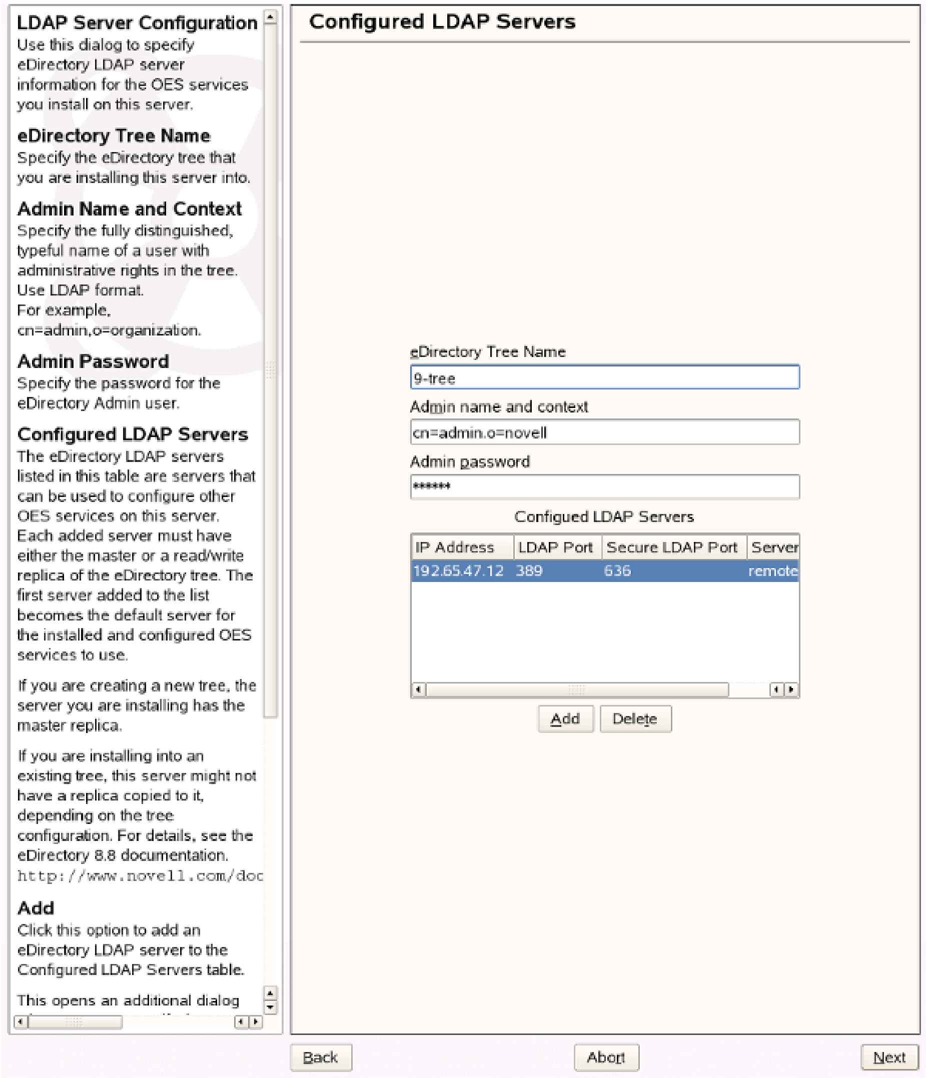
4 Add the LDAP servers that you want the services on this server to use. The servers that you add should hold the master or a read/write replica of eDirectory. Do the following for each server you want to add:

   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



LDAP Server Configuration
Use this dialog to specify eDirectory LDAP server information for the OES services you install on this server.

eDirectory Tree Name
Specify the eDirectory tree that you are installing this server into.

Admin Name and Context
Specify the fully distinguished, typeful name of a user with administrative rights in the tree. Use LDAP format.
For example, cn=admin,o=organization.

Admin Password
Specify the password for the eDirectory Admin user.

Configured LDAP Servers
The eDirectory LDAP servers listed in this table are 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.

If you are creating a new tree, the server you are installing has the master replica.

If you are installing into an existing tree, this server might not have a replica copied to it, depending on the tree configuration. For details, see the eDirectory 8.8 documentation.
`http://www.novell.com/doc`

Add
Click this option to add an eDirectory LDAP server to the Configured LDAP Servers table.

This opens an additional dialog

Configured LDAP Servers

eDirectory Tree Name: 9-tree

Admin name and context: cn=admin.o=novell

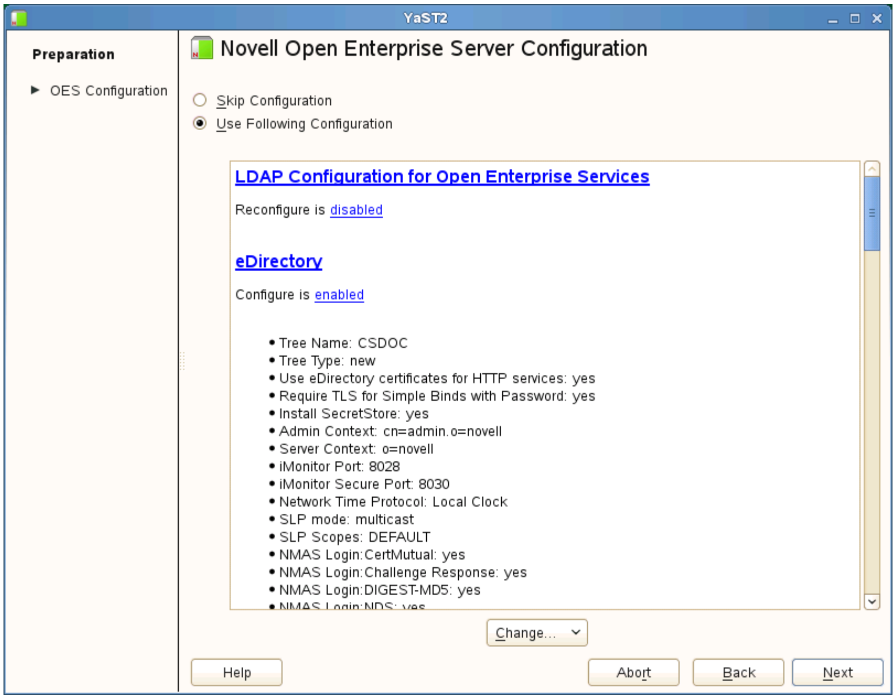
Admin password: ******

Configued LDAP Servers

IP Address	LDAP Port	Secure LDAP Port	Server
192.65.47.12	389	636	remote

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

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



Novell Open Enterprise Server Configuration

○ Skip Configuration
● Use Following Configuration

LDAP Configuration for Open Enterprise Services

Reconfigure is disabled

eDirectory

Configure is enabled

- Tree Name: CSDOC
- Tree Type: new
- Use eDirectory certificates for HTTP services: yes
- Require TLS for Simple Binds with Password: yes
- Install SecretStore: yes
- Admin Context: cn=admin.o=novell
- Server Context: o=novell
- iMonitor Port: 8028
- iMonitor Secure Port: 8030
- Network Time Protocol: Local Clock
- SLP mode: multicast
- SLP Scopes: DEFAULT
- NMAS Login:CertMutual: yes
- NMAS Login:Challenge Response: yes
- NMAS Login:DIGEST-MD5: yes
- NMAS Login:NDS: yes

7 Continue with “Configuring OES Services” on page 77.

3.8.10 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 69
- “Specifying Synchronizing Server Time Options” on page 70
- “Creating a New eDirectory Tree and Installing the Server in It” on page 71
- “Installing the Server into an Existing eDirectory Tree” on page 72
- “Selecting the NetIQ Modular Authentication Services (NMAS) Login Method” on page 74
- “Specifying OES Common Proxy User Information” on page 75

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, then continue with Selecting the NetIQ Modular Authentication Services (NMAS) Login Method.

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.
4. Continue with "Specifying SLP Configuration Options" on page 69.

For more information on time synchronization, see "Implementing Time Synchronization" in the *OES 11 SP3: 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
   - The YaST self-signed common server certificate created in Step 2 on page 64

     Self-signed certificates provide minimal security and limited trust. Unless you have invested in a third-party certificate, we recommend that you use the eDirectory certificates instead.

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

   The default YaST server certificate and key files are:

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

   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, see “Certificate Management” in the *OES 11 SP3: 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 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

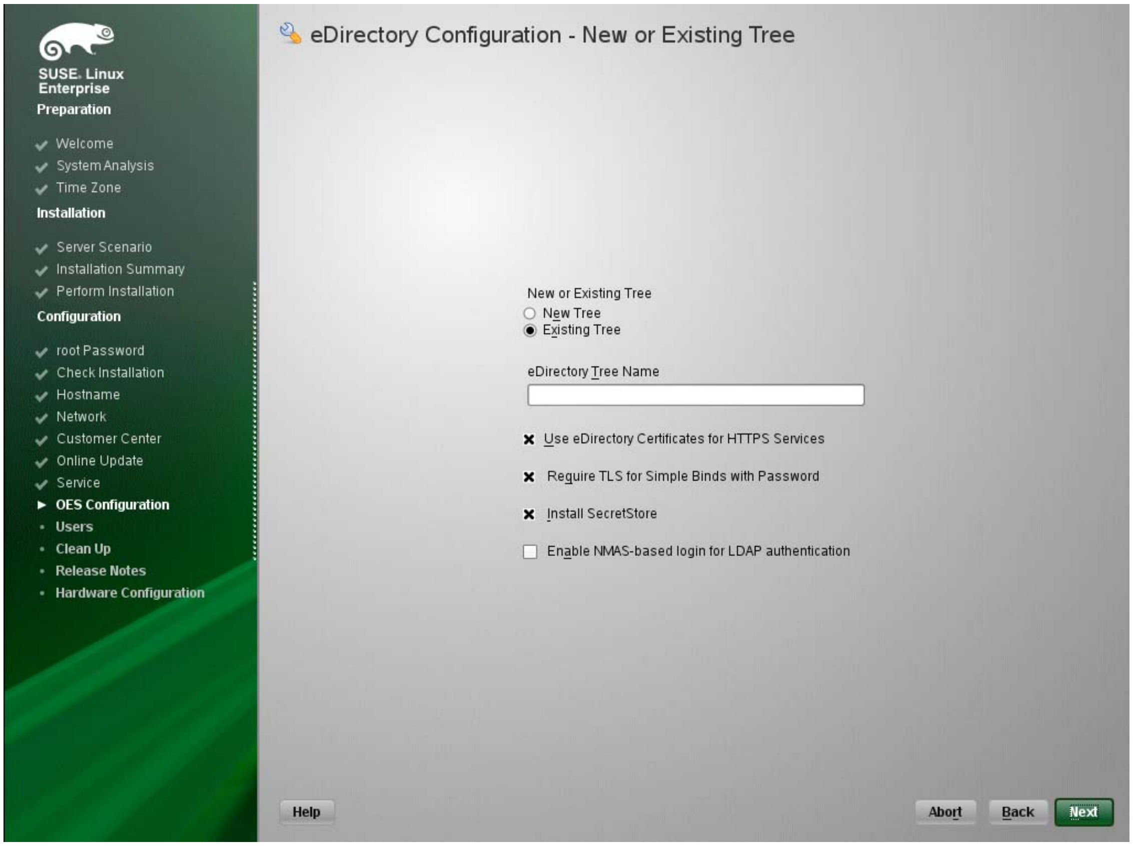
     The default ports are 389 (non-secure) and 636 (secure).

     IMPORTANT: The scripts that manage the common proxy user introduced in OES 11 SP3 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**. Then continue with “Specifying Synchronizing Server Time Options” on page 70.

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.



eDirectory Configuration - New or Existing Tree

New or Existing Tree
○ New Tree
● Existing Tree

eDirectory Tree Name

☒ Use eDirectory Certificates for HTTPS Services

☒ Require TLS for Simple Binds with Password

☒ Install SecretStore

☐ Enable NMAS-based login for LDAP authentication

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)
- The YaST self-signed common server certificate created in Step 2 on page 64

  Self-signed certificates provide minimal security and limited trust. We recommend that you use the eDirectory certificates instead.

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 default YaST server certificate and key files are:

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

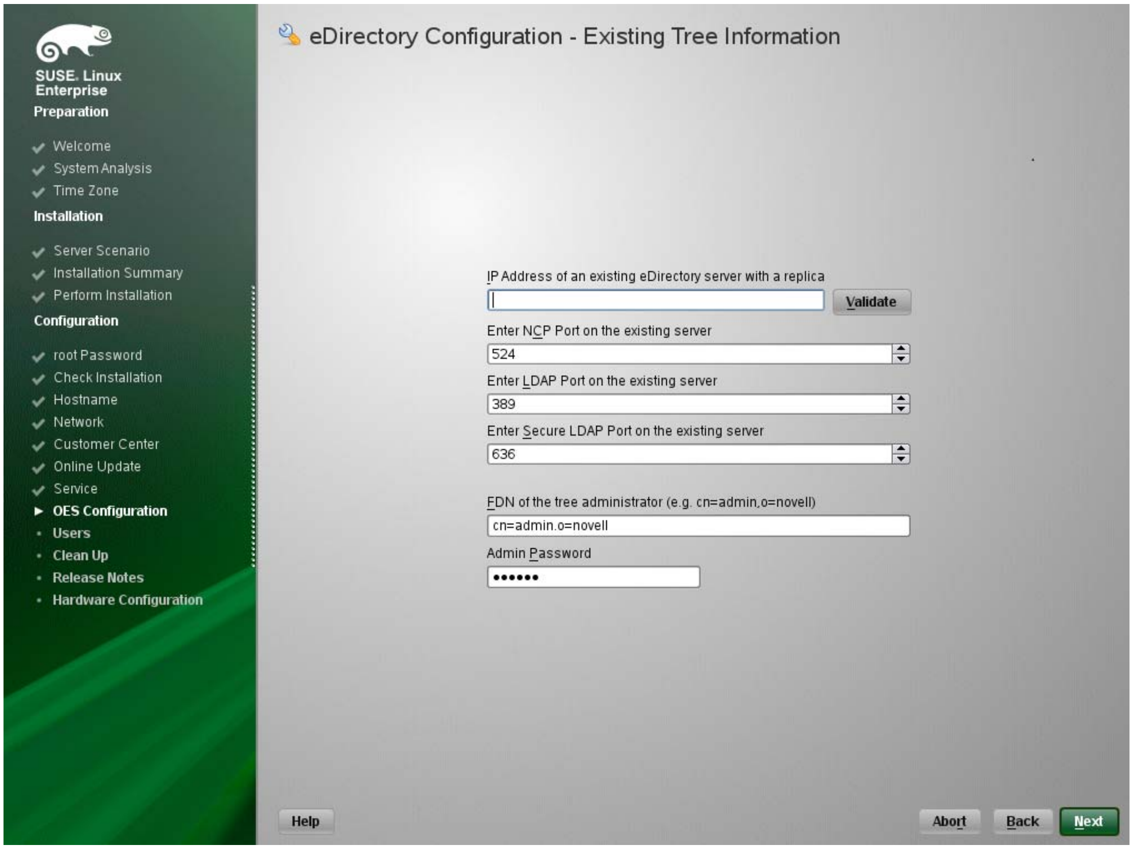
The eDirectory server certificate and key files are:

- 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 11 SP3: Planning and Implementation Guide*.

- Select **Enable NMAS-based login for LDAP authentication** to enforce the use of a single-secure password for all Novell 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:



eDirectory Configuration - Existing Tree Information

IP Address of an existing eDirectory server with a replica:

Enter NCP Port on the existing server: 524

Enter LDAP Port on the existing server: 389

Enter Secure LDAP Port on the existing server: 636

FDN of the tree administrator (e.g. cn=admin,o=novell): cn=admin.o=novell

Admin Password: ••••••

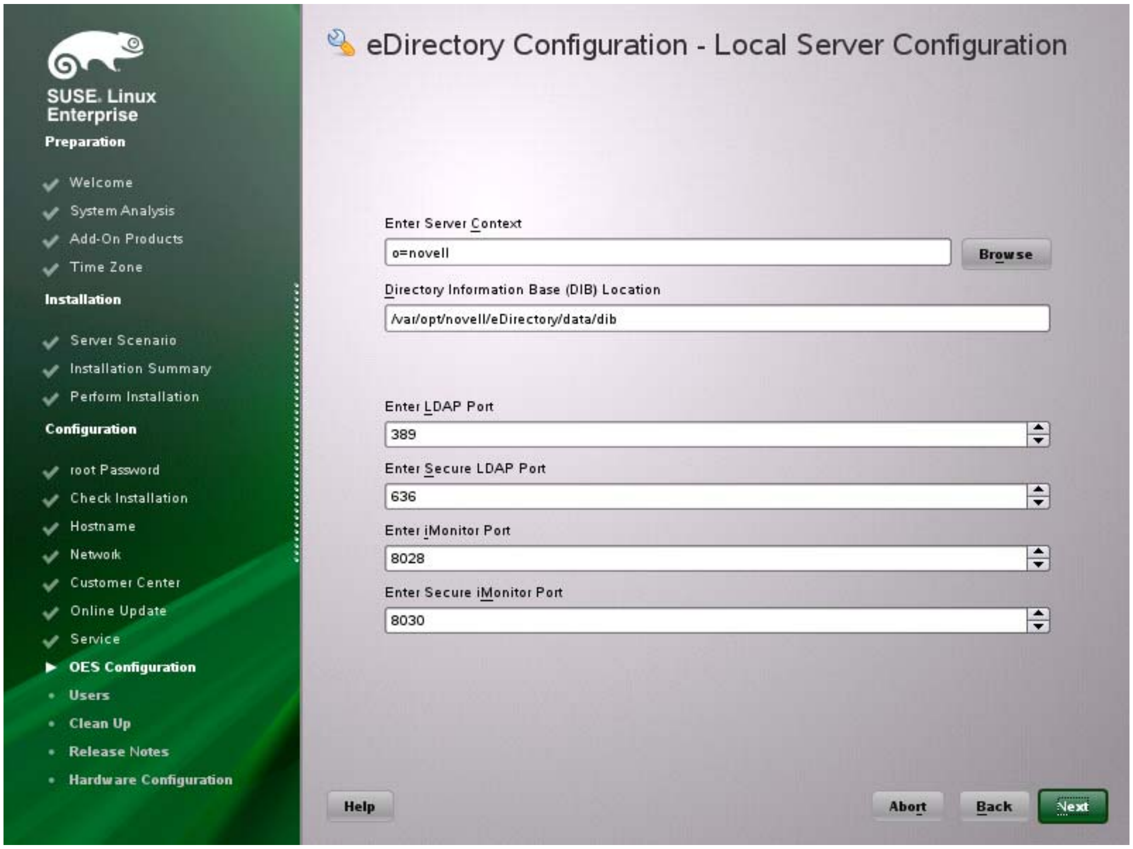
- The IP address of an existing eDirectory server with a replica.

  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:



eDirectory Configuration - Local Server Configuration

Enter Server Context: o=novell

Directory Information Base (DIB) Location: /var/opt/novell/eDirectory/data/dib

Enter LDAP Port: 389

Enter Secure LDAP Port: 636

Enter iMonitor Port: 8028

Enter Secure iMonitor Port: 8030

- 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 introduced in OES 11 SP3 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**. Then continue with "Specifying Synchronizing Server Time Options" on page 70.

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 Novell Client 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 8.8 SP8 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**. Then continue with “Specifying OES Common Proxy User Information” on page 75.

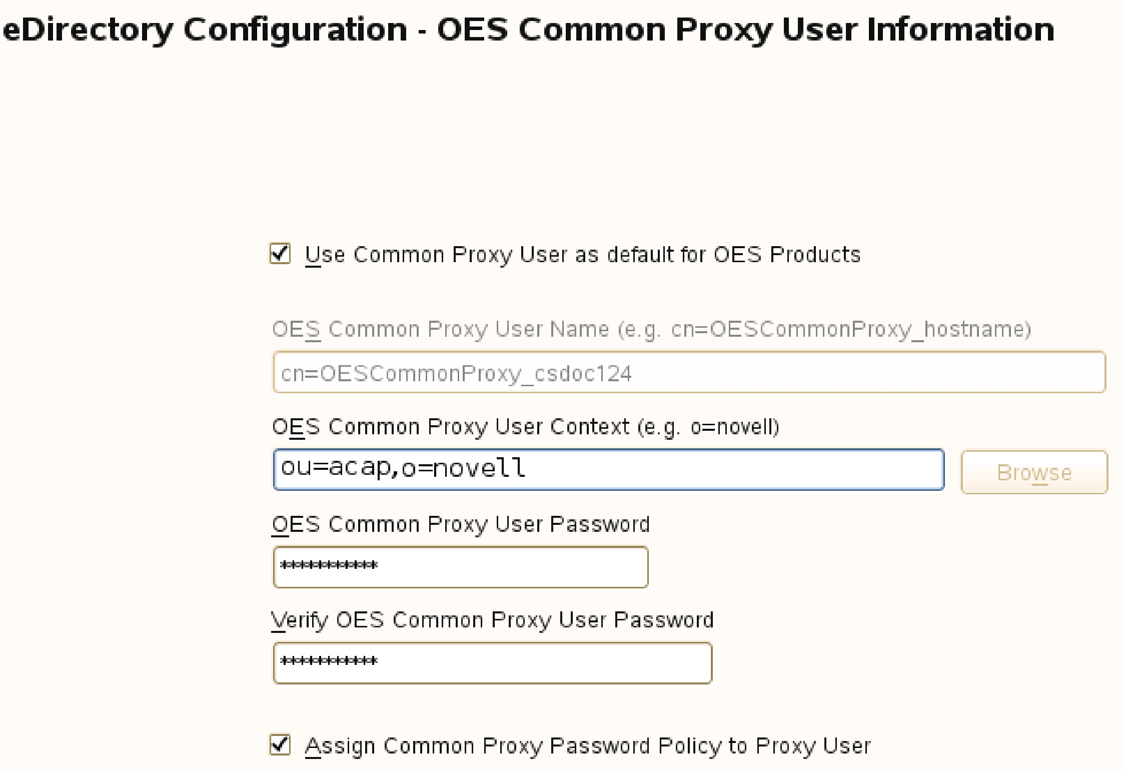
Specifying OES Common Proxy User Information

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 11 SP3: Planning and Implementation Guide*.

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



eDirectory Configuration - OES Common Proxy User Information

☑ Use Common Proxy User as default for OES Products

OES Common Proxy User Name (e.g. cn=OESCommonProxy_hostname)

cn=OESCommonProxy_csdoc124

OES Common Proxy User Context (e.g. o=novell)

ou=acap,o=novell

OES Common Proxy User Password

****

Verify OES Common Proxy User Password

****

☑ Assign Common Proxy Password Policy to Proxy 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, iFolder, 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 11 SP3: 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 nove\'ll. The system-generated password will always be in conformance with the policy rules.

- **Verify OES Common Proxy User Password:** If you specified a different password, type the same password in this field. Otherwise, the system-generated password is automatically included.

- **Assign Common Proxy Password Policy to Proxy User:** The initial common proxy password policy is a simple password policy created with default rules. If desired, you can modify this policy after the installation to enforce stricter rules regarding password length, characters supported, expiration intervals, and so forth.

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

2 Continue with "Configuring OES Services" on page 77.

3.8.11 Configuring OES Services

After you complete the LDAP configuration or the eDirectory configuration, the Novell 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 78.

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 78, or if you are reading online, click a link below:

   - AFP
   - Archive and Version Services
   - Backup/Storage Management Services (SMS)
   - CIFS
   - Clustering (NCS)
   - DHCP
   - DNS
   - Domain Services for Windows (DSfW)
   - eDirectory
   - FTP

- iFolder
- iManager
- iPrint
- Linux User Management (LUM)
- NCP Server/Dynamic Storage Technology
- NetStorage
- Pre-Migration Server
- QuickFinder
- Novell Remote Manager (NRM)
- Novell Samba
- Novell Storage Services

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

3c If you want to skip the configuration of a specific component and configure it later, click **Enable**d in the **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 11 SP3 on an Existing Server" on page 109.

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 3.9, "Finishing the Installation," on page 106.

3.8.12 Configuration Guidelines for OES Services

- "Service Configuration Caveats" on page 79
- "LDAP Configuration for Open Enterprise Services" on page 80
- "Novell AFP Services" on page 81
- "Novell Archive and Version Services" on page 81
- "Novell Backup/Storage Management Services (SMS)" on page 82
- "Novell CIFS for Linux" on page 82
- "Novell Cluster Services" on page 83
- "Novell DHCP Services" on page 85
- "Novell DNS Services" on page 88
- "Novell Domain Services for Windows" on page 89
- "NetIQ eDirectory Services" on page 89
- "Novell FTP Services" on page 94
- "Novell iFolder" on page 94
- "Novell iManager" on page 99
- "Novell iPrint" on page 100
- "Novell Linux User Management" on page 100
- "Novell NCP Server / Dynamic Storage Technology" on page 102

- "Novell NetStorage" on page 102
- "Novell Pre-Migration Server" on page 103
- "Novell QuickFinder" on page 103
- "Novell Remote Manager" on page 104
- "Novell Samba" on page 104
- "Novell Storage Services (NSS)" on page 105

Service Configuration Caveats

Keep the following items in mind as you configure the OES 11 SP3:

***Table 3-3** Caveats for Configuring OES Services*

Issue	Guideline
Software Selections When Using Text-Based YaST	Some older machines, such as a Dell 1300, use the text mode install by default when the video card does not meet SLES 11 SP4 specifications. When you go to the **Software Selection**, and then to the details of the OES software selections, YaST doesn't bring up the OES selections like it does when you use the graphical YaST (YaST2). To view the Software Selection and System Task screen, select **Filter** > **Pattern** (or press Alt+F > Alt+I).

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

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

Issue	Guideline

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

LDAP Configuration for Open Enterprise Services

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

Page and Parameters
Configured LDAP Servers
◆ **eDirectory Tree Name:** The eDirectory tree name that you specified when configuring eDirectory. The tree that you are installing this server into.
◆ **Admin Name and Context:** The eDirectory Admin name you specified when configuring eDirectory.
◆ **Admin Password:** The password of the eDirectory Admin user.

Page and Parameters
◆ **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 *OES 11 SP3: Novell Linux User Management Administration Guide*. **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
◆ **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 11 SP3: Novell AFP for Linux Administration Guide*.

Novell Archive and Version Services

Table 3-6 *Novell Archive and Version Services Parameters and Values*

Page and Parameters
Archive and Version Services Configuration
◆ **Database Port Number:** Specify a port number to use for the archive database communications. **Default:** 5432
◆ **Database Username:** Specify a user name for the administrator of the archive database (the PostgreSQL database for the archived data). **IMPORTANT:** The Postgres user must be an unprivileged user, not the root user. **Default:** arkuser
◆ **Database Password:** Specify and validate a password for the database user. Enter the password for the eDirectory Admin user.

For additional configuration instructions, see "Setting Up Archive and Version Services " in the *OES 11 SP3: Novell Archive and Version Services Administration Guide*.

Novell Backup/Storage Management Services (SMS)

***Table 3-7** Novell Backup/Storage Management Services Parameters and Values*

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

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

Novell CIFS for Linux

***Table 3-8** Novell CIFS Parameters and Values*

Page and Parameters
Novell CIFS Service Configuration
- **eDirectory server address or host name:** Leave the default or select from the drop-down list to change to a different server.
- **LDAP port for CIFS Server:** Displays the port value.
- **Local NCP Server context:** Displays the NCP Server context.

Page and Parameters
◆ **CIFS Proxy User** ◆ **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 *OES 11 SP3: Planning and Implementation Guide*.
◆ **Credential Storage Location:** Accept CASA or specify the **Local File** option. The CIFS proxy user password is encrypted and encoded in the credential storage location. **Default:** CASA
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 11 SP3: Novell CIFS for Linux Administration Guide* and the *OES 11 SP3: Novell AFP for Linux 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 11 SP3: 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

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 11 SP3: Novell Cluster Services for Linux Administration Guide*.
- **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 11 SP3: 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)

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 11 SP3: Novell Cluster Services for Linux Administration Guide*.
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.
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 going to the `/etc/init.d` directory and entering `./novell-ncs start` at the server console of the cluster server. **Default:** Selected

For additional instructions, see the *OES 11 SP3: 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

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

Page and Parameters
◆ **Use Secure Channel for Configuration:** This option is selected by default. When you are configuring DHCP services, it ensures that all configuration is transferred over a secure channel. Deselecting the option lets a user with fewer privileges configure LDAP services and allows configuration information to be transferred over a non-secure channel. **Default:** Selected
◆ **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.
◆ **LDAP Port for DHCP Server:** Select a port for the LDAP operations to use. **IMPORTANT:** The scripts that manage the common proxy user introduced in OES 11 SP3 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 11 SP3: Novell 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 11 SP3: 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 CASA.

Page and Parameters
◆ **Common DNS Configuration Object and User Contexts:**   ◆ **Get Context and Proxy User Information from Existing DNS Server:** Select this option if you are configuring DNS in an existing tree where DNS is already configured, and you want to use the existing Locator, Root Server Info, Group and Proxy User contexts.   ◆ **Existing 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 11 SP3: Novell 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 11 SP3: 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 67 or “Specifying eDirectory Configuration Settings” on page 69, 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 Novell 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/edir88/edir88/data/a2iiie1.html)" in the *NetIQ eDirectory 8.8 Administration Guide (https://www.netiq.com/documentation/edir88/edir88/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 11 SP3: 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 introduced in OES 11 SP3 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 introduced in OES 11 SP3 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 11 SP3: 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 Novell Client 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, iFolder, 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 8.8 SP8 Installation Guide*.

Novell FTP Services

No additional configuration is required.

Novell iFolder

When you configure iFolder as part of the OES install and configuration, you can specify only an EXT3 or ReiserFS volume location for the System Store Path, which is where you store iFolder data for all your users. You cannot create NSS volumes during the system install.

If you want to use an NSS volume to store iFolder data, you must reconfigure iFolder after the initial OES installation. To reconfigure, use Novell iManager to create an NSS volume, then go to **YaST** > **Open Enterprise Server > Install and Configure Open Enterprise Services** and select **iFolder 3.9** to enter new information. All previous configuration information is removed and replaced.

Table 3-13 *Novell iFolder 3.9 Parameters and Values*

Page and Parameters
Novell iFolder System Configuration Options

Page and Parameters

- **iFolder Component to Be Configured**
  - **iFolder Server:** Lets you configure the settings for the iFolder server that is the central repository for storing user iFolders and synchronizing files for enterprise users.
  - **iFolder Web Admin:** Lets you create and configure settings for the administrator user.

    The iFolder Admin user is the primary administrator of the iFolder Enterprise Server. The Web Admin server does not need to be configured on the iFolder Enterprise Server. Devoting a separate server to the Web Admin application improves the performance of the iFolder Enterprise Server by reducing the admin traffic.
  - **iFolder Web Access:** Lets you configure the Web Access server, which is an interface that lets users have remote access to iFolders on the enterprise server.

    The Web Access server lets users perform all the operations equivalent to those of the iFolder client through using a standard web browser.

    The Web Access server does not need to be configured in the same iFolder Enterprise Server. Directing the user tasks to a separate server and thereby reducing the HTTP requests helps to improve the performance of the iFolder Enterprise Server.

  Default: All three items are selected.

Novell iFolder System Configuration

- **Name Used to Identify the iFolder System to Users:** Specify a unique name to identify your iFolder Enterprise Server.

  Default: iFolder

- **System Description (optional):** Specify a descriptive label for your iFolder Enterprise Server to identify it to the users.

  Default: iFolder Enterprise System

- **Path to Server's Data Files:** Specify the case-sensitive address of the location where the iFolder Enterprise Server stores iFolder application files as well as the user iFolders and files.

  IMPORTANT: This location cannot be modified after iFolder is installed.

  Default: `/var/simias/data/`

- **Path to the Recovery Agent Certificates (optional):** Specify the path to the recovery agent certificates that are used for recovering the encryption key.

  Default: `/var/simias/data/simias`

Novell iFolder System Configuration (2)

- **Name of iFolder Server:** Specify a unique name to identify your iFolder Enterprise Server. For example: Host1.

  Default: The name of the OES server

- **iFolder Public URL:** Specify the public URL for users to reach the iFolder Enterprise Server.

  Default: The OES server’s IP address

- **iFolder Private URL:** Specify the private URL corresponding to the iFolder Enterprise Server to allow communication between the servers within the iFolder domain. The private URL and the public URL can be the same.

  Default: The OES server’s IP address

Page and Parameters

- **Select SSL Option for iFolder:** Select the SSL option you want to use to set up a secure connection between the iFolder server and the iFolder clients.

  There are three options for the channel for data transfer: SSL, Non SSL, and Both. However, authentication is always over SSL (not optional).

  - **Both:** (default) This option lets you select a secure or a non-secure channel for communication among the iFolder server, Web Admin server, Web Access server, and the clients. By default, these components use the HTTPS (secure) communication channel. However, all components can also be configured to use HTTP.
  - **Non SSL:** Select this option to enable non-secure communication between the iFolder server, Web Admin server, Web Access server, and the clients. The iFolder uses the HTTP channel for communication.
  - **SSL:** Select this option to enable a secure connection among the iFolder server, iFolder Web Admin server, iFolder Web Access server, and the iFolder clients. The iFolder uses the HTTPS channel for communication.

  Default: Both

- **iFolder Port to Listen On:** Specify the port for the iFolder to listen on.

  Default: 443

- **Install into Existing iFolder Domain:** Select this option when you want to attach to an existing iFolder domain.

  If this option is not selected, this server becomes the Master iFolder server.

  Default: Deselected

- **Private URL of the Master Server:** Specify the private URL of the Master iFolder server that holds the master iFolder data for synchronization to the current iFolder Enterprise Server.

- **Configure LDAP Groups Plugin:** Select this option to configure the LDAP Groups plug-in.

  If this option is left unselected, iFolder does not have LDAP Group support enabled.

Novell iFolder LDAP Configuration

- **Directory server address:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list.

  If you need to add another eDirectory LDAP server to the list, use the LDAP Configuration for Open Enterprise Services dialog box.

  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 are installing into an existing tree, you must enter the password of an admin user in the tree.

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

Page and Parameters
◆ **Use Alternate LDAP server:** If you need to add another LDAP server to the list, select this option and enter the following information: ◆ **Alternate Directory Server Address:** Specify the host or IP address of the alternate LDAP server that iFolder will use. ◆ **LDAP Port:** Specify the LDAP port to use for this alternate server. ◆ **LDAP Secure Port:** Specify the LDAP secure port to use for this alternate server. ◆ **Admin Name and Context:** Specify the administrator name and context for the alternate LDAP server. ◆ **Admin Password:** Type the specified administrator’s password.
Novell iFolder System Configuration
◆ **The iFolder Default Administrator:** Specify the user name for the default iFolder administrative user. Use the full distinguished name of the iFolder administrative user. **Default:** The eDirectory Admin user you specified while configuring eDirectory.
◆ **iFolder Admin Password:** Specify a password for the iFolder administrative user.
◆ **Verify iFolder Admin Password:** Type the password for the iFolder administrative user again.
◆ **LDAP Proxy User:** Specify the full distinguished name of the LDAP Proxy user. This user must have the Read right to the LDAP service. This user is used to provision the users between iFolder Enterprise Server and the LDAP server. If it does not already exist, this user is created and granted the Read right to the root of the tree. The LDAP proxy user's domain name (DN) and password are stored by iFolder. **Default:** If you specified a common proxy user, it is used by default if possible. If you didn’t specify the common proxy user, a user object named iFolderProxy is created in the server context you specified. The common proxy user cannot be used if iFolder is running on a cluster node. If the NCS pattern is selected along with iFolder, this field will be populated with the iFolderProxy by default.
◆ **LDAP Proxy User Password:** Specify a password for the LDAP Proxy user. For more information on proxy user and password management, see “Planning Your Proxy Users” in the *OES 11 SP3: Planning and Implementation Guide*. **Default:** A system-generated password
◆ **Verify LDAP Proxy User Password:** Type the password for the LDAP Proxy user again.
◆ **LDAP Search Context:** Click **Add**, then specify an LDAP tree context to be searched for users to provision them in iFolder. For example, o=acme, o=acme2, or o=acme3 If no context is specified, only the iFolder administrative user is provisioned for services during the install. **Default:** The server context you specified while configuring eDirectory.

Page and Parameters
◆ **LDAP Naming Attribute:** Select which LDAP attribute of the User account to apply when authenticating users. This setting cannot be changed after the install. Each user enters a user name in this specified format at login time. Common Name (CN) is the default, and an email address (email) is the other option. For example, if a user named John Smith has a common name of jsmith and email of john.smith@example.com, this field determines whether the user enters jsmith or john.smith@example.com as the user name when logging in to the iFolder Enterprise Server. **Default:** Common Name (CN)
◆ **Require a Secure Connection Between the LDAP server and the iFolder Server:** If the LDAP server co-exists on the same computer as the iFolder Enterprise Server, you can deselect this option, which increases the performance of LDAP authentications. **Default:** Selected
Novell iFolder Web Access Configuration
◆ **An Apache Alias That Will Point to the iFolder Web Access Application:** This is a user-friendly pointer for the Apache service. **Default:** /ifolder
◆ **The Host or IP Address of the iFolder Server That Will Be Used by the iFolder Web Access Application:** This Web Access application performs all the user-specific iFolder operations on the host that runs the iFolder Enterprise Server. **Default:** The IP address of the OES server you are installing
◆ **Redirect URL for iChain/Access Gateway (optional):** Specify the redirect URL for iChain/ Access Gateway that will be used by the iFolder Web Access application. This URL is used for the proper logout of iChain/Access Gateway sessions along with the iFolder session.
◆ **Connect to the iFolder Server Using SSL:** Select the check box to establish a secure connection between the iFolder enterprise server and the iFolder Web Admin application. **Default:** Selected
◆ **iFolder Server Port to Connect on:** Specify the port for the iFolder server to connect to the Web Access application. **Default:** 443 (SSL communications), 80 (non-SSL communication)
◆ **Require a secure connection between the web browser and the iFolder Web Access application:** Select the check box to establish a secure connection between the web browser and the iFolder Web Access application. **Default:** Selected
Novell iFolder Web Admin Configuration
◆ **An Apache Alias That Will Point to the iFolder Web Admin Application:** This is an admin-friendly pointer for the Apache service. **Default:** /admin
◆ **The Host or IP Address of the iFolder Server That Will Be Used by the iFolder Web Application:** The iFolder Web Admin application manages this host. **Default:** The IP address of the OES server you are installing

Page and Parameters
- **Redirect URL for iChain/Access Gateway (optional):** Specify the redirect URL for iChain/ Access Gateway that will be used by the iFolder Web Admin application. This URL is used for the proper logout of iChain/Access Gateway sessions along with the iFolder session.
- **Connect to the iFolder Server Using SSL:** Select the check box to establish a secure connection between the iFolder Enterprise Server and the iFolder Web Admin application.
- **iFolder Server Port to Connect on:** Specify the port for the iFolder server to connect to the Web Admin application. Port 443 is the default. Port 80 is the default value for non-SSL communication.
- **Require a secure connection between the web browser and the iFolder Web Access application:** Select the check box to establish a secure connection between the web browser and the iFolder Web Admin application.

For additional configuration instructions, see “Installing and Configuring iFolder Services” in the *Novell iFolder 3.9.2 Administration Guide*.

Novell iManager

Table 3-14 *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” in the *NetIQ iManager Installation Guide*.

Novell iPrint

Table 3-15 Novell iPrint Parameters and Values

Page and Parameters
iPrint Configuration
◆ **Directory server address:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add another LDAP server to the list, add it by using the LDAP Configuration for Open Enterprise Services dialog box.
◆ **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 `/etc/opt/novell/iprint/httpd/conf/iprint_ssl.conf`. For most installations, this is adequate because users are often distributed across containers. **IMPORTANT:** If you have multiple peer containers at the top of your eDirectory tree, leave this field blank so that the LDAP search begins at the root of the tree.

For additional configuration instructions, see "Installing and Setting Up iPrint on Your Server" in the *OES 11 SP3: iPrint Linux Administration Guide*.

Novell Linux User Management

Table 3-16 Novell Linux User Management Parameters and Values

Page and Parameters
Linux User Management Configuration
◆ **Directory Server Address:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add another LDAP server to the list, add it by using the LDAP Configuration for Open Enterprise Services dialog box. For information about specifying multiple LDAP servers for Linux User Management (LUM), see "Configuring a Failover Mechanism" in the *OES 11 SP3: Novell 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 11 SP3: 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 11 SP3: 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 ◆ **sfcbd: 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 11 SP3: Novell Linux User Management Administration Guide*.

Novell NCP Server / Dynamic Storage Technology

Table 3-17 *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 11 SP3: NCP Server for Linux Administration Guide*.

Novell NetStorage

Table 3-18 *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 11 SP3: 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 11 SP3: NetStorage Administration Guide for Linux*.

Novell Pre-Migration Server

No additional configuration is required. For information, see "Preparing the Source Server for Migration" the *OES 11 SP3: Migration Tool Administration Guide*.

Novell QuickFinder

Table 3-19 *Novell QuickFinder Parameters and Values*

Page and Parameters
Novell QuickFinder Admin User
- **Novell QuickFinder Admin User Type:** Make the QuickFinder administrator a LUM-enabled eDirectory user or a local Linux user.   - **Local**: Select this option to give QuickFinder Server administration rights to a local Linux user (the default is the `root` user if no other local users exist).   - **Directory LUM Enabled**: Gives QuickFinder Server administration rights to an eDirectory user. **Default:** Directory LUM enabled

Page and Parameters
◆ **QuickFinder Admin Name:** Specify the QuickFinder administrator name. If you selected **Directory LUM enabled** as the user type, include the full context (such as cn=admin,o=novell). If you selected **Local** as the user type, specify only the admin name (such as root). If the user does not already exist, it is created. **Default:** The eDirectory Admin user you specified while configuring eDirectory
◆ **Add novlwww User to the Shadow Group:** If only LUM-enabled eDirectory users will use QuickFinder, this option does not need to be set. QuickFinder uses Pluggable Authentication Modules (PAM) to authenticate users for both administration and rights-based searching. Because QuickFinder is a servlet under Tomcat, it has the same rights to the system as the Tomcat user (wwwrun). For QuickFinder to verify user credentials for local users (including root), the wwwrun user must be added to the local shadow group. **Default:** Yes
Novell QuickFinder Admin Password
◆ **eDirectory Admin Name:** Specified on the previous page.
◆ **Novell QuickFinder Admin User Type:** If a different admin user was created, specify a password.

For additional configuration instructions, see "Installing QuickFinder Server" in the *OES 11 SP3: Novell QuickFinder Server 5.0 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 11 SP3: Novell Remote Manager Administration Guide*.

Novell Samba

Table 3-20 *Novell Samba Parameters and Values*

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

Page and Parameters
◆ **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 11 SP3: Planning and Implementation Guide*.

For additional configuration instructions, see "Installing the Novell Samba Components" in the *OES 11 SP3: Novell Samba Administration Guide*.

Novell Storage Services (NSS)

Table 3-21 *Novell Storage Services Parameters and Values*

Page and Parameters
NSS Unique Admin Object
◆ **Directory Server Address:** The IP address shown is the default LDAP server for this service. If you do not want to use the default, select a different LDAP server in the list. If you are installing into an existing tree, ensure that the server you select has a master replica or read/write replica of eDirectory. If you need to add another LDAP server to the list, add it by using the LDAP Configuration for Open Enterprise Services dialog box. **Default** The first server selected in the **LDAP Configuration** list of servers.
◆ **Unique object Name for NSS Admin of This:** Specify the NSS Admin name and context or accept the default. This is the fully distinguished name of a User object with administrative rights to NSS. You must have a unique NSS admin name for each server that uses NSS. For more information, see "Planning Your Proxy Users" in the *OES 11 SP3: Planning and Implementation Guide*. **Default:** The server hostname concatenated with the LDAP Admin Name you entered for this server,. cn=*myserver*admin,o=*organization*.

For additional configuration instructions, see "Installing and Configuring Novell Storage Services" in the *OES 11 SP3: NSS File System Administration Guide for Linux*.

3.9 Finishing the Installation

The installation concludes with the following steps:

1. User Authentication Method
2. Clean Up
3. Release Notes
4. Hardware Configuration

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 8, “Using AutoYaST to Install and Configure Multiple OES Servers,” on page 177.

2 Finish the installation by clicking **Finish** in the Installation Completed page.

3 After the server reboots, continue with Section 3.10, “Verifying That the Installation Was Successful,” on page 106.

3.10 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 reboot. As each component is loaded, the boot logger provides a status next to it indicating if the component is loading properly.

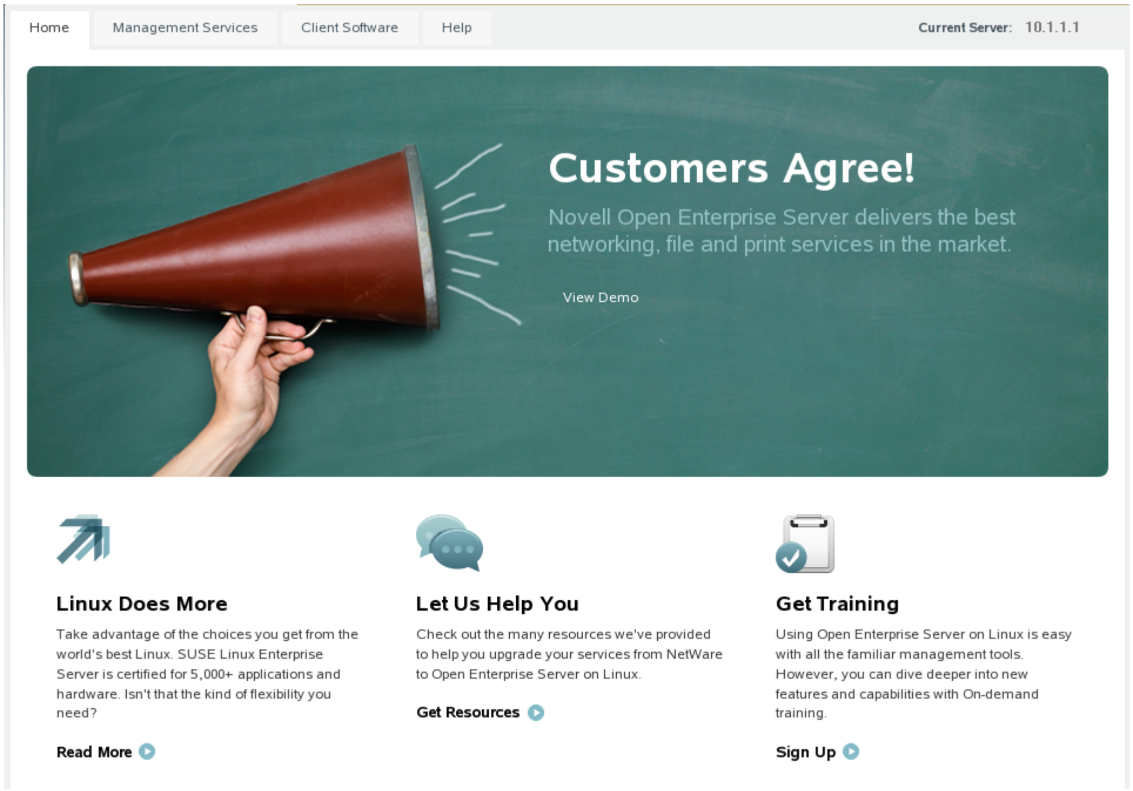
You can also quickly verify a successful installation by accessing the server from your web browser.

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:



Customers Agree!

Novell Open Enterprise Server delivers the best networking, file and print services in the market.

Linux Does More

Take advantage of the choices you get from the world's best Linux. SUSE Linux Enterprise Server is certified for 5,000+ applications and hardware. Isn't that the kind of flexibility you need?

Let Us Help You

Check out the many resources we've provided to help you upgrade your services from NetWare to Open Enterprise Server on Linux.

Get Training

Using Open Enterprise Server on Linux is easy with all the familiar management tools. However, you can dive deeper into new features and capabilities with On-demand training.

IMPORTANT: If you see the statement “It Works!” instead of the OES Welcome Page, that means that the web and LAMP Server option was selected and installed as a SLES component on the server. The default OES behavior can be restored either by deleting the `/srv/www/htdocs/index.html` file from the server or renaming the index.html file to a different name.

You can also view the OES Welcome Page by using http://*IP_or_DNS*/welcome to access the server.

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/iManager.html
```

3 Continue with “What's Next” on page 107.

3.11 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 159.

4 Installing or Configuring OES 11 SP3 on an Existing Server

After installing or upgrading to Novell Open Enterprise Server (OES 11 SP3), you can also install additional products or services and configure them to work in the new environment. If you have installed or upgraded a server to SUSE Linux Enterprise Server (SLES) 11 SP4, you can also add OES 11 SP3 services to the server.

- Section 4.1, “Before You Install OES Services on an Existing Server,” on page 109
- Section 4.2, “Adding/Configuring OES Services on an Existing Server,” on page 110
- Section 4.3, “Adding/Configuring OES Services on a Server That Another Administrator Installed,” on page 114
- Section 4.4, “What's Next,” on page 114

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 Before You Install OES Services on an Existing Server

In addition to the information in “Planning Your OES 11 SP3 Implementation” in the *OES 11 SP3: Planning and Implementation Guide*, the following apply when you install OES on an existing server:

- Section 4.1.1, “Always Use YaST to Install and Initially Configure OES Services,” on page 109
- Section 4.1.2, “Don’t Install OES While Running the Xen Kernel,” on page 110
- Section 4.1.3, “If You Want OES to Use a Local eDirectory Database on the Server,” on page 110

4.1.1 Always Use YaST to Install and Initially Configure OES Services

Linux administrators sometimes wrongly assume that OES services can be installed or uninstalled by simply installing the associated RPMs. OES services require additional configuration that is only supported as an add-on product installation in YaST.

IMPORTANT: You must always install OES as an add-on product using the YaST install. For more information, see Section 2.10, “Always Install OES as an Add-On Product,” on page 40.

4.1.2 Don’t Install OES While Running the Xen Kernel

If you are adding supported OES 11 SP3 components to a server that is running the Xen kernel, you must reset the boot loader to boot the standard kernel before adding the OES 11 SP3 components.

1 In YaST, select **System > Boot Loader > SUSE Linux Enterprise Server 11 SP4 > Set As Default > Finish**.

2 Reboot the server.

After adding the supported OES 11 SP3 components, reset the boot loader option to Xen.

1 In YaST, select **System > Boot Loader > XEN > Set As Default > Finish**.

2 Reboot the server.

Be sure to add only those OES 11 SP3 components that are supported on a VM host server. For more information, see Step 7 on page 187.

4.1.3 If You Want OES to Use a Local eDirectory Database on the Server

If you want the OES components to use a local eDirectory database, you should install eDirectory by itself first, and then rerun the installation for the other OES components.

4.2 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 4.3, “Adding/Configuring OES Services on a Server That Another Administrator Installed,” on page 114.

To add/configure OES 11 SP3 services on an existing OES 11 SP3 server or SLES 11 SP4 server:

1 Open YaST.

2 If an OES 11 SP3 installation source has not been added to the server, continue with this step. Otherwise, skip to Step 3.

2a Click **Software** > **Add-on Product**s.

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 *Open Enterprise Server 11 SP3 DVD 1*.

2e Click **Eject**.

2f Insert the DVD labeled *Open Enterprise Server 11* SP3, then click **Continue**.

2g Read and accept the Novell Open Enterprise Server 11 SP3 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, click **Open Enterprise Server** > **OES Install and Configuration**.

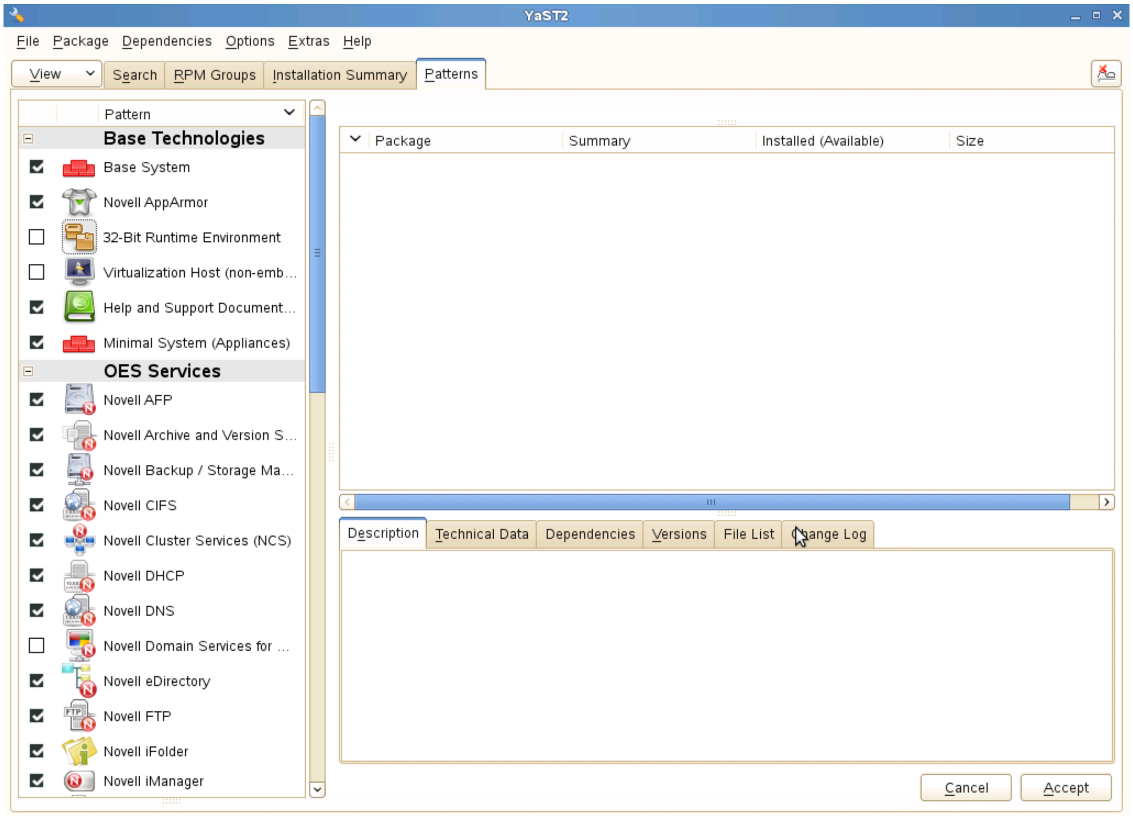
4 On the Software Selection page, select the OES components that you want to install or configure.

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.

IMPORTANT: You cannot uninstall an OES service by deselecting it. For more information about removing service functionality from the server, see Chapter 13, “Disabling OES 11 Services,” on page 215.

---

5 If you are only configuring or reconfiguring services that are already installed, click **Accept**, then skip to Step 9.



Base Technologies
- ☑ Base System
- ☑ Novell AppArmor
- ☐ 32-Bit Runtime Environment
- ☐ Virtualization Host (non-emb…
- ☑ Help and Support Document…
- ☑ Minimal System (Appliances)

OES Services
- ☑ Novell AFP
- ☑ Novell Archive and Version S…
- ☑ Novell Backup / Storage Ma…
- ☑ Novell CIFS
- ☑ Novell Cluster Services (NCS)
- ☑ Novell DHCP
- ☑ Novell DNS
- ☐ Novell Domain Services for …
- ☑ Novell eDirectory
- ☑ Novell FTP
- ☑ Novell iFolder
- ☑ Novell iManager

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

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

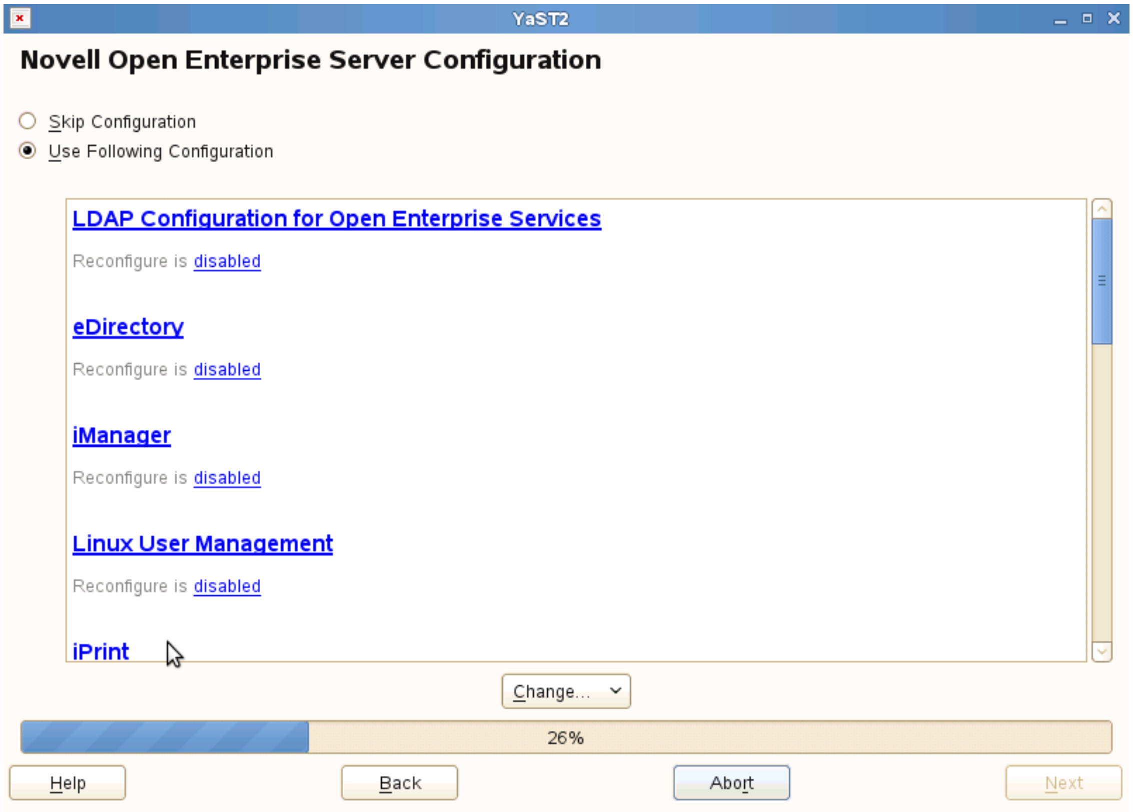
If you need to reconfigure eDirectory and OES services due to database corruption, go to Chapter 14, “Reconfiguring eDirectory and OES Services,” on page 217 and follow the instructions there.

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.



Novell Open Enterprise Server Configuration

○ Skip Configuration
● Use Following Configuration

LDAP Configuration for Open Enterprise Services

Reconfigure is disabled

eDirectory

Reconfigure is disabled

iManager

Reconfigure is disabled

Linux User Management

Reconfigure is disabled

iPrint

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 3.8.12, "Configuration Guidelines for OES Services," on page 78 or click a link below:

- AFP
- Archive and Version Services
- Backup/Storage Management Services (SMS)
- CIFS
- Clustering (NCS)
- DHCP
- DNS
- Domain Services for Windows (DSfW)
- eDirectory
- FTP
- iFolder
- iManager
- iPrint
- Linux User Management (LUM)
- NCP Server/Dynamic Storage Technology
- NetStorage
- Pre-Migration Server
- QuickFinder
- Novell Remote Manager (NRM)
- Novell Samba
- Novell Storage Services

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**.

12 If you are installing on an existing OES server, you can quit the installation at this point.

If you are installing OES services for the first time on this server, see Section 3.8.5, "Specifying Novell Customer Center Configuration Settings," on page 59 for help with registering OES and updating the software.

4.3 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 Novell 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 112 in Section 4.2, "Adding/Configuring OES Services on an Existing Server," on page 110 and continue from there.

4.4 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 159.

5 Upgrading to OES 11 SP3

Novell Open Enterprise Server (OES) 11 SP3 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.

5.1 Supported Upgrade Paths

Table 5-1 outlines the supported paths for upgrading to OES 11 SP3.

All OES releases can be upgraded by installing the interim support packs in order. For example, you can upgrade from OES 2 SP2 to OES 2 SP3, then from OES 2 SP3 to OES 11 SP3. Cross-architecture upgrades (32-bit to 64-bit and 64-bit to 32-bit) are not supported.

Table 5-1 *Supported OES 11 SP3 Upgrade Paths*

Source	Destination	Upgrade Methods Supported
OES 2 SP3 (64-bit)	OES 11 SP3 (64-bit)	Network-based media (offline) Physical media (offline)
OES 11 SP1 (64-bit)	OES 11 SP3 (64-bit)	Network-based media (offline) Physical media (offline)
OES 11 SP2 (64-bit)	OES 11 SP3 (64-bit)	Network-based media (offline) Physical media (offline) Channel or patch upgrade

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

5.2 Planning for the Upgrade to OES 11 SP3

- Section 5.2.1, “Be Sure to Check the Readme,” on page 116
- Section 5.2.2, “Always Upgrade SLES and OES at the Same Time,” on page 116
- Section 5.2.3, “Understanding the Implications for Other Products Currently Installed on the Server,” on page 116

5.2.1 Be Sure to Check the Readme

The “Before You Install” section documents issues that Novell plans to address in a future release.

5.2.2 Always Upgrade SLES and OES at the Same Time

You must upgrade SLES and OES at the same time.

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

- “OES 2 Server Upgrades: Non-OES 2 Packages Are Retained but Might Not Work After Upgrading” on page 116

OES 2 Server Upgrades: Non-OES 2 Packages Are Retained but Might Not Work After Upgrading

During the upgrade process from earlier OES 2 releases to OES 11 SP3, packages that are not part of the SLES 11 SP4 and OES 11 SP3 distributions are automatically retained unless you select them for deletion.

This includes third-party products you have installed, as well as other Novell 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 Novell product installed.

For Information About This Novell 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 SLES 11 SP4 and follow the upgrade instructions that should be included with it.

5.3 Meeting the Upgrade Requirements

Meet the following requirements before you upgrade and install any OES 11 SP3 components:

- Section 5.3.1, “Securing Current Data,” on page 117
- Section 5.3.2, “Ensuring That There Is Adequate Storage Space on the Root Partition,” on page 117
- Section 5.3.3, “Preparing the Server You Are Upgrading,” on page 118
- Section 5.3.4, “Checking the Server’s IP Address,” on page 118
- Section 5.3.5, “Checking the Server’s DNS Name,” on page 119
- Section 5.3.6, “Ensuring That the Server Has a Server Certificate,” on page 119
- Section 5.3.7, “Changing the Mount Options Before an Upgrade,” on page 119
- Section 5.3.8, “Preparing an Installation Source,” on page 122

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.

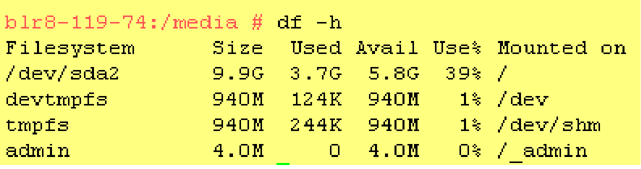
5.3.2 Ensuring That There Is Adequate Storage Space on the Root Partition

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.

WARNING: If you require more root partition space and if it resides in an EVMS container, you might not be able to repartition or expand the size of the root partition without deleting data elsewhere on the device.

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.



```
blr8-119-74:/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

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
SLES 10 SP3	1. Ensure that the products and services you have running on the server can run on the new SLES 11 SP4 kernel. 2. Download and update the latest Sentinel agent from (http://support.novell.com/products/sentinel/secure/sentinelplugins.html). Failing to update the agent could result in SLES 11 booting issues. 3. Ensure that the mount options for all the partitions in SLES 10 are set to **Device ID** or **Device Path**. For more information, see Section 5.3.7, "Changing the Mount Options Before an Upgrade," on page 119. 4. Ensure that the server meets the hardware requirements for SLES 11 SP4. See "System Requirements for Operating Linux" in the *Deployment Guide* (http://www.suse.com/documentation/sles11/book_sle_deployment/data/sec_x86_sysreqs.html). Itanium is not a supported platform for OES 11. 5. See the SLES 11 SP4 entry.
SLES 11 SP4	1. See Chapter 4, "Installing or Configuring OES 11 SP3 on an Existing Server," on page 109.
OES 2 SP3	1. Run **YaST > Software > Online Update** to patch the OES 2 SP3 server to the latest patch level. 2. Ensure that the server and services are still running as desired. 3. Upgrade to OES 11 SP3 using the instructions in this section, then apply all patches and verify services.
OES 11 SP1	1. Run **YaST > Software > Online Update** to patch the OES 11 SP1 server to the latest patch level. 2. Ensure that the server and services are still running as desired. 3. Upgrade to OES 11 SP3 using the instructions in this section, then apply all patches and verify services.
OES 11 SP2	1. Run **YaST > Software > Online Update** to patch the OES 11 SP2 server to the latest patch level. 2. Ensure that the server and services are still running as desired. 3. Upgrade to OES 11 SP3 using the instructions in this section, then apply all patches and verify services.

5.3.4 Checking the Server's IP Address

Ensure the server has a static IP address.

5.3.5 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
```

5.3.6 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**.

5.3.7 Changing the Mount Options Before an Upgrade

Before starting the upgrade from OES2 to OES11 SP3, ensure that the mount options for all the partitions are set to **Device ID** or **Device Path**. The default mount option in SLES 10 is **Kernel Device Name**, which is not persistent, and therefore it is unreliable for use during an upgrade process.

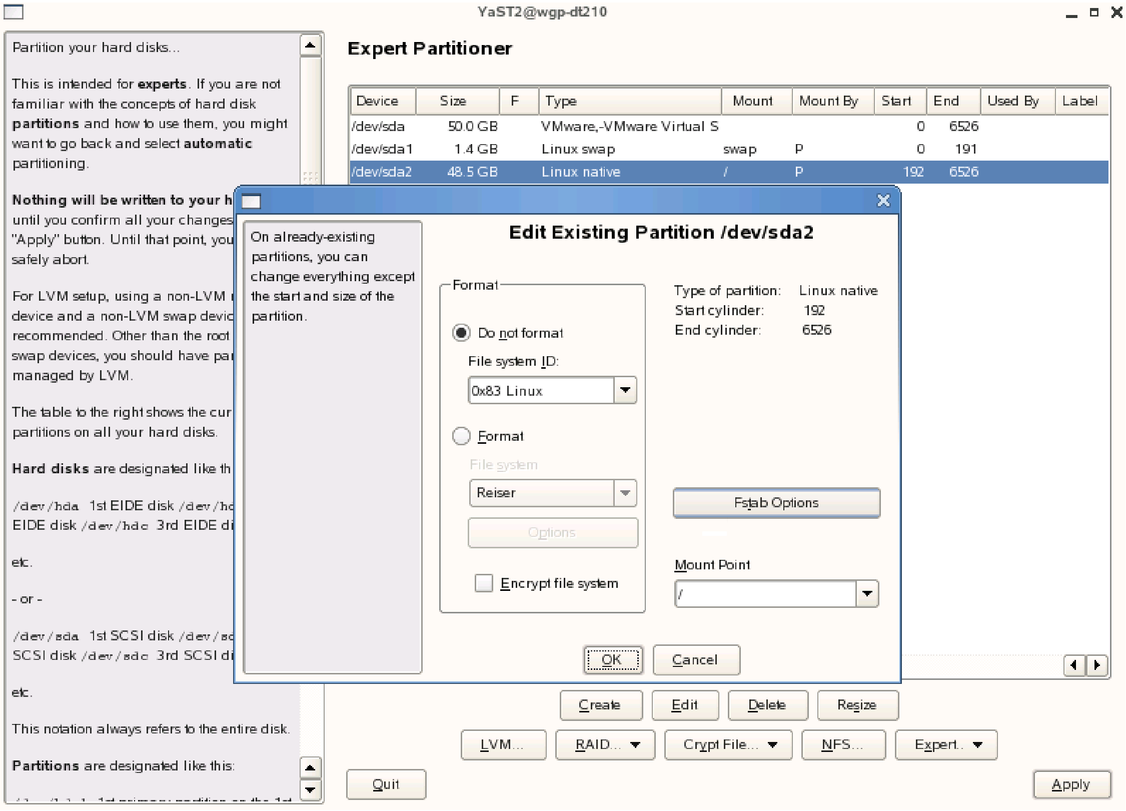
IMPORTANT: Mount options should not be changed when you are upgrading an OES 2 SP3 instance installed on XEN whose `root` partition is on EVMS. Before starting the upgrade, apply the latest patches for OES 2 SP3 and SLES 10, then proceed with the upgrade to OES 11 SP3.

NOTE: After performing this procedure, do not attempt to boot the OES2 server. Instead, start the upgrade to OES11 SP3.

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

1. Log on to the OES2 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**.



Partition your hard disks...

This is intended for **experts**. If you are not familiar with the concepts of hard disk **partitions** and how to use them, you might want to go back and select **automatic** partitioning.

Nothing will be written to your h
until you confirm all your changes
"Apply" button. Until that point, you
safely abort.

For LVM setup, using a non-LVM r
device and a non-LVM swap devic
recommended. Other than the root
swap devices, you should have pa
managed by LVM.

The table to the right shows the cur
partitions on all your hard disks.

Hard disks are designated like th

/dev/hda 1st EIDE disk /dev/hc
EIDE disk /dev/hdc 3rd EIDE di

etc.

- or -

/dev/sda 1st SCSI disk /dev/sc
SCSI disk /dev/sdc 3rd SCSI di

etc.

This notation always refers to the entire disk.

Partitions are designated like this:

Expert Partitioner

Device	Size	F	Type	Mount	Mount By	Start	End	Used By	Label
/dev/sda	50.0 GB		VMware,-VMware Virtual S			0	6526		
/dev/sda1	1.4 GB		Linux swap	swap	P	0	191		
/dev/sda2	48.5 GB		Linux native	/	P	192	6526		

Edit Existing Partition /dev/sda2

On already-existing partitions, you can change everything except the start and size of the partition.

Format

● Do not format

File system ID: 0x83 Linux

○ Format

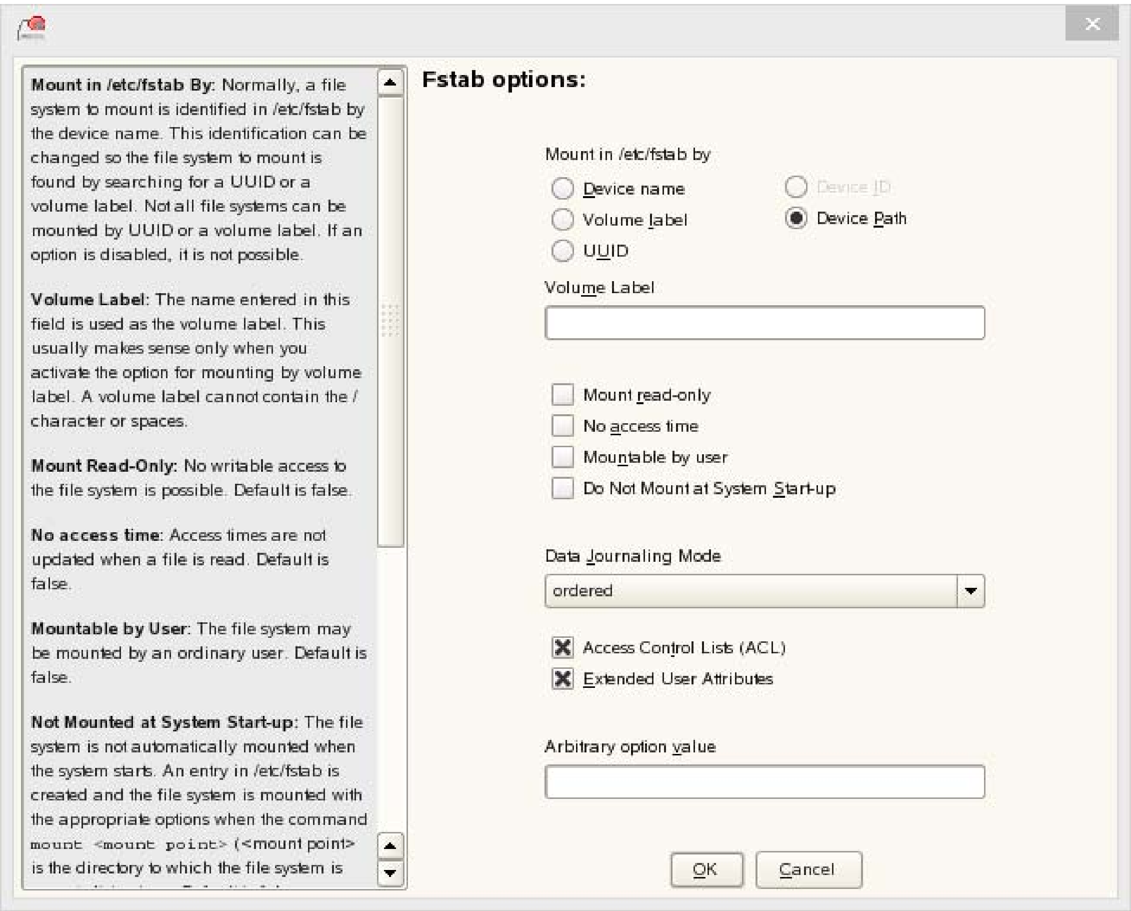
File system: Reiser

□ Encrypt file system

Type of partition: Linux native
Start cylinder: 192
End cylinder: 6526

Mount Point: /

5 Under **Fstab options:**, click **Device ID or Device path > OK > OK**.



Mount in /etc/fstab By: Normally, a file system to mount is identified in /etc/fstab by the device name. This identification can be changed so the file system to mount is found by searching for a UUID or a volume label. Not all file systems can be mounted by UUID or a volume label. If an option is disabled, it is not possible.

Volume Label: The name entered in this field is used as the volume label. This usually makes sense only when you activate the option for mounting by volume label. A volume label cannot contain the / character or spaces.

Mount Read-Only: No writable access to the file system is possible. Default is false.

No access time: Access times are not updated when a file is read. Default is false.

Mountable by User: The file system may be mounted by an ordinary user. Default is false.

Not Mounted at System Start-up: The file system is not automatically mounted when the system starts. An entry in /etc/fstab is created and the file system is mounted with the appropriate options when the command `mount <mount point>` (<mount point> is the directory to which the file system is

Fstab options:

Mount in /etc/fstab by

○ Device name ○ Device ID
○ Volume label ● Device Path
○ UUID

Volume Label

□ Mount read-only
□ No access time
□ Mountable by user
□ Do Not Mount at System Start-up

Data Journaling Mode: ordered

☒ Access Control Lists (ACL)
☒ Extended User Attributes

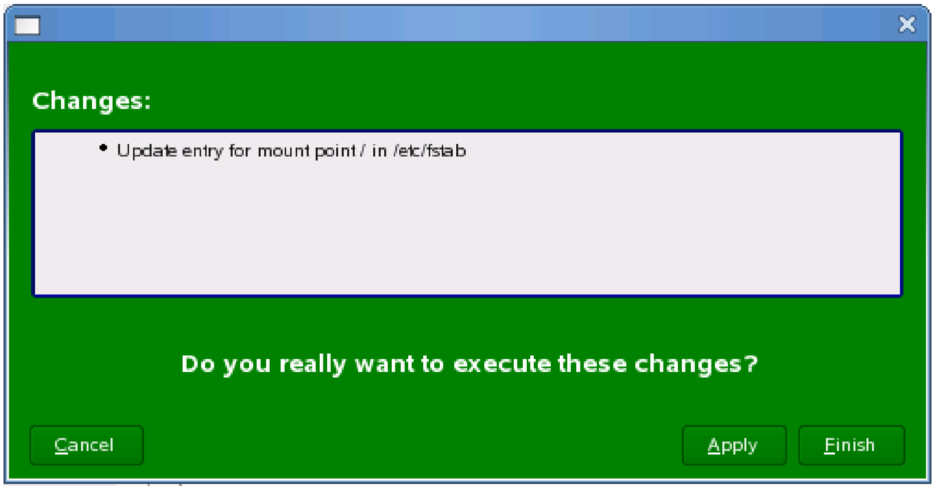
Arbitrary option value

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 120 for all the partitions.

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

8 In the **Change**s: dialog box, click **Finish**.


Changes:

- Update entry for mount point / in /etc/fstab

Do you really want to execute these changes?

The mount options are successfully changed.

5.3.8 Preparing an Installation Source

Review and complete the instructions for "Setting Up a Network Installation Source" on page 36. We recommend using the network installation option, especially if you are upgrading multiple servers.

5.4 Upgrading to OES 11 SP3

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

- Section 5.4.1, "For Servers with EVMS and LVM on the System Device," on page 123
- Section 5.4.2, "To Upgrade Using a Network Installation Source with DHCP (Offline)," on page 123
- Section 5.4.3, "Upgrading Using a Network Installation Source without DHCP (Offline)," on page 124
- Section 5.4.4, "Using Physical Media to Upgrade (Offline)," on page 126
- Section 5.4.5, "Selecting the Installation Mode Options," on page 126
- Section 5.4.6, "Specifying the Partition to Update," on page 127
- Section 5.4.7, "Specifying the Add-On Product Installation Information," on page 129
- Section 5.4.8, "Verifying and Customizing the Update Options in Installation Settings," on page 129
- Section 5.4.9, "Accepting the Installation Settings," on page 134
- Section 5.4.10, "Specifying Configuration Information," on page 134

5.4.1 For Servers with EVMS and LVM on the System Device

If you are attempting to upgrade an OES 2 SP3 server that has boot and swap partitions controlled by EVMS, to OES 11 SP3, you must manually perform the following steps before the system reboots in order to restore the boot and swap disks to the default `/dev/system/sys_lx` directory.

Do the following before the system reboots:

1. Update the `/etc/fstab` file by removing `/evms/lvm2` from the swap and root partitions, then modify the `/dev/evms/` path for `/boot` to `/dev`.
2. Remove the `/evms/lvm2` path from the `/boot/grub/menu.lst` file. Optionally, verify that the `/etc/sysconfig/bootloader` file has the correct entry for the boot device.

5.4.2 To Upgrade Using a Network Installation Source with DHCP (Offline)

1. Ensure that the server meets the upgrade requirements. See "Meeting the Upgrade Requirements" on page 117.
2. Insert the *SUSE Linux Enterprise Server 11 SP4 DVD* into the DVD drive of the server you want to upgrade to OES 11 SP3, then reboot the server.
3. From the boot menu, select one of the following Installation options that matches your environment, but do not press Enter.
   - **Installation:** The normal installation mode. All modern hardware functions are enabled.
   - **Installation—ACPI Disabled:** If the normal installation fails, it might be because the system hardware does not support ACPI (advanced configuration and power interface). If this seems to be the case, use this option to install without ACPI support.
   - **Installation—Local APIC Disabled:** If the normal installation fails, it might be because the system hardware does not support local APIC (advanced programmable interrupt controllers). If this seems to be the case, use this option to install without local APIC support.

     If you are not sure, try **Installation—ACPI Disabled** or **Installation—Safe Settings** first.
   - **Installation—Safe Settings:** Boots the system with the DMA mode (for DVD drives) and power management functions disabled. Experts can also use the command line to enter or change kernel parameters.
4. Specify the network installation source.

   Because your network has DHCP, you don't need to specify an IP address for the server. However, you do need to specify the path to your network installation source.

   Do one of the following:
   - Press F4. Select the network installation type (NFS, FTP, HTTP). Type the server name and installation path of your network installation source, then click OK.

     For more information, see "Setting Up a Network Installation Source" on page 36.

     or
   - Specify the network installation type and path using the **Boot Options** line (see "Using Custom Boot Options" in the *SUSE Linux Enterprise Server Installation and Administration Guide* (http://www.suse.com/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html)).
5. Press Enter to begin the upgrade.

6 Select a language, then click **Next**.

7 On the License Agreement page, click **Yes, I Agree to the License Agreement** > **Next**.

8 Follow the prompts, using the information contained in the following sections:

- 8a “Selecting the Installation Mode Options” on page 126.
- 8b “Specifying the Partition to Update” on page 127.
- 8c “Specifying the Add-On Product Installation Information” on page 129.
- 8d “Verifying and Customizing the Update Options in Installation Settings” on page 129.
- 8e “Accepting the Installation Settings” on page 134.
- 8f “Specifying Configuration Information” on page 134.
- 8g “Finishing the Upgrade” on page 143.

9 Verify that the upgrade was successful. See the procedures in “Verifying That the Installation Was Successful” on page 106.

10 Complete the server setup by following the procedures in “Completing OES Installation or Upgrade Tasks” on page 159.

5.4.3 Upgrading Using a Network Installation Source without DHCP (Offline)

1 Ensure that the server meets the upgrade requirements. See “Meeting the Upgrade Requirements” on page 117.

2 Insert *SUSE Linux Enterprise Server 11 SP4 DVD* into the DVD drive of the server that you are upgrading to OES 11 SP3, then reboot the machine.

3 From the DVD boot menu, select one of the following Installation options that matches your environment, but do not press Enter.

- **Installation:** The normal installation mode. All modern hardware functions are enabled.
- **Installation—ACPI Disabled:** If the normal installation fails, it might be because the system hardware does not support ACPI (advanced configuration and power interface). If this seems to be the case, use this option to install without ACPI support.
- **Installation—Local APIC Disabled:** If the normal installation fails, this might be because the system hardware does not support local APIC (advanced programmable interrupt controllers). If this seems to be the case, use this option to install without local APIC support.

  If you are not sure, try I**nstallation—ACPI Disabled** or **Installation—Safe Settings** first.
- **Installation—Safe Settings:** Boots the system with the DMA mode (for DVD drives) and power management functions disabled. Experts can also use the command line to enter or change kernel parameters.

4 To proceed with the upgrade, your server must have the following:

- An IP address assigned
- The location of your network installation source

To specify this information on the **Boot Options** line, proceed with Step 5.

To supply the information in a series of dialog boxes, skip to Step 7.

5 Specify the server’s IP address information and the path to the installation source on the **Boot Options** line (see “Using Custom Boot Options” in the *SUSE Linux Enterprise Server Deployment Guide* (https://www.suse.com/documentation/sles11/book_sle_deployment/data/sec_deployment_remoteinst_bootinst.html#sec_deployment_remoteinst_bootinst_custom)).

6 Press Enter and continue with Step 24.

7 Continuing from Step 4, press Enter.

The following error displays:

```
Could not find the SUSE Linux Enterprise Server 11 Installation source.
Activating manual set up program.
```

8 Press Enter.

9 Select the language, then select **OK** and press Enter.

10 Select a keyboard map, then select **OK** and press Enter.

11 Select **Start Installation or System**, then select **OK** and press Enter.

12 Select **Start Installation or Update**, then select **OK** and press Enter.

13 Select **Network**, then select **OK** and press Enter.

14 Select the network protocol that matches the configured protocol on your network installation server, then press Enter.

15 (Conditional) If you have more than one network interface card, select one of the cards, then press Enter.

We recommend eth0, if it is connected to the subnet for the primary static IP address used by the server you are upgrading.

16 When you are prompted whether you want to use DHCP, select **No**, then press Enter.

17 Specify the static IP address of the server you are upgrading, then press Enter.

18 Specify the subnet mask, then press Enter.

19 Specify the gateway, then press Enter.

20 Specify the IP addresses of a name server, then press Enter.

21 Specify the IP address of the network installation server, then press Enter.

22 (Conditional) Depending on the protocol you specified, you might see additional screens for FTP or HTTP. Select the options that are appropriate for your network, then continue with Step 23.

23 Specify the path to your installation source on the network installation server, then press Enter.

The installation system loads and the YaST install starts.

24 Select the language, then click **Next**.

25 On the License Agreement page, click **Yes, I Agree to the License Agreement** > **Next**.

26 Follow the prompts, using the information contained in the following sections:

26a "Selecting the Installation Mode Options" on page 126.

26b "Specifying the Partition to Update" on page 127.

26c "Specifying the Add-On Product Installation Information" on page 129.

26d "Verifying and Customizing the Update Options in Installation Settings" on page 129.

26e "Accepting the Installation Settings" on page 134.

26f "Specifying Configuration Information" on page 134.

26g "Finishing the Upgrade" on page 143.

27 Verify that the upgrade was successful. See the procedures in "Verifying That the Installation Was Successful" on page 106.

28 Complete the server setup by following the procedures in "Completing OES Installation or Upgrade Tasks" on page 159.

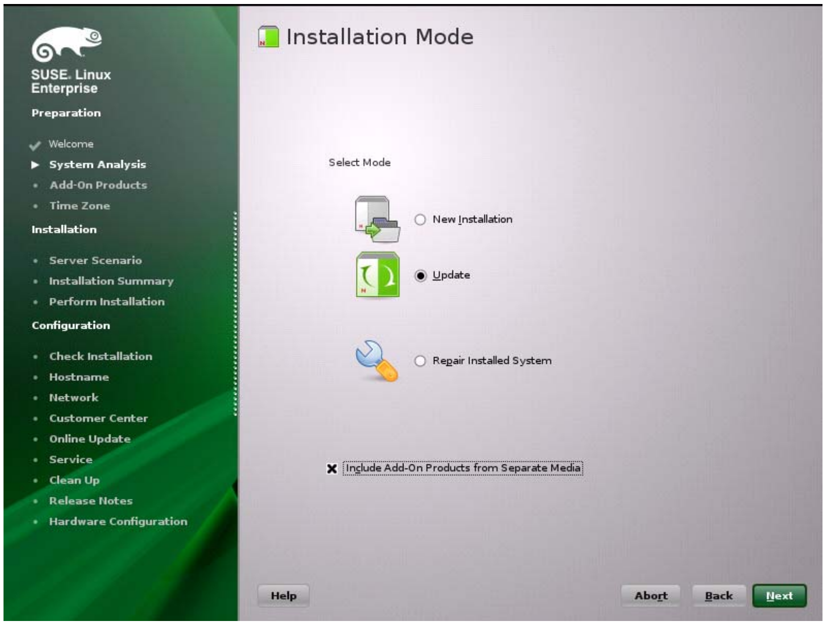
5.4.4 Using Physical Media to Upgrade (Offline)

1. Ensure that the server meets the upgrade requirements. See "Meeting the Upgrade Requirements" on page 117.
2. Insert the *SUSE Linux Enterprise Server 11 SP4 DVD* or the OES 11 SP3 Integrated DVD into the DVD drive of the server that you are upgrading to OES 11 SP3, then reboot the machine.
3. From the DVD boot menu, select the **Installation** option that best fits your environment, then press Enter.
4. Select the language that you want to use.
5. On the License Agreement page, click **Yes, I Agree to the License Agreement** > **Next**.
6. Follow the prompts, using the information contained in the following sections:
   - **6a** "Selecting the Installation Mode Options" on page 126.
   - **6b** "Specifying the Partition to Update" on page 127.
   - **6c** "Specifying the Add-On Product Installation Information" on page 129.
   - **6d** "Verifying and Customizing the Update Options in Installation Settings" on page 129.
   - **6e** "Accepting the Installation Settings" on page 134.
   - **6f** "Specifying Configuration Information" on page 134.
   - **6g** "Finishing the Upgrade" on page 143.
7. Verify that the upgrade was successful. See the procedures in "Verifying That the Installation Was Successful" on page 106.
8. Complete the server setup by following the procedures in "Completing OES Installation or Upgrade Tasks" on page 159.

5.4.5 Selecting the Installation Mode Options

1. When the Installation Mode page displays, select the following menu options:
   1. **Update**
   2. **Include Add-On Products from Separate Media**

IMPORTANT: To upgrade previously installed OES services and install any additional OES services, you must select the **Include Add-On Products from Separate Media** option. If you don't, only SLES is updated (if necessary). None of the OES services are upgraded.



Installation Mode

Select Mode

○ New Installation

● Update

○ Repair Installed System

☒ Include Add-On Products from Separate Media

2 Click **Next**.

3 Continue with "Specifying the Partition to Update" on page 127 or "Specifying the Add-On Product Installation Information" on page 129, depending on which matches your installation.

5.4.6 Specifying the Partition to Update

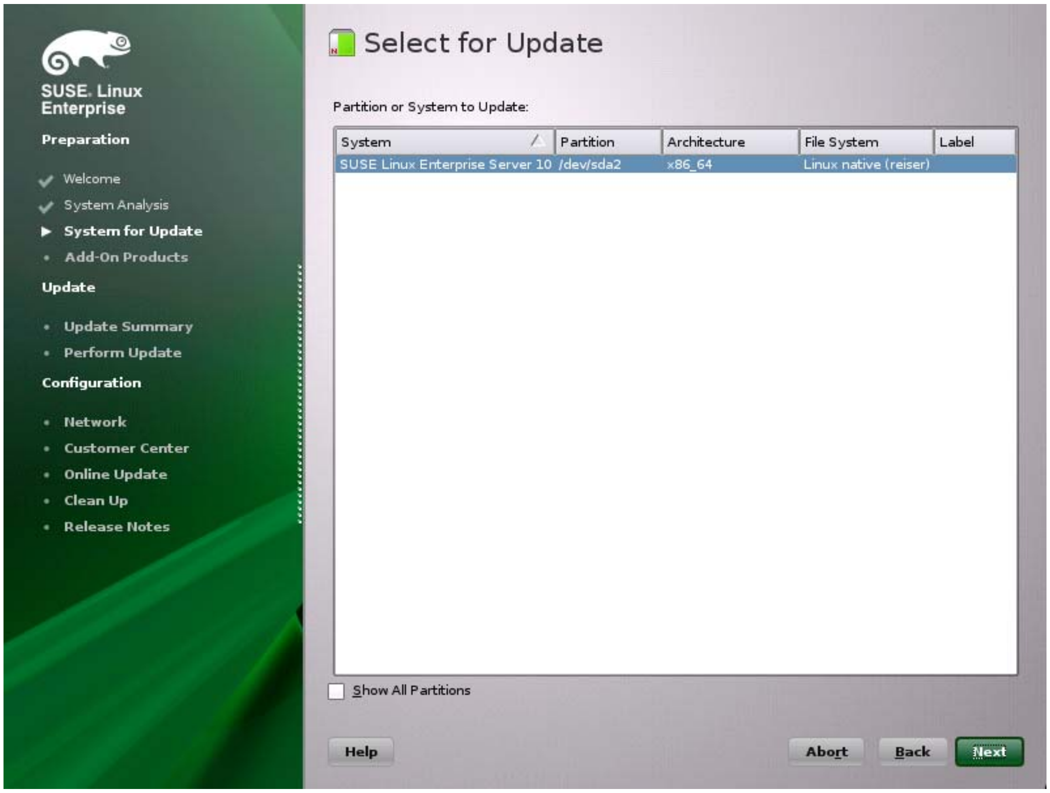
YaST tries to determine the correct root (/) partition. If there are several possibilities, or if YaST can't definitely determine the correct root partition, the Select for Update page displays.

1 If there is only one partition listed, click **Next**.

2 If there are several partitions, select the partition with `/lvm` in the path.

3 Click **Next**.

YaST reads the old fstab on this partition to analyze and mount the file systems listed there.



Select for Update

Partition or System to Update:

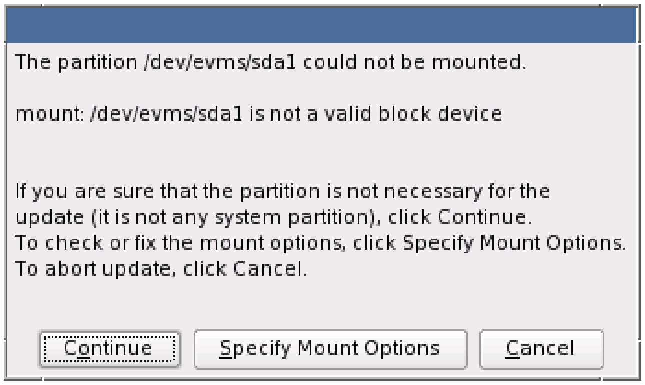
System	Partition	Architecture	File System	Label
SUSE Linux Enterprise Server 10	/dev/sda2	x86_64	Linux native (reiser)	

□ Show All Partitions

Next, YaST tries to mount the boot (`/boot`) partition.

4 If no error displays, skip to “Specifying the Add-On Product Installation Information” on page 129.

NOTE: Step 4 on page 128 and Step 5 on page 128 are applicable when you are upgrading from an OES 2 SP3 server.



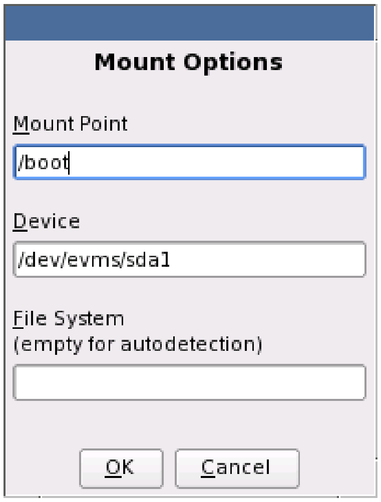
The partition /dev/evms/sda1 could not be mounted.

mount: /dev/evms/sda1 is not a valid block device

If you are sure that the partition is not necessary for the update (it is not any system partition), click Continue.
To check or fix the mount options, click Specify Mount Options.
To abort update, click Cancel.

5 If this error displays, click **Specify Mount Options**.

The Mount Options dialog box appears.



Mount Options

Mount Point: /boot

Device: /dev/evms/sda1

File System (empty for autodetection):

6 Click **OK**.

7 Continue with "Specifying the Add-On Product Installation Information" on page 129.

5.4.7 Specifying the Add-On Product Installation Information

1 When the Add-On Product Installation page displays, click **Add**.

2 In the Add-On Product Media page, if you are installing from physical media, click **DVD** > **Next**. Otherwise, skip to Step 3.

   2a In the Insert the Add-On Product DVD dialog box, select the drive where you want to insert the DVD labeled *Novell Open Enterprise Server 11 SP3 DVD* if there is more than one drive.

   2b Click **Eject**.

   2c Insert the DVD labeled *Novell Open Enterprise Server 11 SP3 DVD*, click **Continue**, then skip to Step 4.

3 If you are using an alternate installation source (such as a network location), click the appropriate option (such as the network protocol that matches your installation source), then click **Next** and specify the information for the source you have specified.

4 Read and accept the Novell Open Enterprise Server 11 SP3 license agreement, then click **Next**.

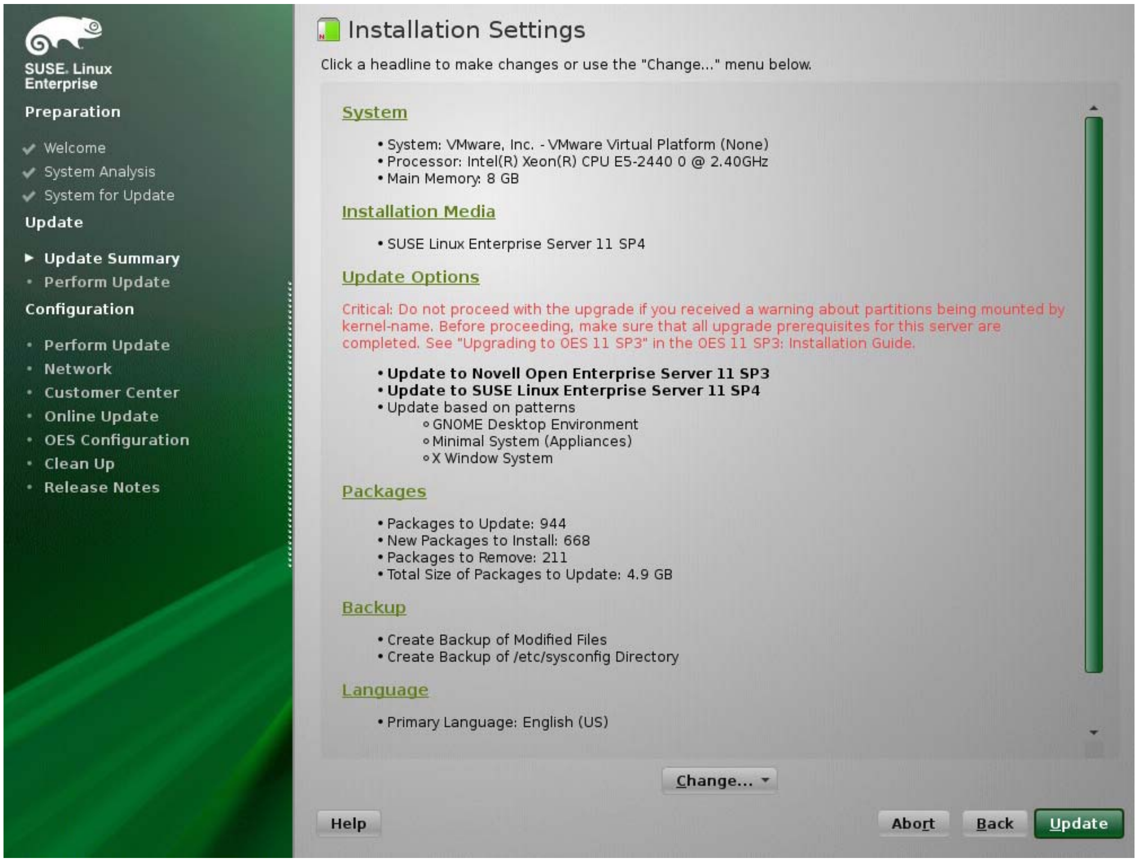
5 Confirm that the Add-On Product Installation page shows the correct path to the OES media, then click **Next**.

5.4.8 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, ensure Novell Open Enterprise Server 11 SP3 is listed under the **Add-On Products** link. If it is, proceed with Step 3.



Installation Settings

Click a headline to make changes or use the "Change..." menu below.

System

- System: VMware, Inc. - VMware Virtual Platform (None)
- Processor: Intel(R) Xeon(R) CPU E5-2440 0 @ 2.40GHz
- Main Memory: 8 GB

Installation Media

- SUSE Linux Enterprise Server 11 SP4

Update Options

Critical: Do not proceed with the upgrade if you received a warning about partitions being mounted by kernel-name. Before proceeding, make sure that all upgrade prerequisites for this server are completed. See "Upgrading to OES 11 SP3" in the OES 11 SP3: Installation Guide.

- **Update to Novell Open Enterprise Server 11 SP3**
- **Update to SUSE Linux Enterprise Server 11 SP4**
- Update based on patterns
  - GNOME Desktop Environment
  - Minimal System (Appliances)
  - X Window System

Packages

- Packages to Update: 944
- New Packages to Install: 668
- Packages to Remove: 211
- Total Size of Packages to Update: 4.9 GB

Backup

- Create Backup of Modified Files
- Create Backup of /etc/sysconfig Directory

Language

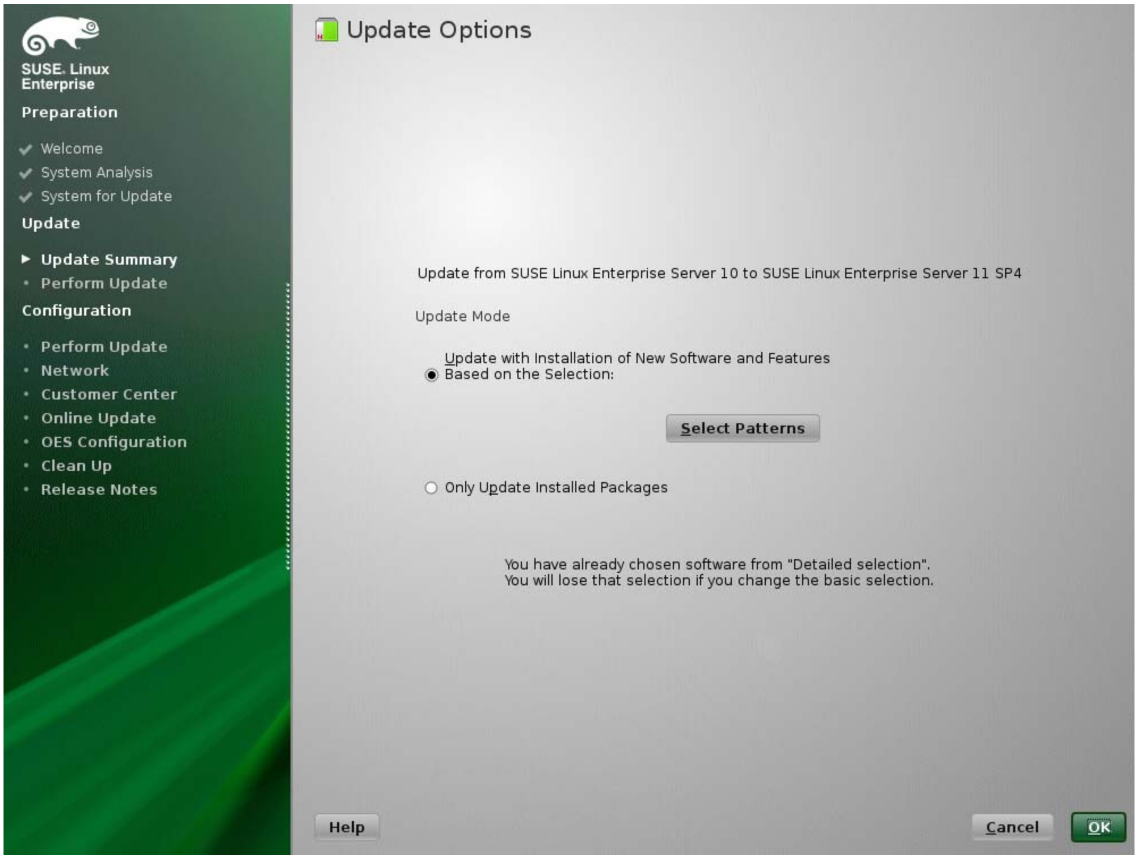
- Primary Language: English (US)

2 If Novell Open Enterprise Server is not listed, click the **Add-On Products** link and follow the steps in "Specifying the Add-On Product Installation Information" on page 129. When the Installation Settings page shows Novell Open Enterprise Server 11 SP3 as an installation setting, proceed with Step 3.

3 If you see package conflict errors (red text under the **Packages** link), refer to the *OES 11 SP3: Readme* for resolution instructions.

4 On the Installation Settings page, click **Update Options**.

5 In the Update Options page, click **Update with Installation of New Software and Features Based on the Selection > Select Patterns.**



Update Options

Update from SUSE Linux Enterprise Server 10 to SUSE Linux Enterprise Server 11 SP4

Update Mode

● Update with Installation of New Software and Features Based on the Selection:

○ Only Update Installed Packages

You have already chosen software from "Detailed selection".
You will lose that selection if you change the basic selection.

6 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 patterns 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 27.

Some OES services, such as Novell CIFS and Novell Samba, are not supported together on the same server. For more information, see “Unsupported Service Combinations” in the *OES 11 SP3: Planning and Implementation Guide*.

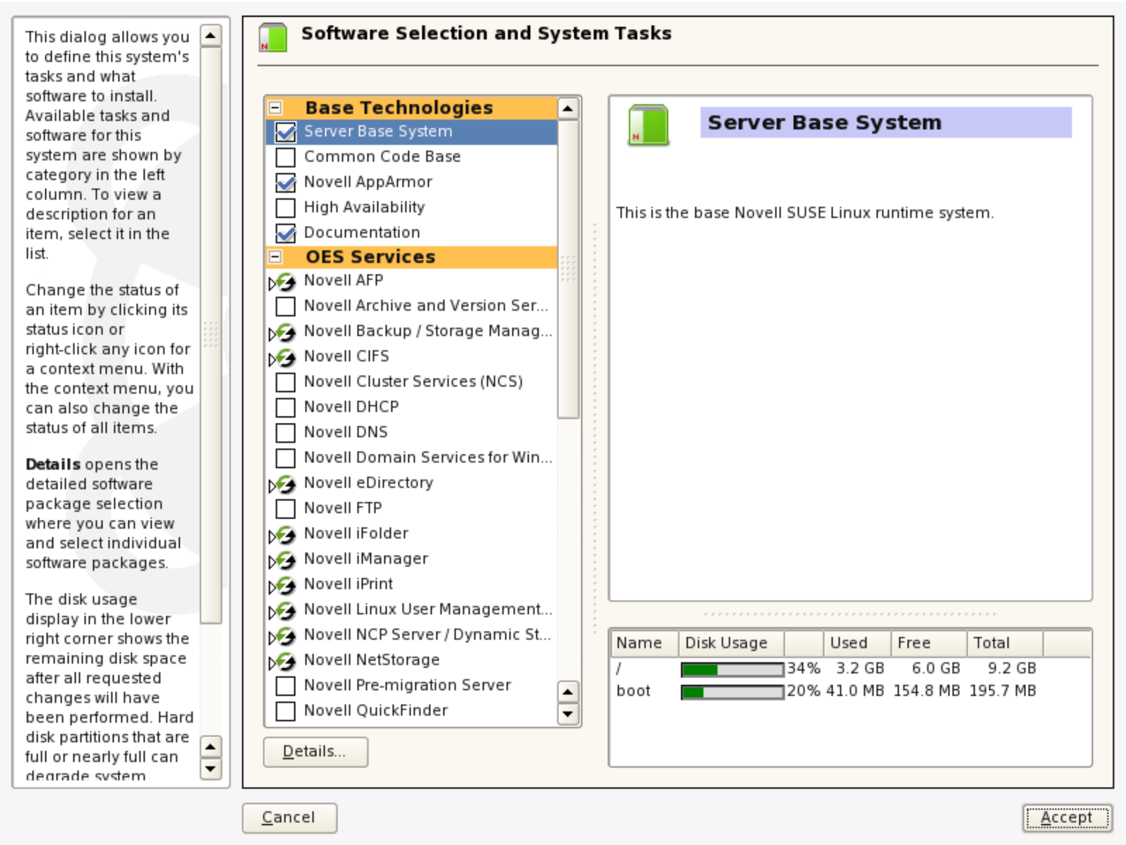
IMPORTANT: If you deselect a pattern after selecting it, you are instructing the installation program to not install that pattern and all of its dependent patterns. Rather than deselecting a pattern, click **Cancel** to cancel your software selections, then click the **Select Patterns** heading again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

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

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

Attempting to uninstall a service by deselecting its pattern is not recommended. For more information, see Chapter 13, “Disabling OES 11 Services,” on page 215.

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



This dialog allows you to define this system's tasks and what software to install. Available tasks and software for this system are shown by category in the left column. To view a description for an item, select it in the list.

Change the status of an item by clicking its status icon or right-click any icon for a context menu. With the context menu, you can also change the status of all items.

Details opens the detailed software package selection where you can view and select individual software packages.

The disk usage display in the lower right corner shows the remaining disk space after all requested changes will have been performed. Hard disk partitions that are full or nearly full can degrade system

Software Selection and System Tasks

Base Technologies

- ☑ Server Base System
- □ Common Code Base
- ☑ Novell AppArmor
- □ High Availability
- ☑ Documentation

OES Services

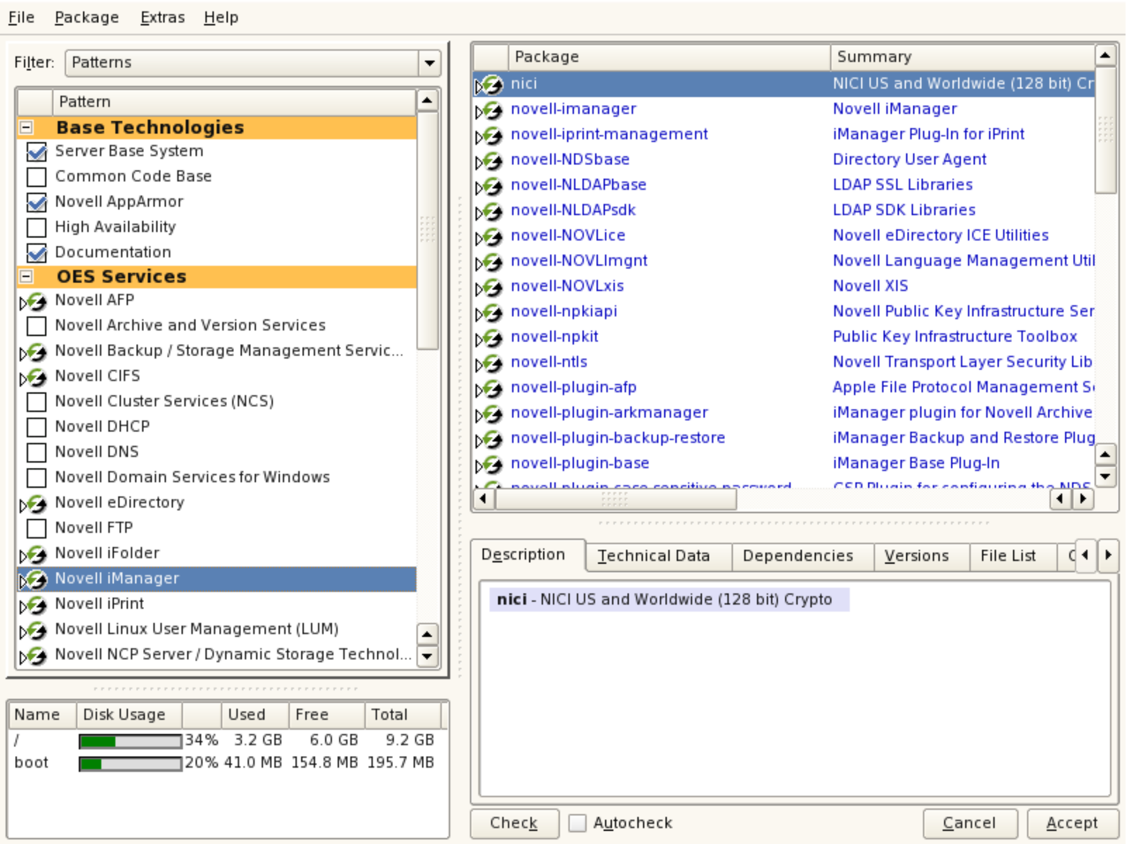
- Novell AFP
- □ Novell Archive and Version Ser...
- Novell Backup / Storage Manag...
- Novell CIFS
- □ Novell Cluster Services (NCS)
- □ Novell DHCP
- □ Novell DNS
- □ Novell Domain Services for Win...
- Novell eDirectory
- □ Novell FTP
- Novell iFolder
- Novell iManager
- Novell iPrint
- Novell Linux User Management...
- Novell NCP Server / Dynamic St...
- Novell NetStorage
- □ Novell Pre-migration Server
- □ Novell QuickFinder

Server Base System

This is the base Novell SUSE Linux runtime system.

Name	Disk Usage	Used	Free	Total
/	34%	3.2 GB	6.0 GB	9.2 GB
boot	20%	41.0 MB	154.8 MB	195.7 MB

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



Pattern
Base Technologies
☑ Server Base System
□ Common Code Base
☑ Novell AppArmor
□ High Availability
☑ Documentation
OES Services
Novell AFP
□ Novell Archive and Version Services
Novell Backup / Storage Management Servic...
Novell CIFS
□ Novell Cluster Services (NCS)
□ Novell DHCP
□ Novell DNS
□ Novell Domain Services for Windows
Novell eDirectory
□ Novell FTP
Novell iFolder
Novell iManager
Novell iPrint
Novell Linux User Management (LUM)
Novell NCP Server / Dynamic Storage Technol...

Package	Summary
nici	NICI US and Worldwide (128 bit) Cr
novell-imanager	Novell iManager
novell-iprint-management	iManager Plug-In for iPrint
novell-NDSbase	Directory User Agent
novell-NLDAPbase	LDAP SSL Libraries
novell-NLDAPsdk	LDAP SDK Libraries
novell-NOVLice	Novell eDirectory ICE Utilities
novell-NOVLlmgnt	Novell Language Management Util
novell-NOVLxis	Novell XIS
novell-npkiapi	Novell Public Key Infrastructure Ser
novell-npkit	Public Key Infrastructure Toolbox
novell-ntls	Novell Transport Layer Security Lib
novell-plugin-afp	Apple File Protocol Management S
novell-plugin-arkmanager	iManager plugin for Novell Archive
novell-plugin-backup-restore	iManager Backup and Restore Plug
novell-plugin-base	iManager Base Plug-In
novell-plugin-case-sensitive-password	CSP Plugin for configuring the NDS

nici - NICI US and Worldwide (128 bit) Crypto

Name	Disk Usage	Used	Free	Total
/	34%	3.2 GB	6.0 GB	9.2 GB
boot	20%	41.0 MB	154.8 MB	195.7 MB

NOTE: The RPMs listed here are not selected automatically during an upgrade to OES 11 SP3. They must be manually selected under the following upgrade scenarios:

- When upgrading to OES 11 SP3 from OES 2 SP3 or OES 11, ensure that you select the `novell-ndsgrepair` RPM under the eDirectory pattern. This RPM was added to OES beginning with OES 11 SP1.
- When upgrading to OES 11 SP3 from any of the earlier releases, ensure that you select the following RPMs under the eDirectory pattern: `novell-edirectory-log4cxx`, `novell-edirectory-xdaslog`, `novell-edirectory-xdaslog-conf`, and `novell-edirectory-xdasinstrument`. Under the iManager pattern, select `novell-plugin-instrumentation` RPM. These RPMs were added to OES beginning with OES 11 SP3. The `novell-plugin-instrumentation` RPM is required only on servers that have iManager installed. If you attempt to install this RPM with `zypper in novell-plugin-instrumentation` on a server that does not have iManager installed, zypper will install iManager automatically due to the dependencies. This will result in iManager getting installed on all server.

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

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

10 (Conditional) If the prompt for the AGFA Fonts license displays, read the agreement, then click **Accept**.

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

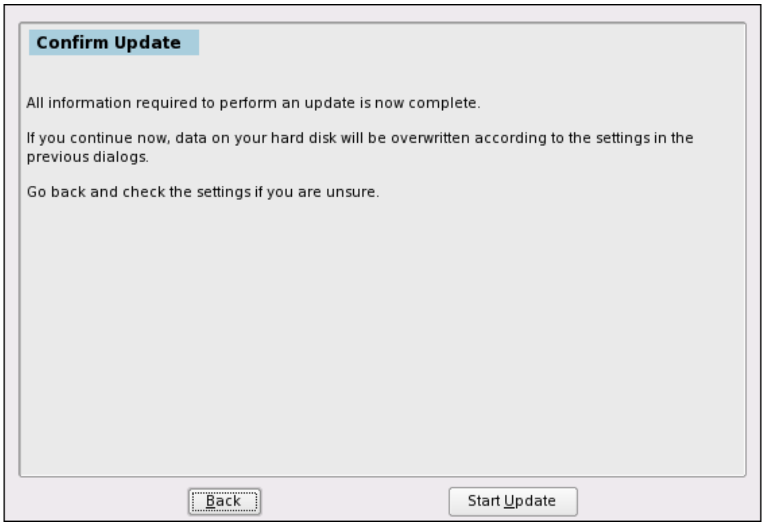
12 (Conditional) If you are prompted, resolve any dependency conflicts.

13 If the Update Options page displays again, click **Accept**.

14 Continue with "Accepting the Installation Settings" on page 134.

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



Confirm Update

All information required to perform an update is now complete.

If you continue now, data on your hard disk will be overwritten according to the settings in the previous dialogs.

Go back and check the settings if you are unsure.

   The base installation settings are applied and the packages are installed.
4. While the server is updating the files, do one of the following:
   - For installations using a network installation source, remove the boot DVD (*SUSE Linux Enterprise Server 11 SP4 DVD1*) from the DVD drive.
   - For installations using a DVD installation source, leave the DVD in the DVD drive. When the installation process prompts you for each DVD at the appropriate time, insert the DVD. The progress status at the bottom of the screen indicates which DVD will be prompted for next.
5. After the server reboots, continue with "Specifying Configuration Information" on page 55.

TIP: If you have the disk driver situation mentioned in Step 7 on page 129, your server boots to a prompt for the root password. Specify the password, and then use an editor such as VI to modify the /etc/fstab file so that the path to the boot partition uses sda instead of hda. Then reboot the server. The upgrade should continue normally.

5.4.10 Specifying Configuration Information

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

- "Testing the Connection to the Internet" on page 135
- "Specifying Novell Customer Center Configuration Settings" on page 135
- "Updating the Server Software During the Upgrade" on page 138
- "Upgrading eDirectory" on page 140
- "Specifying LDAP Configuration Settings" on page 141
- "Configuring Novell Open Enterprise Server Services" on page 141

Testing the Connection to the Internet

On the Test Internet Connection page:

1. Select **Yes**, **Test Connection to the Internet**, then click **Next**.
2. Obtaining the latest SUSE release notes might fail at this point. If it does, view the log to verify that the network configuration is correct, then click **Next**.
3. If the network configuration is not correct, click **Back** > **Back** and fix your network configuration. See "Network Interface" on page 56. The most common problem is that an invalid DNS server is specified.

   or

   Skip this test by clicking **No, Skip This Test**, then continue with Step 4.

   IMPORTANT: Most OES services configurations require a connection to the Internet.

   Skipping this test also skips downloading release notes, configuring the Novell Customer Center, and updating online.

   ---

4. If you skipped the customer center test, continue with "Upgrading eDirectory" on page 140. Otherwise, continue with "Specifying Novell Customer Center Configuration Settings" on page 135.

Specifying Novell Customer Center Configuration Settings

To receive support and updates for your OES 11 SP3 server, you need to register it in the Novell Customer Center. When the Novell Customer Center Configuration page is displayed, you have three options:

- "Updating a Registered Server (Recommended)" on page 135
- "Registering the Server Later / Skipping a Registered Server Update" on page 135
- "Registering the Server During the Upgrade" on page 135

Updating a Registered Server (Recommended)

1. If you have already registered your OES 11 SP3 server and you want to download the available patches, leave **Configure Now** selected, then click Next.

   YaST contacts the server (which might take a few minutes) and then downloads the available patches.
2. Go to Step 8 on page 138.

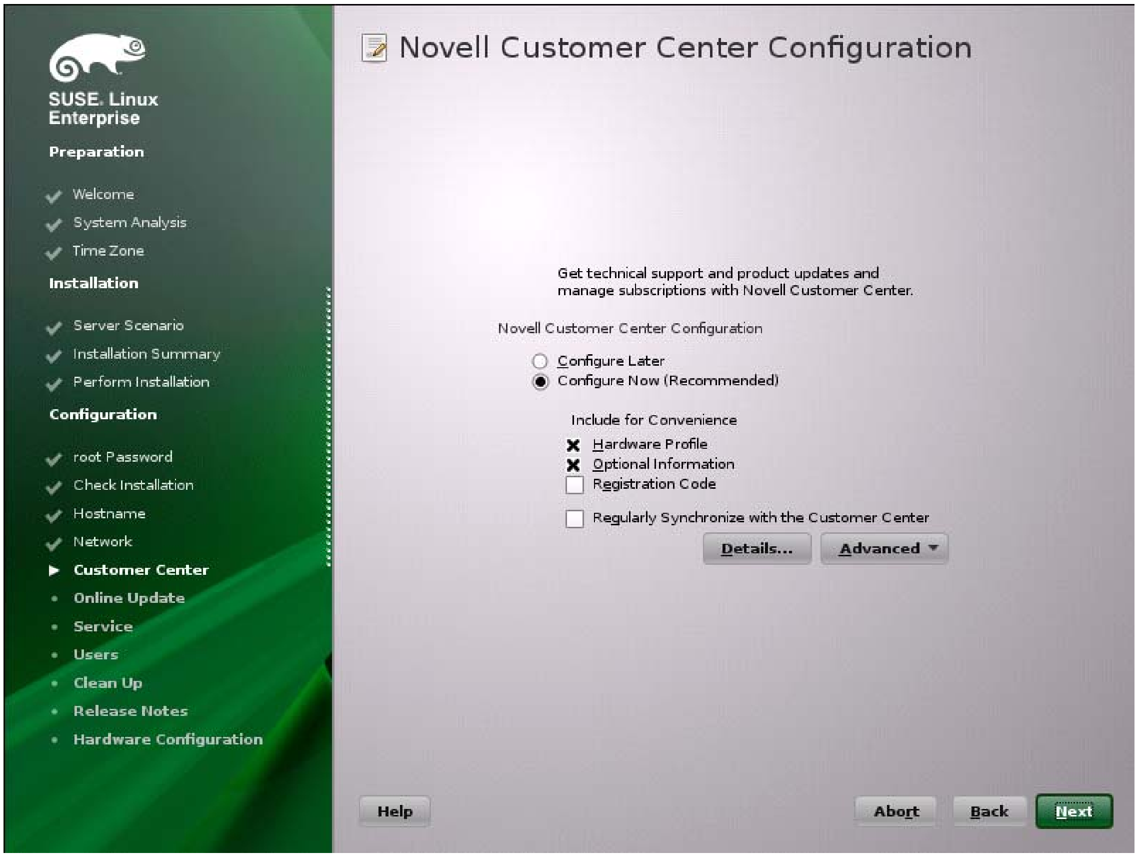
Registering the Server Later / Skipping a Registered Server Update

1. Click **Configure Later**.
2. Continue with "Upgrading eDirectory" on page 140.

Registering the Server During the Upgrade

1. On the Novell 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 SLES 11 SP4 and OES product in the Novell Customer Center.
Hardware Profile	Sends information to the Novell Customer Center about the hardware that you are installing SLES 11 SP4 and OES 11 SP3 on.
Optional Information	Sends optional information to the Novell 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.



Get technical support and product updates and manage subscriptions with Novell Customer Center.

Novell Customer Center Configuration

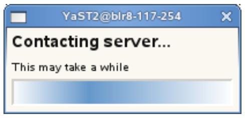
○ Configure Later
● Configure Now (Recommended)

Include for Convenience

☒ Hardware Profile
☒ Optional Information
□ Registration Code

□ Regularly Synchronize with the Customer Center

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



Contacting server...

This may take a while

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

4 On the Novell Customer Center Registration page, specify the required information in the following fields:

- **Email Address:** The email address for your Novell Login account.
- **Confirm Email Address:** The same email address for your Novell Login account
- **Activation Code for SLES Components (optional):** Specify your purchased or 60-day evaluation registration code for the SLES 11 SP4 product.

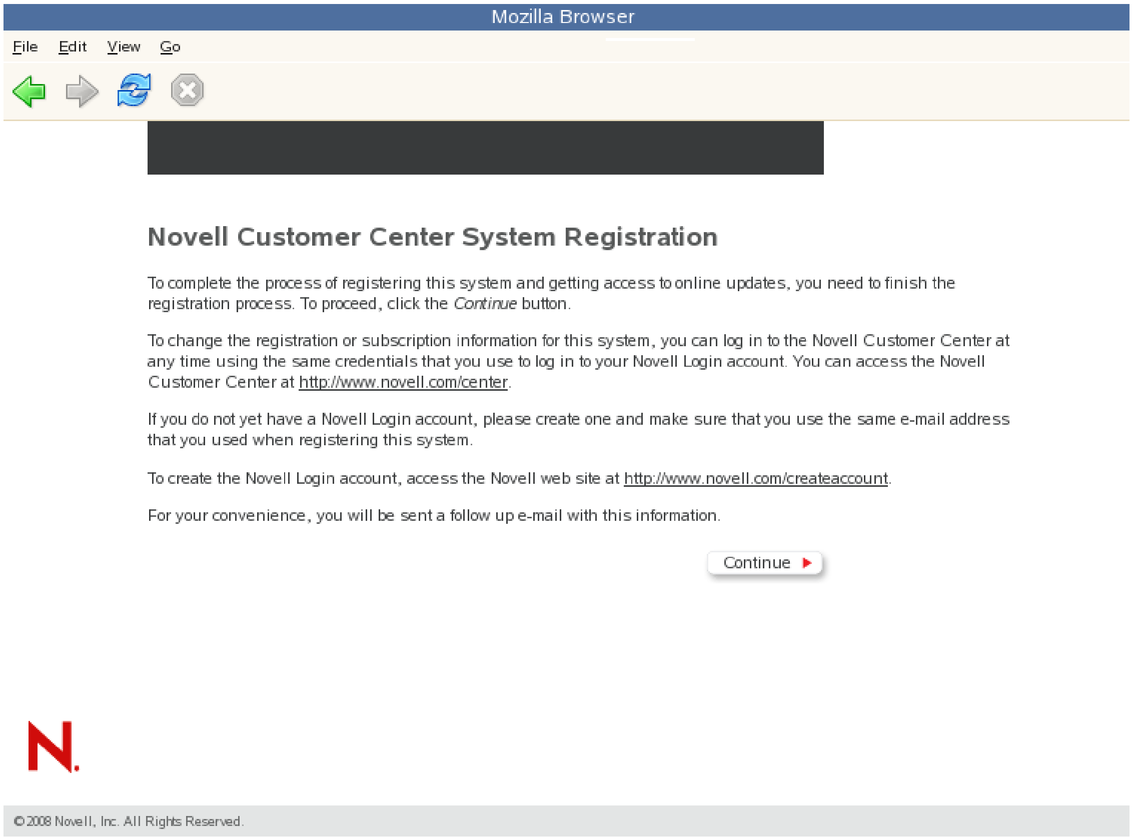
  If you don't specify a code, the server cannot receive any updates or patches.
- **Activation Code for OES Components (optional):** Specify your purchased or 60-day evaluation registration code for the OES 11 SP3 product.

  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 Novell Customer Center, specify a description to identify this server.

5 Click **Submit**.

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



Novell Customer Center System Registration

To complete the process of registering this system and getting access to online updates, you need to finish the registration process. To proceed, click the *Continue* button.

To change the registration or subscription information for this system, you can log in to the Novell Customer Center at any time using the same credentials that you use to log in to your Novell Login account. You can access the Novell Customer Center at http://www.novell.com/center.

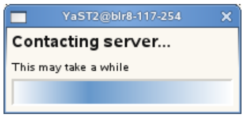
If you do not yet have a Novell Login account, please create one and make sure that you use the same e-mail address that you used when registering this system.

To create the Novell Login account, access the Novell web site at http://www.novell.com/createaccount.

For your convenience, you will be sent a follow up e-mail with this information.

© 2008 Novell, Inc. All Rights Reserved.

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



Contacting server...

This may take a while

8. When you see the message `Your configuration was successful` on the Novell Customer Center Configuration, click **Ok**.
9. Continue with "Updating the Server Software" on page 61.

Updating the Server Software During the Upgrade

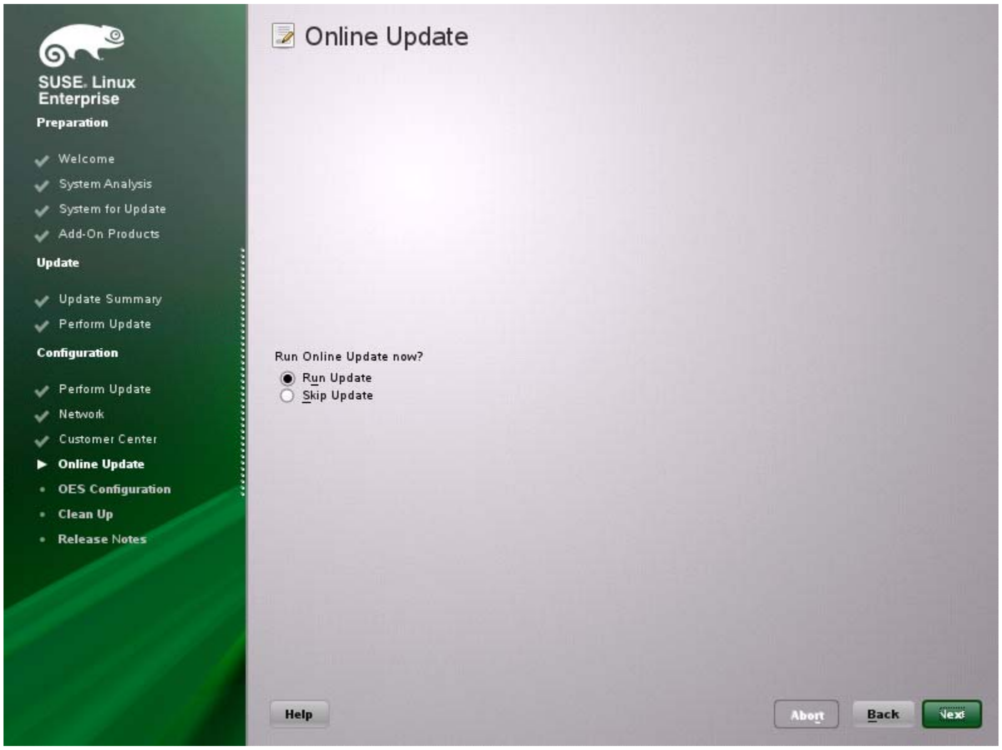
If you have a successful connection to the Internet and have registered the server in the Novell Customer Center, the server displays the Online Update page. You can run the online update now or skip it and get updates later.

To skip getting updates during the upgrade:

1. On the Online Update page, click **Skip Update**.
2. Continue with "Upgrading eDirectory" on page 140.

To get updates during the upgrade:

1. On the Online Update page, click **Run Update**.



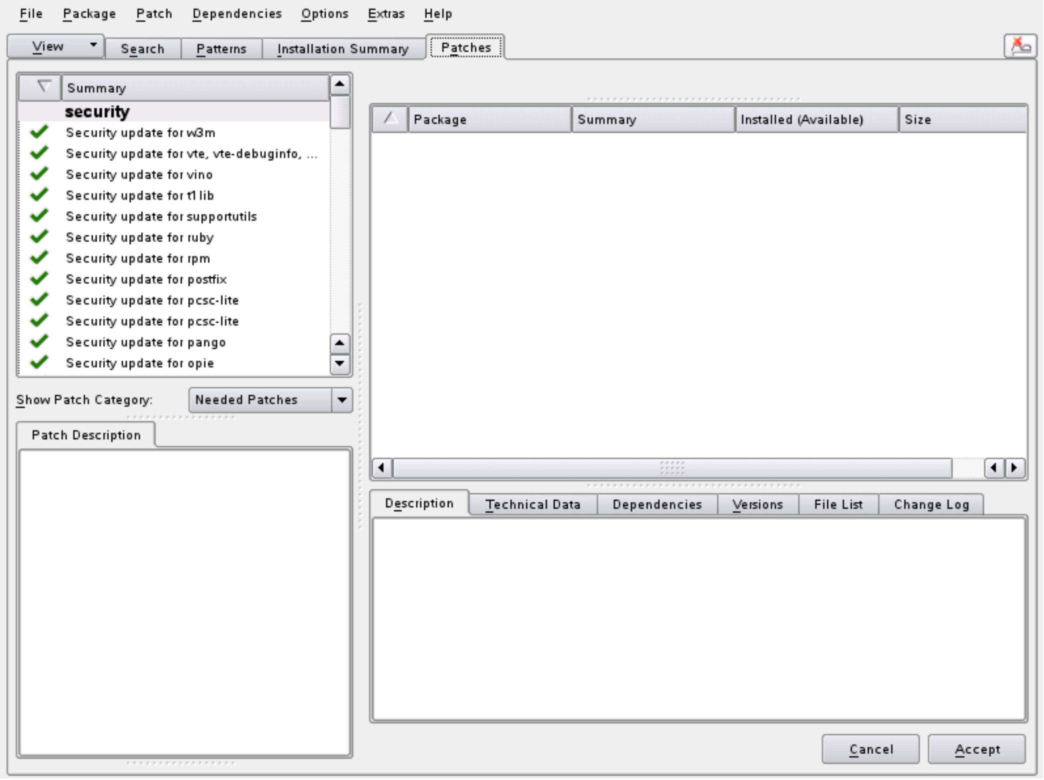
Online Update

Run Online Update now?

● Run Update
○ Skip Update

2. On the page that shows that updates are available, select the updates that you want to install, then click **Accept**.

   The check marks that are shown in the summary column of the patches list are the patches that have already been installed on your system.



Summary

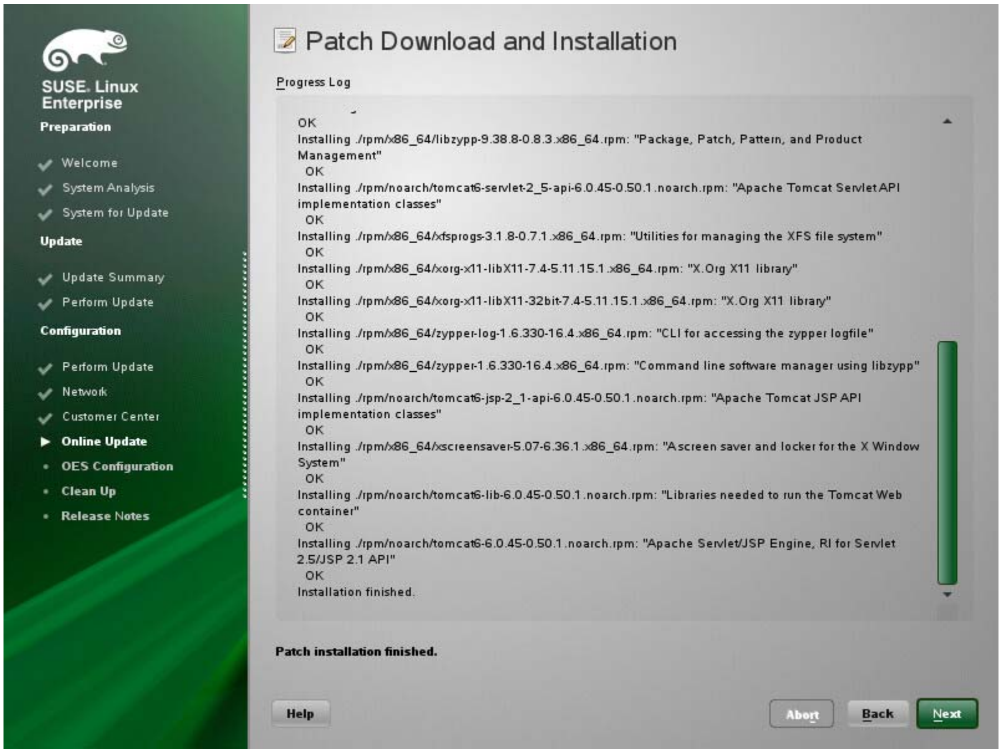
security

- ✓ Security update for w3m
- ✓ Security update for vte, vte-debuginfo, ...
- ✓ Security update for vino
- ✓ Security update for t1lib
- ✓ Security update for supportutils
- ✓ Security update for ruby
- ✓ Security update for rpm
- ✓ Security update for postfix
- ✓ Security update for pcsc-lite
- ✓ Security update for pcsc-lite
- ✓ Security update for pango
- ✓ Security update for opie

Show Patch Category: Needed Patches

Patch Description

3 When you see the message, `Installation finished` on the Patch Download and Installation page, click **Next**.



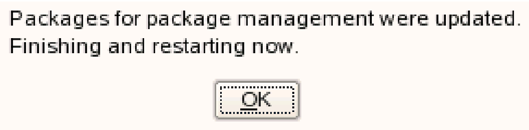
Patch Download and Installation

Progress Log

```
OK
Installing ./rpm/x86_64/libzypp-9.38.8-0.8.3.x86_64.rpm: "Package, Patch, Pattern, and Product
Management"
  OK
Installing ./rpm/noarch/tomcat6-servlet-2_5-api-6.0.45-0.50.1.noarch.rpm: "Apache Tomcat Servlet API
implementation classes"
  OK
Installing ./rpm/x86_64/xfsprogs-3.1.8-0.7.1.x86_64.rpm: "Utilities for managing the XFS file system"
  OK
Installing ./rpm/x86_64/xorg-x11-libX11-7.4-5.11.15.1.x86_64.rpm: "X.Org X11 library"
  OK
Installing ./rpm/x86_64/xorg-x11-libX11-32bit-7.4-5.11.15.1.x86_64.rpm: "X.Org X11 library"
  OK
Installing ./rpm/x86_64/zypper-log-1.6.330-16.4.x86_64.rpm: "CLI for accessing the zypper logfile"
  OK
Installing ./rpm/x86_64/zypper-1.6.330-16.4.x86_64.rpm: "Command line software manager using libzypp"
  OK
Installing ./rpm/noarch/tomcat6-jsp-2_1-api-6.0.45-0.50.1.noarch.rpm: "Apache Tomcat JSP API
implementation classes"
  OK
Installing ./rpm/x86_64/xscreensaver-5.07-6.36.1.x86_64.rpm: "A screen saver and locker for the X Window
System"
  OK
Installing ./rpm/noarch/tomcat6-lib-6.0.45-0.50.1.noarch.rpm: "Libraries needed to run the Tomcat Web
container"
  OK
Installing ./rpm/noarch/tomcat6-6.0.45-0.50.1.noarch.rpm: "Apache Servlet/JSP Engine, RI for Servlet
2.5/JSP 2.1 API"
  OK
Installation finished.
```

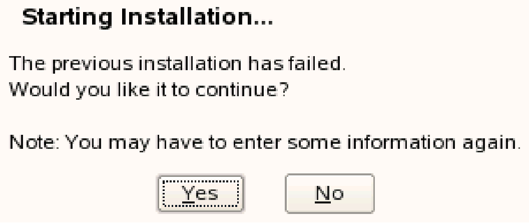
Patch installation finished.

4 If the update makes changes to YaST, the following message displays. If so, click **OK** to restart YaST.



Packages for package management were updated.
Finishing and restarting now.

5 If the installation was interrupted, the following message might display. If so, click **Yes** to continue with the installation, then enter the `root` password.



Starting Installation...

The previous installation has failed.
Would you like it to continue?

Note: You may have to enter some information again.

The online update displays again with additional updates. If a patch has changes to the kernel, you might want to deselect it and install it later after the installation is complete.

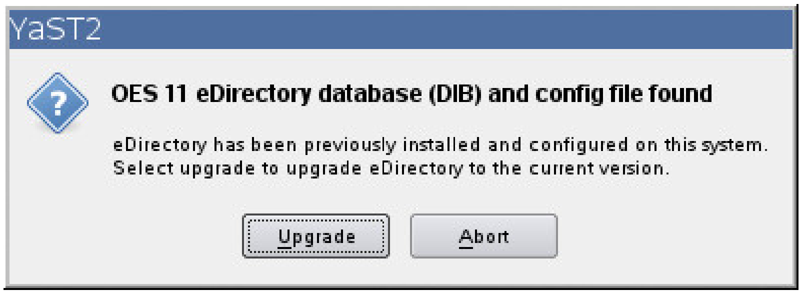
6 If you do install patches that have changes to the kernel, click **OK**.

7 After all the patches are installed, continue with "Upgrading eDirectory" on page 140.

Upgrading eDirectory

OES 11 SP3 includes eDirectory 8.8.8.

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



OES 11 eDirectory database (DIB) and config file found

eDirectory has been previously installed and configured on this system.
Select upgrade to upgrade eDirectory to the current version.

NOTE: If you are upgrading from OES 2 SP3, this dialog will show that the OES 2.0 eDirectory database (DIB) and config file were found.

2 On the eDirectory Upgrade - Existing Server Information page, type the Admin password.

3 Click **Next**.

4 On the NetIQ Modular Authentication Service page, click **Next**.

5 Continue with "Specifying LDAP Configuration Settings" on page 141.

Specifying LDAP Configuration Settings

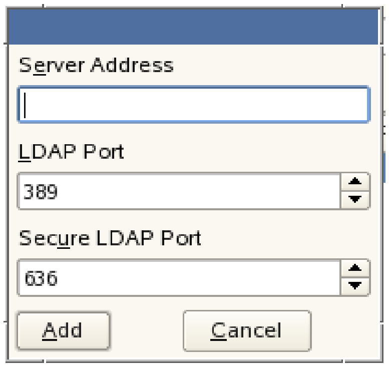
Many of the OES services require eDirectory. If eDirectory was not selected as a product to upgrade or install but other OES services that do require LDAP services were installed, the LDAP Configuration service displays so that you can complete the required information.

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

   Server Address

   LDAP Port

   389

   Secure LDAP Port

   636

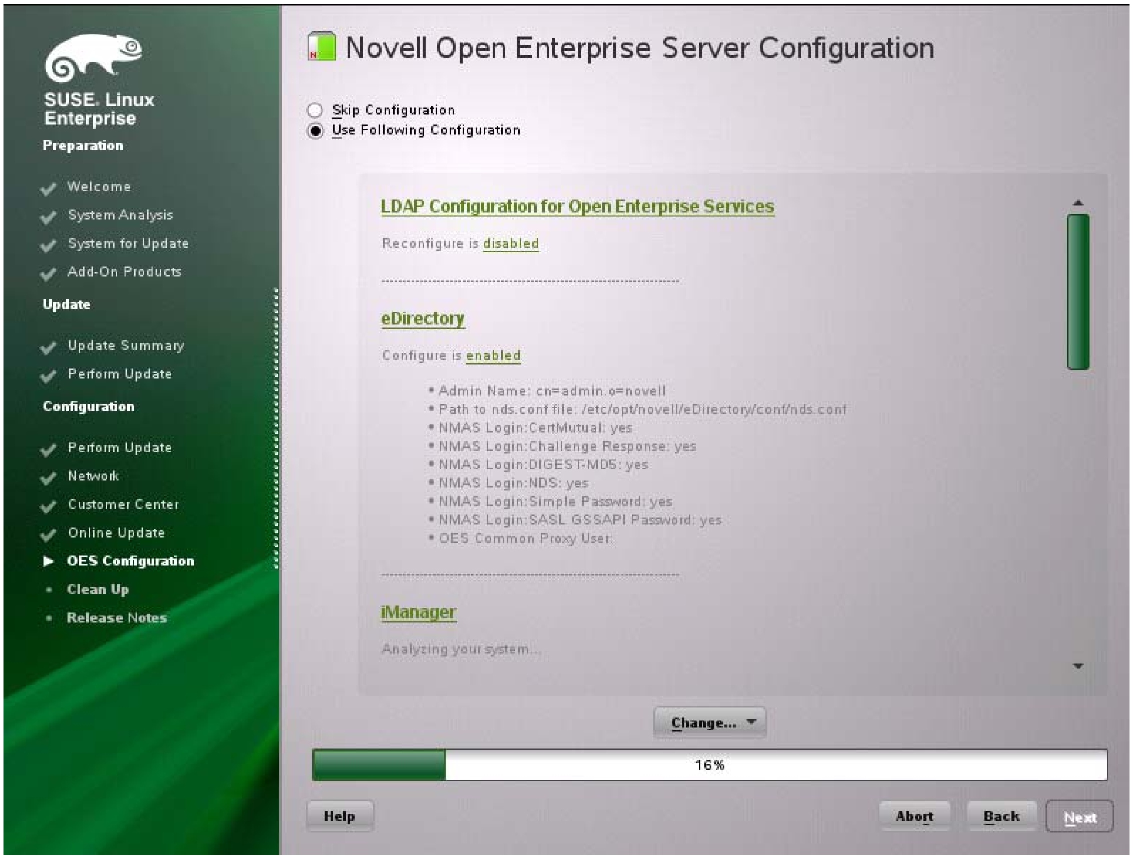
   4c Click **Add**.

   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 Novell Open Enterprise Server Services" on page 141.

Configuring Novell Open Enterprise Server Services

After you complete the LDAP configuration or eDirectory configuration, the **Novell 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.



Novell Open Enterprise Server Configuration

○ Skip Configuration
● Use Following Configuration

LDAP Configuration for Open Enterprise Services

Reconfigure is disabled

eDirectory

Configure is enabled

- Admin Name: cn=admin.o=novell
- Path to nds.conf file: /etc/opt/novell/eDirectory/conf/nds.conf
- NMAS Login:CertMutual: yes
- NMAS Login:Challenge Response: yes
- NMAS Login:DIGEST-MD5: yes
- NMAS Login:NDS: yes
- NMAS Login:Simple Password: yes
- NMAS Login:SASL GSSAPI Password: yes
- OES Common Proxy User:

iManager

Analyzing your system...

16%

When you specify the configuration information for OES services, see the information in "Configuration Guidelines for OES Services" on page 78, or click a link below:

- AFP
- Archive and Version Services
- Backup/Storage Management Services (SMS)
- CIFS
- Clustering (NCS)
- DHCP
- DNS
- Domain Services for Windows (DSfW)
- eDirectory
- FTP
- iFolder
- iManager
- iPrint
- Linux User Management (LUM)
- NCP Server/Dynamic Storage Technology
- NetStorage
- Pre-Migration Server
- QuickFinder

- Novell Remote Manager (NRM)
- Novell Samba
- Novell Storage Services

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 78.

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

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

If you change the status to **Configuration is disabled**, you must configure the OES components after the installation is complete. See "Installing or Configuring OES 11 SP3 on an Existing Server" on page 109.

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 5.5, "Finishing the Upgrade," on page 143.

5.5 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.

5.6 Using AutoYaST for an OES 11 SP3 Upgrade

If you are a system administrator who needs to upgrade multiple OES 2, OES 11, OES 11 SP1, or OES 11 SP2 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 OES 2 (64-bit), OES 11, OES 11 SP1 or OES 11 SP2 server to OES 11 SP3 with no user intervention. Ensure that you use the integrated OES 11 SP3 ISO (`OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso`) for the upgrade.

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 5.6.1, “Prerequisites,” on page 144
- Section 5.6.2, “Remastering the Integrated ISO without the add_on_products.xml,” on page 145
- Section 5.6.3, “Creating an Answer File to Provide the eDirectory and DSfW Passwords,” on page 145
- Section 5.6.4, “Upgrading an OES 2 (64-bit), OES 11, OES 11 SP1 or OES 11 SP2 Server to OES 11 SP3,” on page 146
- Section 5.6.5, “Upgrading an OES 2 (64-bit), OES 11, OES 11 SP1 or OES 11 SP2 XEN Guest Server to OES 11 SP3,” on page 147
- Section 5.6.6, “Troubleshooting an AutoYaST Upgrade,” on page 148

5.6.1 Prerequisites

- Identify the 64-bit OES 2 SP3, OES 11, OES 11 SP1, or OES 11 SP2 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 11 SP3 upgrade requirements specified in Section 5.3, “Meeting the Upgrade Requirements,” on page 117.
- 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 2 SP2, the file name is `edir2_sp2`, for OES 2 SP3, it is `edir2_sp3`, for OES 11, it is `edir11`, for OES 11 SP1, it is `edir_oes11_sp1` and OES 11 SP2, it is `edir_oes11_sp2`) at `/etc/sysconfig/novell/` as shown below:

  `CONFIG_EDIR_REPLICA_SERVER="`*<specify the eDirectory Replica IP>*`"`
- Download the `OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso`, remove the `add_on_products.xml`, and then remaster the ISO. Use the remastered ISO for the upgrade. For more information, see Section 5.6.2, “Remastering the Integrated ISO without the add_on_products.xml,” on page 145.
- Create an answer file that provides the eDirectory password. For more information, see Section 5.6.3, “Creating an Answer File to Provide the eDirectory and DSfW Passwords,” on page 145.

5.6.2 Remastering the Integrated ISO without the add_on_products.xml

For a truly unattended OES 11 SP3 upgrade from OES 2, OES 11, OES 11 SP1 or OES 11 SP2, use the remastered integrated ISO (`OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso`) that does not have the `add_on_products.xml` file.

To remaster the ISO:

1. Download the `OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso` and loop mount it under any directory using the following command:

   ```
   mount -o loop OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso /mnt/autoupgrade
   ```

   It is mounted in read-only mode.
2. Copy the autoupgrade folder to another location, and then delete the `add_on_products.xml` file.

   ```
   cp -r /mnt/autoupgrade /tmp
   ```
3. Remaster the `OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso` without the `add_on_products.xml` file.

   ```
   mkisofs -R -b boot/x86_64/loader/isolinux.bin -c boot.cat -no-emul-boot -boot-
   load-size    4 -boot-info-table -o /tmp/SLES11-with-OES11-SP3.iso /tmp/
   autoupgrade
   ```

5.6.3 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 2 (64-bit), OES 11, OES 11 SP1 or OES 11 SP2 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 and Above

1. Using the GUI on OES 11 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.

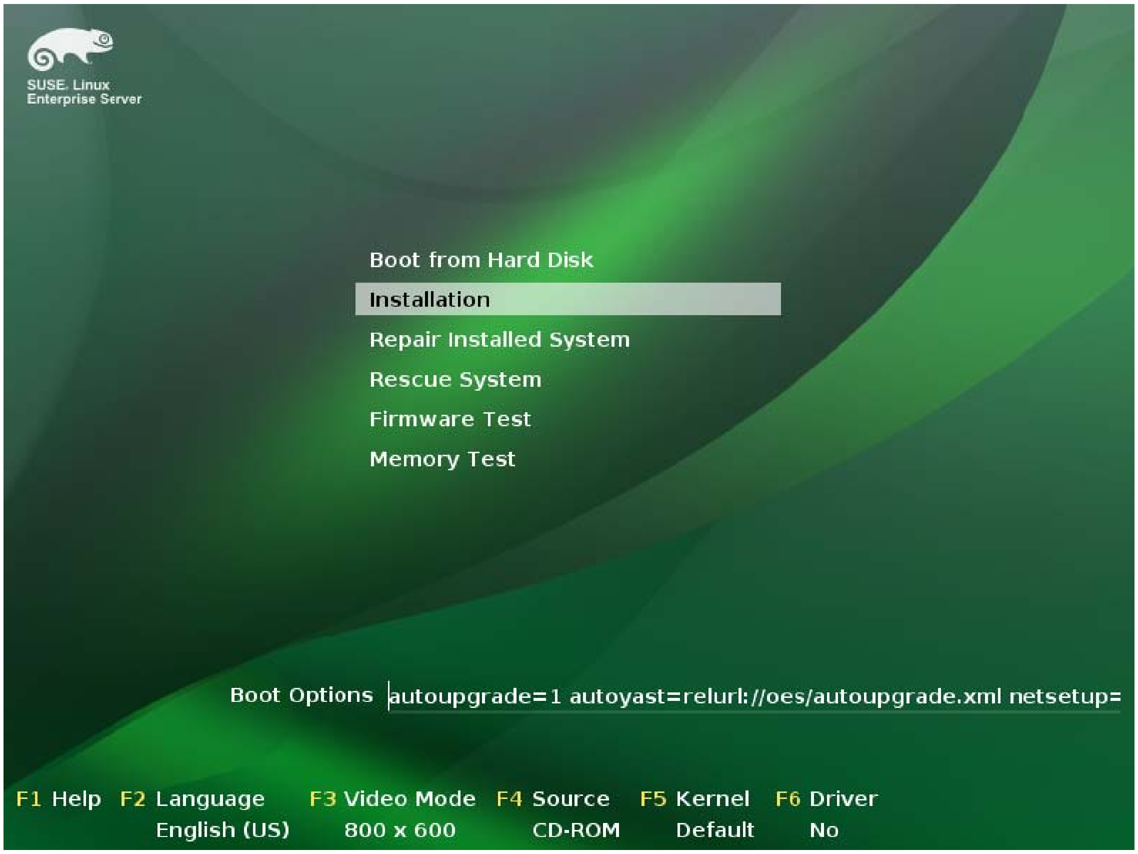
Once you have successfully generated the answer key file using any of the above stated methods, copy it from the current working directory to `/opt/novell/oes-install/`. For example, `cp answer /opt/novell/oes-install/`.

TIP: To invoke help for creating the answer key file, in the terminal window, type `yast2 create-answer-file.ycp --help`.

5.6.4 Upgrading an OES 2 (64-bit), OES 11, OES 11 SP1 or OES 11 SP2 Server to OES 11 SP3

Ensure that you have met all the requirements listed in Section 5.6.1, “Prerequisites,” on page 144.

1. Use the remastered integrated iso (`OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso`) to boot the OES 2, OES 11, OES 11 SP1 or OES 11 SP2 machine that you want to upgrade.



Boot Options autoupgrade=1 autoyast=relurl://oes/autoupgrade.xml netsetup=

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

```
autoupgrade=1 autoyast=relurl://oes/autoupgrade.xml
```

For example:

```
autoupgrade=1 autoyast=relurl://oes/autoupgrade.xml
```

3 Press Enter.

The upgrade proceeds without any user intervention.

5.6.5 Upgrading an OES 2 (64-bit), OES 11, OES 11 SP1 or OES 11 SP2 XEN Guest Server to OES 11 SP3

Ensure that you have met all the requirements listed in Section 5.6.1, “Prerequisites,” on page 144.

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:

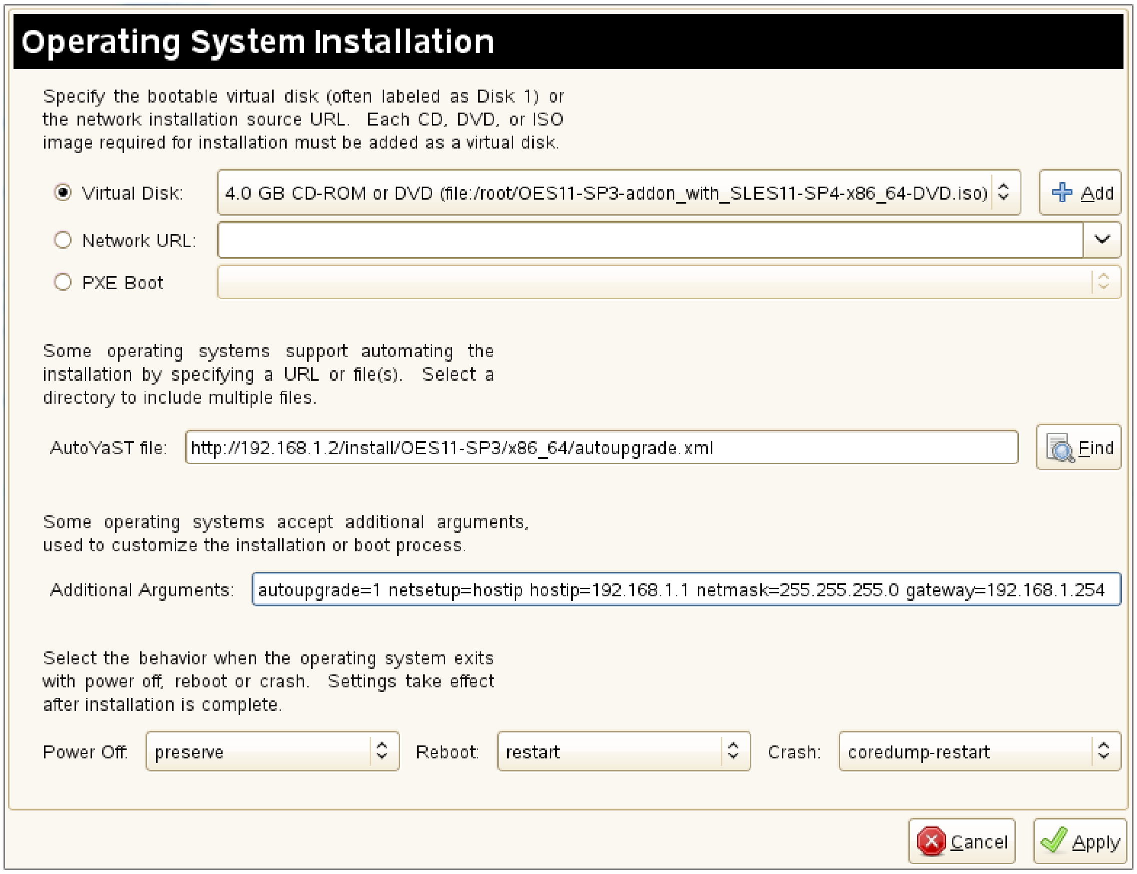
```
xm delete <guest machine>
```

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

```
os=sles11; 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 11 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: 4.0 GB CD-ROM or DVD (file:/root/OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.iso)

○ 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: http://192.168.1.2/install/OES11-SP3/x86_64/autoupgrade.xml

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

Additional Arguments: autoupgrade=1 netsetup=hostip hostip=192.168.1.1 netmask=255.255.255.0 gateway=192.168.1.254

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

NOTE: If you choose to upgrade using an ISO, in the **Virtual Disk**, select the path where the remastered 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.

5.6.6 Troubleshooting an AutoYaST Upgrade

- "Providing the Correct eDirectory and DSfW Administrator Password" on page 149
- "Unattended Upgrade Scenarios That Require User Input" on page 149

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 5.6.3, "Creating an Answer File to Provide the eDirectory and DSfW Passwords," on page 145

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 2 SP2, the file name is `edir2_sp2`, for OES 2 SP3, it is `edir2_sp3`, for OES 11, it is `edir11` and for OES 11 SP1, it is `edir_oes11_sp1`) at `/etc/sysconfig/novell/`, you will be prompted for the same. For more information, see Section 5.6.1, "Prerequisites," on page 144.

5.7 Channel Upgrade from OES 11 SP2 to OES 11 SP3

- Section 5.7.1, "Channel Upgrade from OES 11 SP2 to OES 11 SP3 Via Wagon," on page 149
- Section 5.7.2, "Channel Upgrade from OES 11 SP2 to OES 11 SP3 Using Zypper," on page 152
- Section 5.7.3, "Upgrading OES 11 SP2 to OES 11 SP3 Using SMT," on page 153
- Section 5.7.4, "Rolling Back the Server in the Middle of a Wagon-based Channel Upgrade," on page 153

5.7.1 Channel Upgrade from OES 11 SP2 to OES 11 SP3 Via Wagon

1 Register the OES 11 SP2 server with NCC using the following command:

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

2 Run the `zypper ca` command to ensure that OES11-SP2-Pool, OES11-SP2-Updates, SLES-11-SP3-Pool and SLES11-SP3-Updates catalogs are subscribed and enabled.

3 Apply all the available patches either using `zypper` or `yast2 online_update`. In the list of available patches, ensure that the `Enable update to Novell Open Enterprise Server 11 Service Pack 3` is selected. If this patch is not installed, you cannot proceed with the upgrade.

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

4 Start the wagon upgrade module using the `yast2 wagon` command.

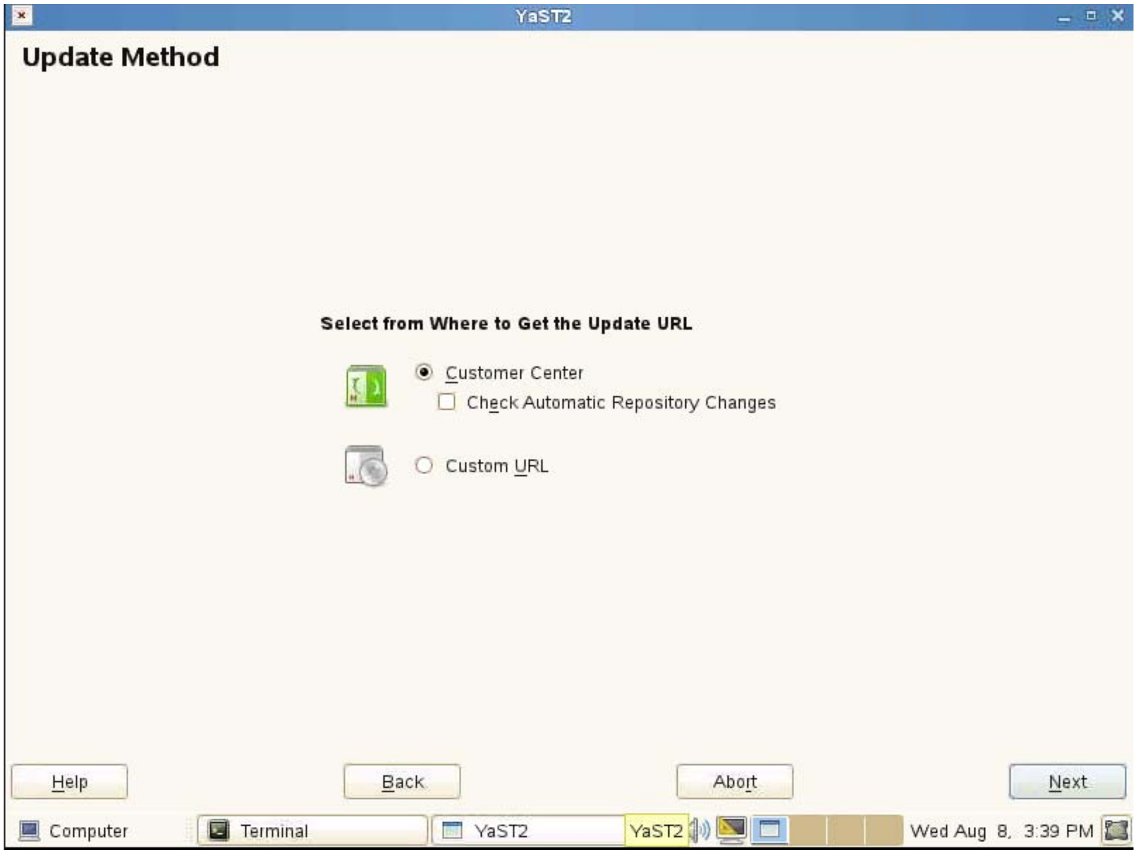
5 On the welcome screen, click **Next**.

6 In Registration Check screen, click **Run Registration** if the "System not Registered" warning is displayed.

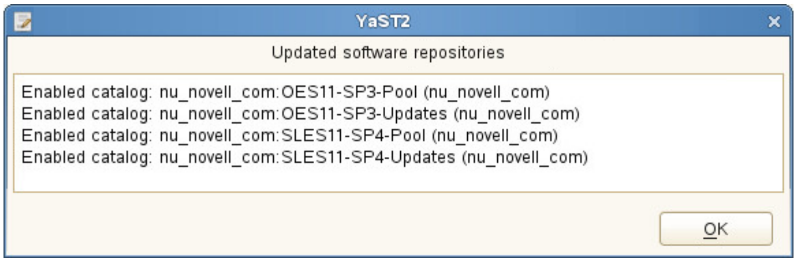
7 The Run Registration redirects to the NCC screen and click **Next.** Wagon does a sync and pops up a message stating that the software repositories need not be changed. This happens as there are no updates at this stage.

8 In the Registration Check screen, ensure that the registration summary displays “Product SUSE Linux Enterprise Server 11 SP3 has a valid registration and Product Novell Open Enterprise Server 11 SP2 has a valid registration”. If the valid registration message is displayed, click **Next,** and it resets the package manager.

9 In the Update Method screen, select **Customer Center > Next**.



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



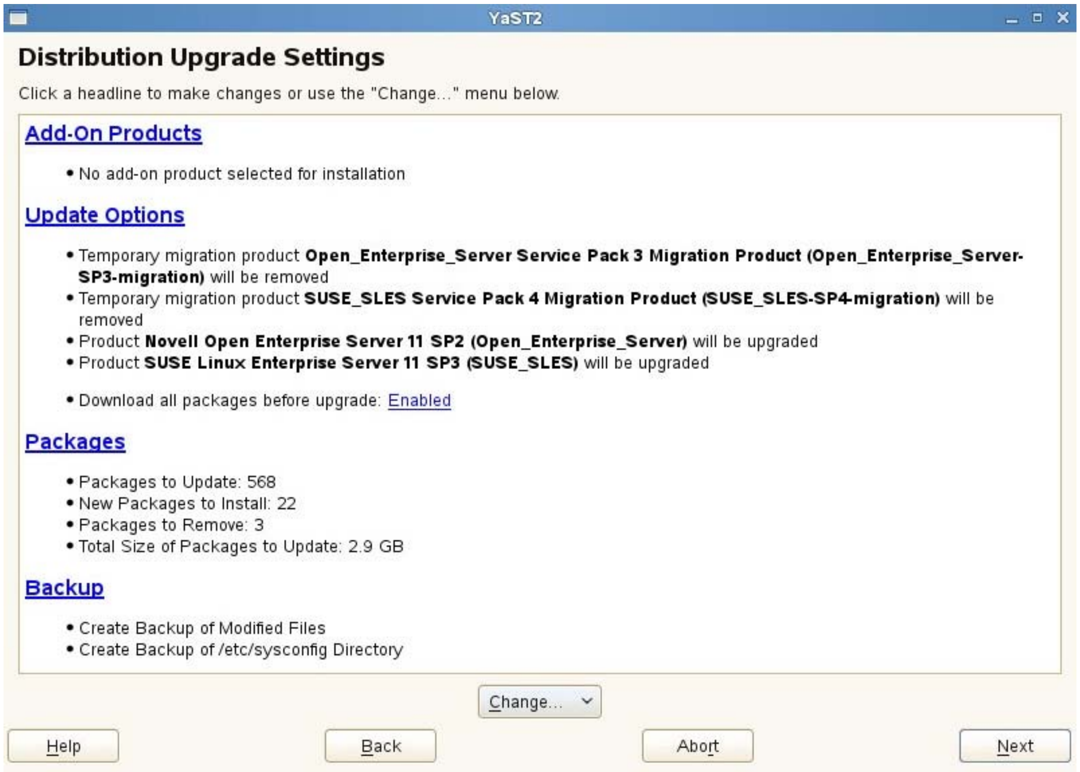
```
Enabled catalog: nu_novell_com:OES11-SP3-Pool (nu_novell_com)
Enabled catalog: nu_novell_com:OES11-SP3-Updates (nu_novell_com)
Enabled catalog: nu_novell_com:SLES11-SP4-Pool (nu_novell_com)
Enabled catalog: nu_novell_com:SLES11-SP4-Updates (nu_novell_com)
```

NOTE: If the repositories are not enabled, click **Back > Nex**t and redo the NCC registration until it is successful. If you are not able to do a successful NCC registration after multiple attempts, abort the process and roll back the server. For more information, see Section 5.7.4, “Rolling Back the Server in the Middle of a Wagon-based Channel Upgrade,” on page 153.

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

- Temporary migration product Open_Enterprise_Server Service Pack 3 Migration Product (Open_Enterprise_Server-SP3-migration) will be removed
- Temporary migration product SUSE_SLES Service Pack 4 Migration Product (SUSE_SLES-SP4-migration) will be removed
- Product Novell Open Enterprise Server 11 SP2 (Open_Enterprise_Server) will be upgraded
- Product SUSE Linux Enterprise Server 11 SP3 (SUSE_SLES) will be upgraded

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



Distribution Upgrade Settings

Click a headline to make changes or use the "Change..." menu below.

Add-On Products

- No add-on product selected for installation

Update Options

- Temporary migration product **Open_Enterprise_Server Service Pack 3 Migration Product (Open_Enterprise_Server-SP3-migration)** will be removed
- Temporary migration product **SUSE_SLES Service Pack 4 Migration Product (SUSE_SLES-SP4-migration)** will be removed
- Product **Novell Open Enterprise Server 11 SP2 (Open_Enterprise_Server)** will be upgraded
- Product **SUSE Linux Enterprise Server 11 SP3 (SUSE_SLES)** will be upgraded

- Download all packages before upgrade: Enabled

Packages

- Packages to Update: 568
- New Packages to Install: 22
- Packages to Remove: 3
- Total Size of Packages to Update: 2.9 GB

Backup

- Create Backup of Modified Files
- Create Backup of /etc/sysconfig Directory

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

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

13 The NCC screen is displayed once again, wherein the registration of the final product is triggered. Click **Next** and at the final success message dialog, click **Finish**.

14 Reboot the server to get the new kernel.

15 After the reboot, log on to the server and run the `yast2 channel-upgrade-oes` command to complete the OES services reconfiguration. This will prompt for eDirectory and DSfW passwords if the answer file is not created. Provide the password and continue. For more information on creating the answer file, see Section 5.6.3, “Creating an Answer File to Provide the eDirectory and DSfW Passwords,” on page 145.

5.7.2 Channel Upgrade from OES 11 SP2 to OES 11 SP3 Using Zypper

1. Register the OES 11 SP2 server with NCC using the `suse_register -a email=<Email-Address> -a regcode-sles=<SLESactivation-key> -a regcode-oes=<OES-activation-key> -L /root/.suse_register.log` command.
2. Run the `zypper ca` command to ensure that OES11-SP2-Pool, OES11-SP2-Updates, SLES-11-SP3-Pool and SLES11-SP3-Updates catalogs are subscribed and enabled.
3. Run the `zypper update -t patch` command to install package management updates.
4. Run the `zypper update -t patch` command once again to install all available updates for SLES 11 SP3 and OES11 SP2. Ensure that the `oes11sp2-enable-OES11-SP3-online-migration` patch is installed. If this patch is not installed, you cannot proceed with the upgrade.

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

5. Run the `zypper pd` command to ensure that the Open_Enterprise_Server-SP3-migration and SUSE_SLES-SP4-migration are listed but not installed. To check the products installed, run `zypper pd -i` command.
6. The installed products contain information about the distribution upgrades and the migration products that should be installed to perform the migration. Use the `zypper se -t product | grep -h -- "-migration" | cut -d\| -f2` command.

   A sample output is as follows:

   ```
   Open_Enterprise_Server-SP3-migration
   SUSE_SLES-SP4-migration
   ```

7. Install these migration products using the `zypper in -t product Open_Enterprise_Server-SP3-migration SUSE_SLES-SP4-migration` command.
8. Run the `suse_register -L /root/.suse_register.log` command to register the products and to get the corresponding repositories.
9. Run the `zypper ref -s` command to refresh services and repositories.
10. Check the repositories using the `zypper lr` command. It should list OES11-SP3-Pool, OES11-SP3-Updates, SLES11-SP4-Pool and SLES11-SP4-Updates repositories, and they should be enabled.
11. Perform a distribution upgrade using the `zypper dup --from SLES11-SP4-Pool --from SLES11-SP4-Updates --from OES11-SP3-Pool --from OES11-SP3-Updates` command.
    - `The following products are going to be REMOVED:`

      `Open_Enterprise_Server Service Pack 3 Migration Product SUSE_SLES Service Pack 4 Migration Product`

      REMARK: You can choose to ignore this message. The actual product that is being removed are OES 11 SP2 Migration Product and SLES 11 SP3 Migration Product.

      It’s safe to ignore the following messages as well. They have no impact on the channel upgrade.
    - `The following packages are going to be downgraded:`

      `ifolder3-tsa novell-afp-nmasmethods novell-cluster-services novell-cluster-services-32bit novell-cluster-services-cli novell-cluster-services-kmp-default novell-clvmd novell-edirectory-passstore novell-filesystem novell-ifolder-enterprise-migration novell-ifolder-enterprise-plugins novell-migration-arkmanager novell-migration-edirectory novell-migration-ntp novell-oes-dhcp-migration novell-plugin-pwdmanagement`

```
novell-sasl-gssapi-method novell-shadowfs novell-sms-cmpi-provider ntp
openssh-askpass perl-Bootloader yast2-bootloader yast2-http-server yast2-
sound yast2-users yelp yelp-lang
```

- `The following packages are not supported by their vendor:`

  ```
  crash-eppic libblas3 libcryptsetup1 libiptc0 liblapack3 libxtables9
  postgresql94 postgresql94-server
  ```

  NOTE: The packages listed here may vary based on your setup.

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

13 Reboot the server.

14 After the reboot, log on to the server and run the `yast2 channel-upgrade-oes` command to complete the OES services reconfiguration. This will prompt for eDirectory and DSfW passwords if the answer file is not created. Provide the password and continue. For more information on creating the answer file, see Section 5.6.3, “Creating an Answer File to Provide the eDirectory and DSfW Passwords,” on page 145.

5.7.3 Upgrading OES 11 SP2 to OES 11 SP3 Using SMT

1 Install and set up the SMT server. For more information on setting up SMT, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.

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

- **OES 11 SP2:** OES11-SP2-Pool and OES11-SP2-Updates channels
- **OES 11 SP3:** OES11-SP3-Pool and OES11-SP3-Updates channels
- **SLES 11 SP3:** SLES11-SP3-Pool and SLES11-SP3-Updates
- **SLES 11 SP4:** SLES11-SP4-Pool and SLES11-SP4-Updates Channels

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

3 Register the OES 11 SP2 server with the SMT server. For more information on registering, see Configuring Clients with the clientSetup4SMT.sh Script in the Subscription Management Tool Guide.

4 After registration, upgrading the OES 11 SP2 to OES 11 SP3 is the same as that of NCC upgrades as described from Step 2 in Section 5.7, “Channel Upgrade from OES 11 SP2 to OES 11 SP3,” on page 149.

NOTE: If you use Wagon and SMT based upgrade, you will not go through the Step 6 to Step 8 on page 150 mentioned in Section 5.7.1, “Channel Upgrade from OES 11 SP2 to OES 11 SP3 Via Wagon,” on page 149. After clicking on next in Step 5 continue from Step 9 on page 150.

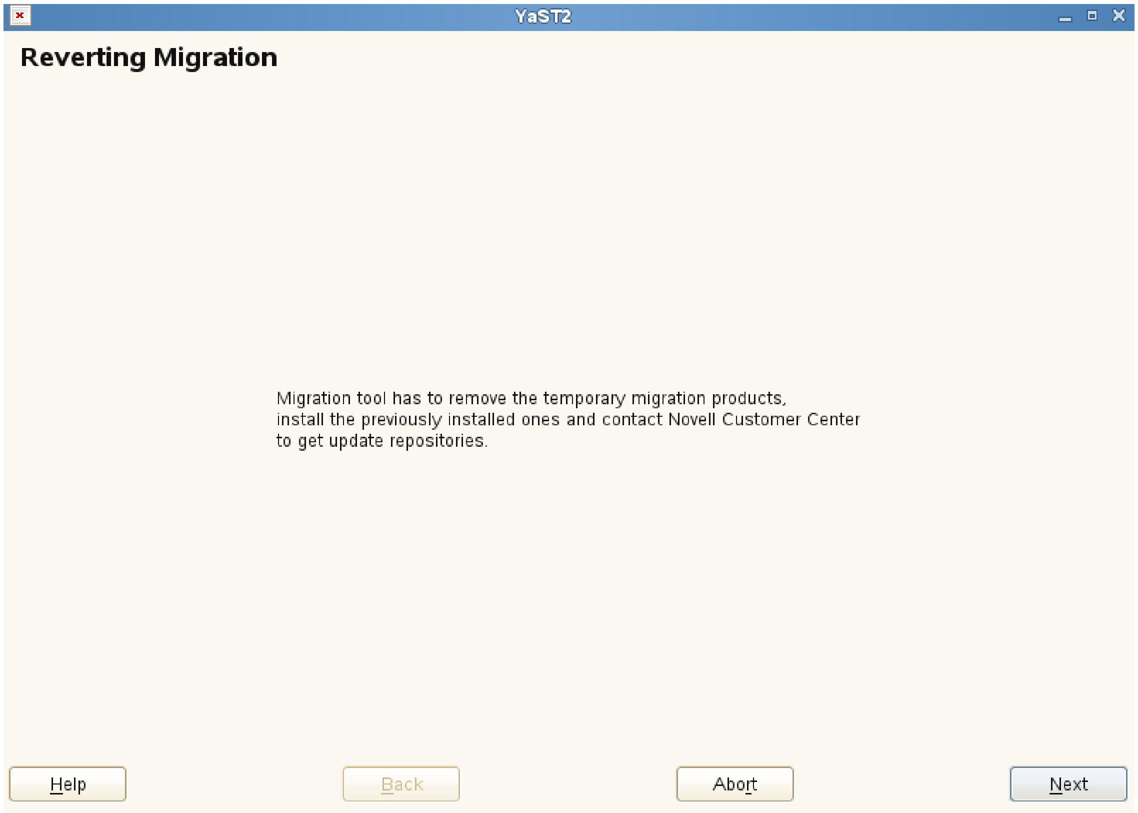
5.7.4 Rolling Back the Server in the Middle of a Wagon-based Channel Upgrade

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

1 Click **Abort**.

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

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



Reverting Migration

Migration tool has to remove the temporary migration products,
install the previously installed ones and contact Novell Customer Center
to get update repositories.

3 In NCC registration screen, click **Next**.

4 Follow the screen prompts and complete the revert process.

5.8 Manual Upgrade from OES 11 SP3 to OES 2015 SP1 Using Zypper

1 Install and configure OES 11 SP3 on SLES 11 SP4 with the required OES services. For more information, see Chapter 3, “Installing OES 11 SP3 as a New Installation,” on page 43.

2 Register the OES 11 SP3 server with the SMT or NCC server.

- To register with the NCC server, run the following command:

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

- For information on registering with the SMT server, see Configuring Clients with the clientSetup4SMT.sh Script in the Subscription Management Tool Guide.

3 Update the SLES 11 SP4 and OES 11 SP3 to latest patches available. For more information, see Chapter 7, “Updating (Patching) an OES 11 SP3 Server,” on page 165.

4 Check the repositories using the `zypper lr` command. It should list the following repositories, and they should be enabled.

- OES11-SP3-Pool
- OES11-SP3-Updates

- SLES11-SP4-Pool
- SLES11-SP4-Updates

5 Run the following commands to add OES2015-SP1-Pool and OES2015-SP1-Updates repositories manually from the SMT or NCC server.

```
zypper ar -c "https://<SMT/NCC_Server>/repo/\$RCE/OES2015-SP1-Pool/sle-11-
x86_64/" OES2015-SP1-Pool
```

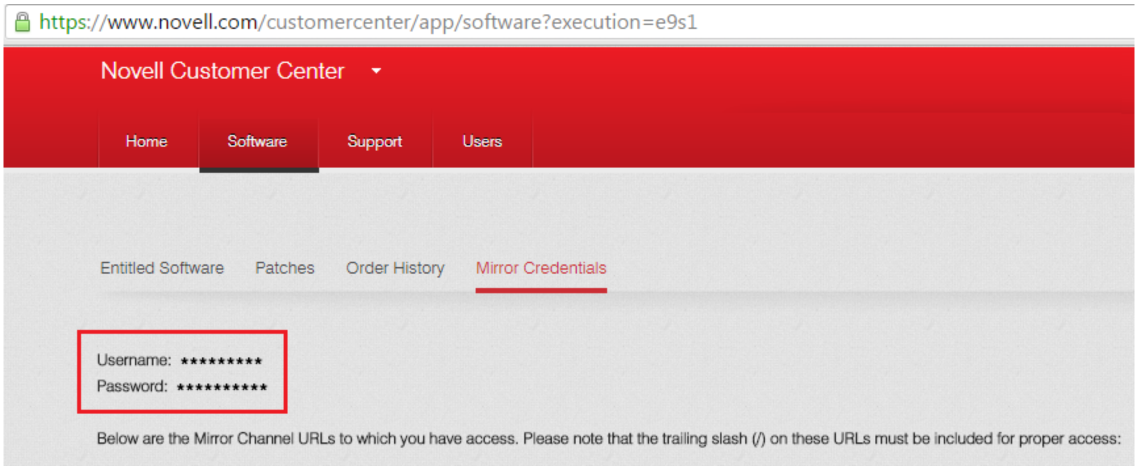
```
zypper ar -c "https://<SMT/NCC_Server>/repo/\$RCE/OES2015-SP1-Updates/sle-11-
x86_64/" OES2015-SP1-Updates
```

If you use *nu.novell.com*, run the following command with username and password to add OES2015-SP1-Pool repository.

```
zypper ar -c "https://<Username>:<Password>@nu.novell.com/repo/\$RCE/OES2015-
SP1-Pool/sle-11-x86_64" OES2015-SP1-Pool
```

```
zypper ar -c "https://<Username>:<Password>@nu.novell.com/repo/\$RCE/OES2015-
SP1-Updates/sle-11-x86_64" OES2015-SP1-Updates
```

The username and password must be Mirror Credentials available in Novell Customer Center (https://www.novell.com/customercenter/app/software?execution=e2s1) as follows:



https://www.novell.com/customercenter/app/software?execution=e9s1

Username: ***********
Password: ************

Below are the Mirror Channel URLs to which you have access. Please note that the trailing slash (/) on these URLs must be included for proper access:

6 Run the `zypper ref` command to refresh the repositories.

NOTE: If any error occurs while executing `zypper ref` command, ensure to resolve the error before proceeding.

7 Check the repositories using the `zypper lr` command. It should list the following repositories, and they should be enabled.

- OES11-SP3-Pool
- OES11-SP3-Updates
- OES2015-SP1-Pool
- OES2015-SP1-Updates
- SLES11-SP4-Pool
- SLES11-SP4-Updates

8 Perform a distribution upgrade using the `zypper dup --from SLES11-SP4-Pool --from SLES11-SP4-Updates --from OES2015-SP1-Pool --from OES2015-SP1-Updates` command.

- `The following product is going to be upgraded:`

```
Novell Open Enterprise Server 11 SP3
```

- `The following packages are going to be downgraded:`

  ```
  ifolder3-clients novell-NDSbase novell-NDSbase-32bit novell-NDScommon
  novell-NDSimon novell-NDSmasv novell-NDSmasv-32bit novell-NDSrepair novell-
  NDSserv novell-NDSserv-32bit novell-NLDAPbase novell-NLDAPbase-32bit
  novell-NLDAPsdk novell-NLDAPsdk-32bit novell-NOVLembox novell-NOVLice
  novell-NOVLice-32bit novell-NOVLsnmp novell-NOVLsubag novell-dclient
  novell-dclient-32bit novell-edirectory-jclnt novell-edirectory-ldap-
  extensions novell-edirectory-ldap-extensions-32bit novell-edirectory-
  log4cxx novell-edirectory-tsands novell-edirectory-tsands-32bit novell-
  edirectory-xdasinstrument novell-edirectory-xdaslog novell-ganglia-
  monitor-core-gmetad novell-ganglia-monitor-core-gmond novell-ganglia-web
  novell-nmas novell-nmas-libnmasext novell-nmas-libnmasext-32bit novell-
  nmas-libspmclnt novell-nmas-libspmclnt-32bit novell-nmasclient novell-
  nmasclient-32bit novell-npkiapi novell-npkiapi-32bit novell-npkiserver
  novell-npkiserver-32bit novell-npkit novell-npkit-32bit novell-ntls novell-
  ntls-32bit novell-plugin-nmas novell-plugin-pki novell-sss
  ```

  NOTE: The packages listed here may vary based on your setup.

Verify the products to be upgraded and enter 'y' to continue.

9. Once the upgrade is successfully completed, run the `zypper rr OES2015-SP1-Pool OES2015-SP1-Updates` command to remove the OES2015-SP1-Pool and OES2015-SP1-Updates repositories that are added manually.
10. Run the `suse_register -L /root/.suse_register.log` command to remove the old repositories (OES11-SP3) and to obtain the OES2015-SP1 repositories.

    NOTE: If any error occurs while executing this command, repeat Step 2 on page 154 with SLES and OES activation key.

11. Run the `zypper ar -c -f <URL_Of_OES2015SP1_Media_Network_Source> <OES2015SP1-Media>` command to add the OES2015-SP1 media.

    For example,

    - If CD is used to add repositories, run the following command:

      ```
      zypper ar -c -f /media/OES2015-SP1-addon-x86_6400521 OES2015SP1-Media
      ```

    - If Network Source is used to add repositories, run the following command:

      ```
      zypper ar -c -f http://10.0.0.0/install/OES2015SP1-Media OES2015SP1-Media
      ```

      Where 10.0.0.0 is the server IP address of the network source.

12. Reboot the server.
13. After the reboot, log on to the server and run the `yast2 channel-upgrade-oes` command to complete the OES services reconfiguration. This will prompt for eDirectory or DSfW password if the answer file is not created. Provide the password and continue. For more information on creating the answer file, see Section 5.6.3, “Creating an Answer File to Provide the eDirectory and DSfW Passwords,” on page 145.

5.9 Verifying That the Upgrade Was Successful

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

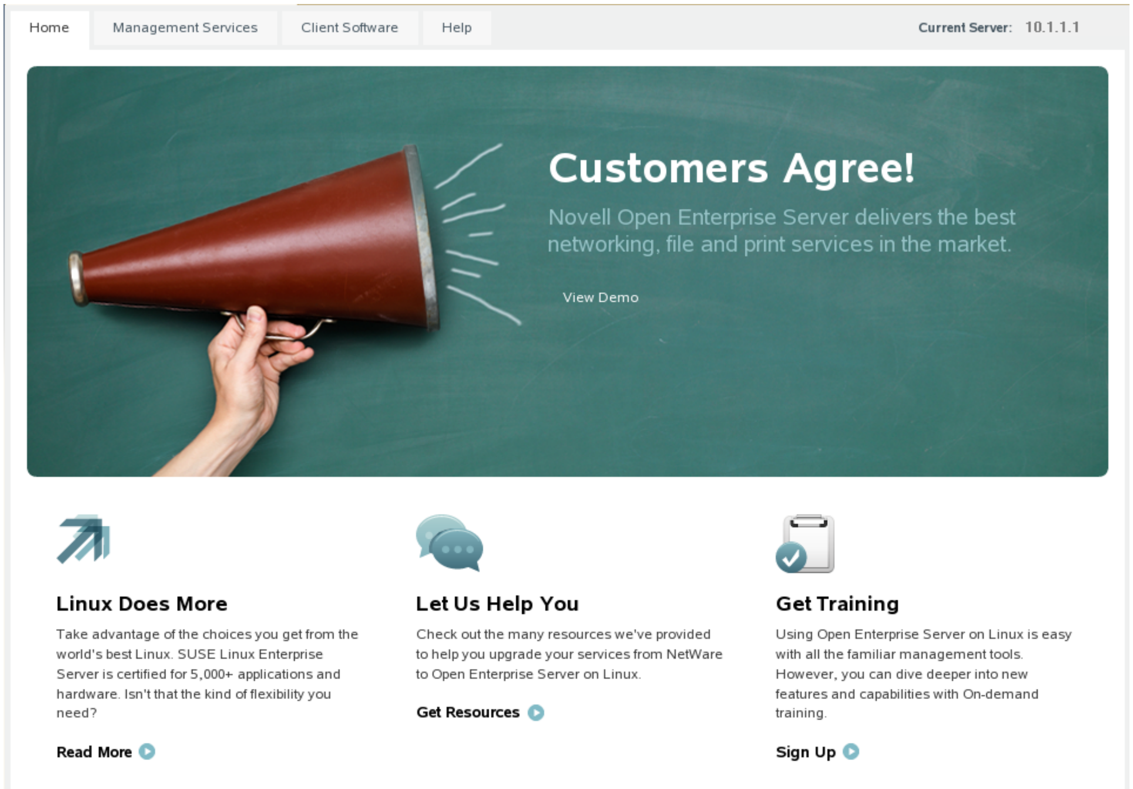
You can also quickly verify a successful installation by accessing the server from your Web browser.

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:



Customers Agree!

Novell Open Enterprise Server delivers the best networking, file and print services in the market.

Linux Does More

Take advantage of the choices you get from the world's best Linux. SUSE Linux Enterprise Server is certified for 5,000+ applications and hardware. Isn't that the kind of flexibility you need?

Let Us Help You

Check out the many resources we've provided to help you upgrade your services from NetWare to Open Enterprise Server on Linux.

Get Training

Using Open Enterprise Server on Linux is easy with all the familiar management tools. However, you can dive deeper into new features and capabilities with On-demand training.

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 SLES and OES using the following command. It should be SLES 11 SP4 and OES 11 SP3.

```
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 11 SP3 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 158.

5.10 Moving to Common Proxy Users After an Upgrade

After you successfully upgrade to OES 11 SP3 from OES 2 SP3, OES 11, OES 11 SP1 or OES 11 SP2, it is recommended to run the `move_to_common_proxy.sh` script as a post-upgrade activity. This script moves services (CIFS, DNS, DHCP, iFolder, 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. After migrating OES 2 SP3, OES 11, OES 11 SP1 or OES 11 SP2 to OES 11 SP3, 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
   ```

   IMPORTANT: If you choose to provide your own password, it should conform to the policy that is in effect for common proxy user. If the password contains single (') or double (") quotes, OES configuration fails. Quotes must be escaped by prefixing them with a backslash \. For example, to add a single quote, escape it as nove\'ll. The system-generated password always conforms to the policy rules.

After moving to common proxy user, verify the value of the field `CONFIG_LDAP_PROXY_CONTEXT` in the file `/etc/sysconfig/novell/oes-ladp`. 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-ladp`.

5.11 What's Next

After you complete the upgrade and verify that it was successful, see “Completing OES Installation or Upgrade Tasks” on page 159.

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 159
- Section 6.2, "Rebooting the Server after Installing NSS," on page 161
- Section 6.3, "Restarting Tomcat," on page 161
- Section 6.4, "Launching and Configuring Firefox for Linux," on page 161
- Section 6.5, "Implementing Digital Certificates in an OES Environment," on page 161

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.

For more information, see "Caveats for Implementing OES 11 SP3 Services" in the *OES 11 SP3: Planning and Implementation Guide*.

If a component requires additional configuration that is not part of the Novell Open Enterprise Server (OES) 11 SP3 installation, see the component's administration guide for more information. The following table include links to the installation and configuration information for most OES 11 SP3 services.

Table 6-1 *OES 11 SP3 Services Additional Installation and Configuration Instructions*

OES 11 SP3 Service	For Additional Installation and Configuration Information
Domain Services for Windows	See "Installing Domain Services for Windows" in the *OES 11 SP3: Domain Services for Windows Administration Guide*.
Novell AFP	See "Installing and Setting Up AFP" in the *OES 11 SP3: Novell AFP for Linux Administration Guide*.
Novell Archive and Version Services	See "Setting Up Archive and Version Services " in the *OES 11 SP3: Novell Archive and Version Services Administration Guide*.
Novell Backup/Storage Management Services (SMS)	See "Installing and Configuring SMS" in the *OES 11 SP3: Storage Management Services Administration Guide for Linux*.
Novell CIFS	See "Installing and Setting Up CIFS" in the*OES 11 SP3: Novell CIFS for Linux Administration Guide*.

OES 11 SP3 Service	For Additional Installation and Configuration Information
Novell Cluster Services	See “Installing, Configuring, and Repairing Novell Cluster Services” in the *OES 11 SP3: Novell Cluster Services for Linux Administration Guide*.
Novell DHCP	See “Installing and Configuring DHCP ” in the *OES 11 SP3: Novell DNS/ DHCP Services for Linux Administration Guide*.
Novell DNS	See “Installing and Configuring DNS ” in the *OES 11 SP3: Novell DNS/ DHCP Services for Linux Administration Guide*.
NetIQ eDirectory 8.8	See “Installing or Upgrading NetIQ eDirectory on Linux” in the *NetIQ eDirectory 8.8 SP8 Installation Guide*.
Novell iFolder 3.9	When you configure iFolder as part of the OES install and configuration, you can specify only an EXT3 or ReiserFS volume location for the System Store Path, which is where you are storing iFolder data for all your users. You cannot create NSS volumes during the system install. If you want to use an NSS volume to store iFolder data, you must reconfigure iFolder after the initial OES installation. To reconfigure, use Novell iManager to create an NSS volume, then go to **YaST** > **Open Enterprise Server > Install and Configure Open Enterprise Services** and select iFolder 3.9 to enter new information. All previous configuration information is removed and replaced. See “Installing and Configuring iFolder Services” in the *Novell iFolder 3.9.2 Administration Guide*.
Novell iManager 2.7.7	See “Installing iManager” in the *NetIQ iManager Installation Guide*.
Novell iPrint	See “Installing and Setting Up iPrint on Your Server” in the *OES 11 SP3: iPrint Linux Administration Guide*.
Novell Linux User Management	See “Setting Up Linux User Management” in the *OES 11 SP3: Novell Linux User Management Administration Guide*.
Novell NCP Server	See “Installing and Configuring NCP Server for Linux” in the *OES 11 SP3: NCP Server for Linux Administration Guide*.
Novell NetStorage	See “Installing NetStorage” in the *OES 11 SP3: NetStorage Administration Guide for Linux*.
Novell QuickFinder	See “Installing QuickFinder Server” in the *OES 11 SP3: Novell QuickFinder Server 5.0 Administration Guide*.
Novell Remote Manager	See “Changing the HTTPSTKD Configuration” in the *OES 11 SP3: Novell Remote Manager Administration Guide*.
Novell Samba	See “Installing the Novell Samba Components” in the *OES 11 SP3: Novell Samba Administration Guide*.
Novell Storage Services	See “Installing and Configuring Novell Storage Services” in the *OES 11 SP3: NSS File System Administration Guide for Linux*.
Pre-Migration Server	See “Preparing for Transfer ID” in the *OES 11 SP3: 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` at the command 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 at a command line prompt.

```
/etc/init.d/novell-tomcat6 restart
```

6.4 Launching and Configuring Firefox for Linux

After upgrading to OES 11 SP3, you need to launch and configure Mozilla Firefox before accessing other applications via a URL.

For example, you cannot configure the Novell Customer Center from the YaST until Firefox is configured.

To configure Firefox:

1. On the GNOME desktop, click **Computer** > **Firefox**.

   or

   On the KDE desktop, click the **Main Menu** icon > **Browse** > **Web Browser** > **Firefox**.
2. When Firefox opens, configure the browser by supplying all of the information that it requests. After Firefox is ready to browse the Internet, it is also ready to be used with OES.

6.5 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.

6.5.1 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).

6.5.2 Reconfiguring Services after Importing the Certificate

The following services must reconfigured so that these services use the latest verified certificate: LDAP, Apache, and LUM.

Reconfiguring LDAP

To point the LDAP server object to the verified certificate:

1. Log in to iManager with administrative privileges.
2. Click the **LDAP > LDAP Options > View LDAP Groups** tab and the LDAP group, then select the **Require TLS for Simple Binds with Password** check box.
3. Click **Apply** and **OK**.
4. Click the **LDAP Options > View LDAP Servers** tab, then click the LDAP server **> Connections**. In the Server Certificate text box, search for and select the certificate that you created.
5. Click **Apply** and **OK**.
6. Repeat Step 4 and Step 5 for all the LDAP servers in the LDAP group.

Reconfiguring Apache

- If you have used an eDirectory SSL certificate, see the TID on How to use eDirectory SSL certificates for Apache2 on SLES OES (7014029) to reconfigure Apache.
- If you have used a third-party SSL certificate, see the TID on Using Apache SSL default certificates or third party certificates on SLES (7004384) to reconfigure Apache.

Reconfiguring LUM

For LUM to use the latest signed certificate:

1 Rename the .der certificate that you generated in Step 3 in Section 6.5.1, “Configuring the Digital Certificate,” on page 162 to `.<your OES IP address>.der` format and copy it to `/var/lib/novell-lum`.

For example, to rename `SourceCert.der`, execute `cp /root/certs/SourceCert.der /var/lib/novell-lum/.198.162.1.1.der`.

2 Refresh the nam settings using the `namconfig cache_refresh` command.

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 Updating (Patching) an OES 11 SP3 Server

Updating an Novell Open Enterprise Server (OES) 11 SP3 Linux server is essentially the same as updating a SUSE Linux Enterprise Server (SLES) 11 SP4 server except that you apply patches for both SLES 11 SP4 and OES 11 SP3.

To update your server with the patches released from Novell 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 7.1, “Overview of Updating (Patching),” on page 165
- Section 7.2, “Preparing the Server for Updating,” on page 166
- Section 7.3, “Registering the Server in the Novell Customer Center,” on page 167
- Section 7.4, “Updating the Server,” on page 171
- Section 7.5, “Verifying That Your Repository Subscriptions Are Up-to-Date,” on page 172
- Section 7.6, “Frequently Asked Questions about Updating,” on page 173
- Section 7.7, “Patching From Behind a Proxy Server,” on page 173
- Section 7.8, “GUI Based Patching,” on page 173
- Section 7.9, “Quick Path Updating,” on page 173
- Section 7.10, “Installing the Latest iManager NPMs After Applying OES Patches,” on page 175
- Section 7.11, “Restarting the OES Instance of Tomcat After Applying a Tomcat Update,” on page 176

7.1 Overview of Updating (Patching)

- Section 7.1.1, “The Patch Process Briefly Explained,” on page 165
- Section 7.1.2, “Update Options,” on page 166

7.1.1 The Patch Process Briefly Explained

The OES 11 SP3 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.

7.1.2 Update Options

OES 11 SP3 administrators have three options for updating servers with patches from Novell.

- **Novell Online Update Servers:** For those who don't require an internal update source, OES 11 SP3 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=5YxjWD8_ZZk~).
- **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).

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.

7.2 Preparing the Server for Updating

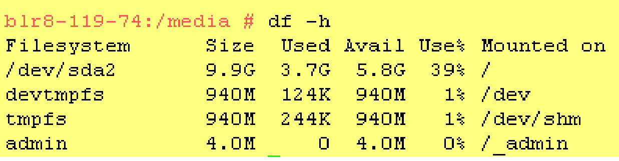
1 Make sure you have installed all the services that you need on the server.

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

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

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

Example: List with df -h.



```
blr8-119-74:/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 in `/var/cache/zypp/`.

Depending on the number of patches that you are going to apply, you might need about 3 GB for OES 11 SP3.

3. Before updating the server, secure the current data on the server.

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

7.3 Registering the Server in the Novell Customer Center

Before you can patch an OES 11 SP3 server with updates from Novell, 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 Novell 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 7.3.1, “Prerequisites,” on page 167
- Section 7.3.2, “Registering the Server in the Novell Customer Center Using the Command Line,” on page 168
- Section 7.3.3, “Registering the Server in the Novell Customer Center Using the GUI,” on page 168

7.3.1 Prerequisites

To complete these procedures, you must have the following:

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

  For more information about creating a Novell Customer Center account, see “Creating an Account” in the *Novell Customer Center User Guide* (http://www.novell.com/documentation/ncc/ncc/data/b5exp8k.html#b5exj2f). This is the same account that you use for Bugzilla.
- The activation codes for SLES and OES 11 SP3 that you received when you purchased your product.
- An established connection to the Internet.

7.3.2 Registering the Server in the Novell 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-sles=*SLES_registration_code* -a regcode-oes=*oes11_registration_code*

   For example:

   ```
   suse_register -a email=joe@example.com -a regcode-sles=4adab769abc68 -a
   regcode-oes=30a74ebb94fa
   ```

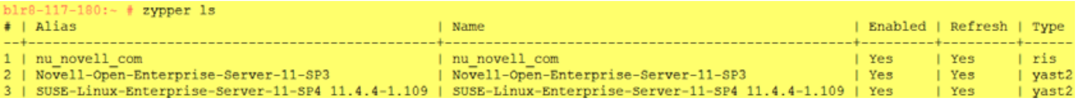
   IMPORTANT: If you are replacing evaluation codes with purchased codes, simply enter the codes. No further action is required.

3. Verify that the server is registered by checking whether you have the service types and catalogs needed for updates:

   3a To verify the service type, enter

   ```
   zypper ls
   ```

   The results should be similar to the following:



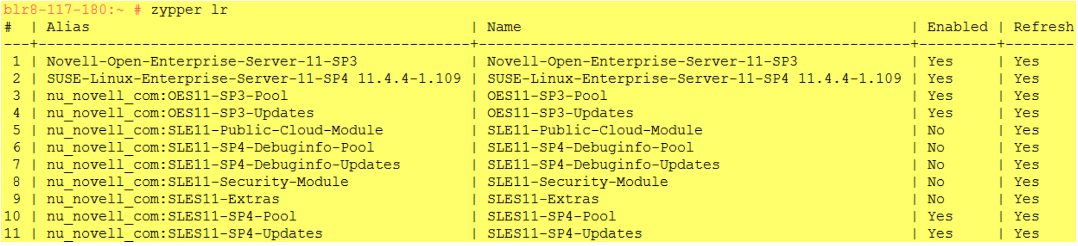
```
blr8-117-180:~ # zypper ls
# | Alias                                         | Name                                          | Enabled | Refresh | Type
--+-----------------------------------------------+-----------------------------------------------+---------+---------+------
1 | nu_novell_com                                 | nu_novell_com                                 | Yes     | Yes     | ris
2 | Novell-Open-Enterprise-Server-11-SP3          | Novell-Open-Enterprise-Server-11-SP3          | Yes     | Yes     | yast2
3 | SUSE-Linux-Enterprise-Server-11-SP4 11.4.4-1.109 | SUSE-Linux-Enterprise-Server-11-SP4 11.4.4-1.109 | Yes     | Yes     | yast2
```

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

   3b To verify the catalogs, enter

   ```
   zypper lr
   ```

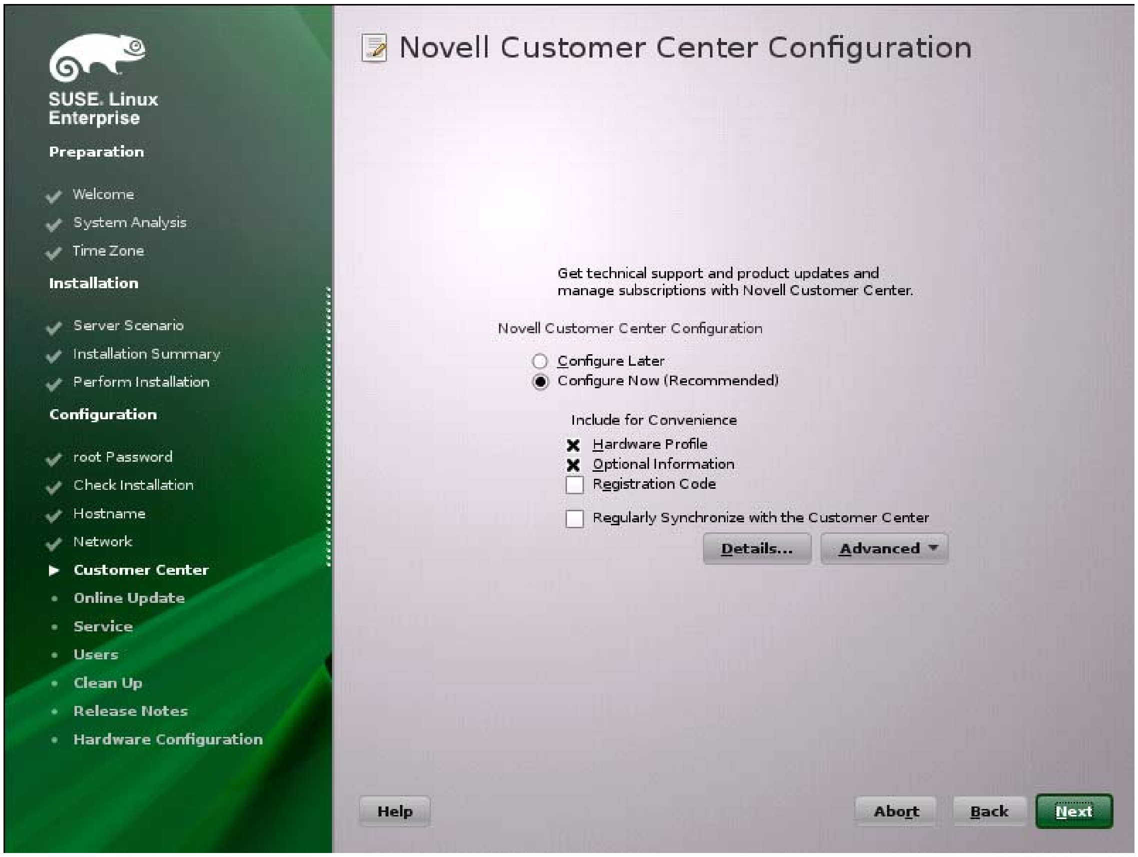
   The results should be similar to the following:



```
blr8-117-180:~ # zypper lr
#  | Alias                                            | Name                                             | Enabled | Refresh
---+--------------------------------------------------+--------------------------------------------------+---------+--------
 1 | Novell-Open-Enterprise-Server-11-SP3             | Novell-Open-Enterprise-Server-11-SP3             | Yes     | Yes
 2 | SUSE-Linux-Enterprise-Server-11-SP4 11.4.4-1.109 | SUSE-Linux-Enterprise-Server-11-SP4 11.4.4-1.109 | Yes     | Yes
 3 | nu_novell_com:OES11-SP3-Pool                     | OES11-SP3-Pool                                   | Yes     | Yes
 4 | nu_novell_com:OES11-SP3-Updates                  | OES11-SP3-Updates                                | Yes     | Yes
 5 | nu_novell_com:SLE11-Public-Cloud-Module          | SLE11-Public-Cloud-Module                        | No      | Yes
 6 | nu_novell_com:SLE11-SP4-Debuginfo-Pool           | SLE11-SP4-Debuginfo-Pool                         | No      | Yes
 7 | nu_novell_com:SLE11-SP4-Debuginfo-Updates        | SLE11-SP4-Debuginfo-Updates                      | No      | Yes
 8 | nu_novell_com:SLE11-Security-Module              | SLE11-Security-Module                            | No      | Yes
 9 | nu_novell_com:SLES11-Extras                      | SLES11-Extras                                    | No      | Yes
10 | nu_novell_com:SLES11-SP4-Pool                    | SLES11-SP4-Pool                                  | Yes     | Yes
11 | nu_novell_com:SLES11-SP4-Updates                 | SLES11-SP4-Updates                               | Yes     | Yes
```

7.3.3 Registering the Server in the Novell Customer Center Using the GUI

1. In the **YaST Control Center**, click **Other** > **Novell Customer Center Configuration**.
2. On the Novell Customer Center Configuration configuration page, select all of the following options, then click **Next**.



Novell Customer Center Configuration

Get technical support and product updates and manage subscriptions with Novell Customer Center.

Novell Customer Center Configuration

○ Configure Later
● Configure Now (Recommended)

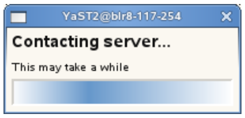
Include for Convenience

☒ Hardware Profile
☒ Optional Information
□ Registration Code

□ Regularly Synchronize with the Customer Center

- **Configure Now:** Proceeds with registering this server and the OES product with the Novell Customer Center.
- **Hardware Profile:** Sends information to the Novell Customer Center about the hardware that you are installing SLES 11 SP4 and OES 11 SP3 on.
- **Optional Information:** Sends optional information to the Novell 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.



Contacting server...

This may take a while

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

4 On the Novell Customer Center Registration page, specify the required information in the following fields:

- **Email Address:** The e-mail address for your Novell Login account.
- **Confirm Email Address:** The same e-mail address for your Novell Login account

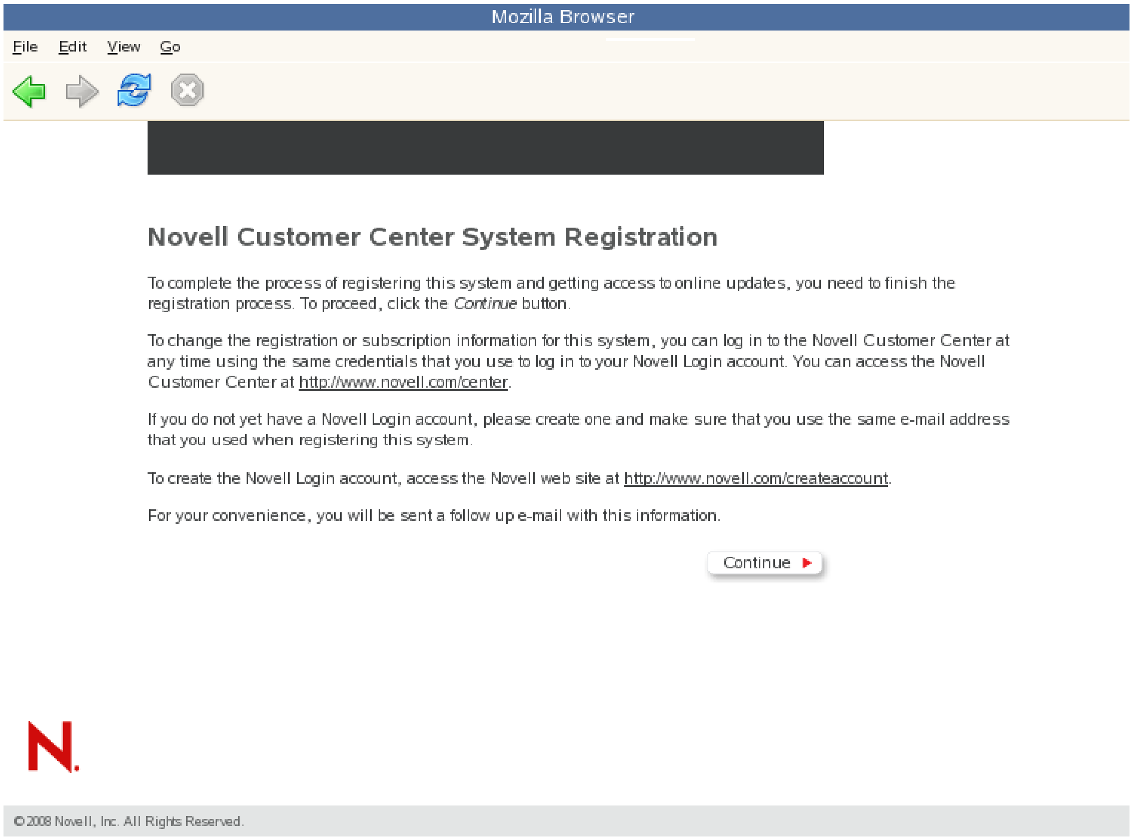
- **SUSE Linux Enterprise Server 11 SP4 (optional):** Specify your purchased or 60-day evaluation registration code for the SLES 11 SP4 product.

  If you don’t specify a code, the server cannot receive any updates or patches.
- **Open Enterprise Server 11 SP3 (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 Novell Customer Center, specify a description to identify this server.

5 Click **Submit**.

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



Novell Customer Center System Registration

To complete the process of registering this system and getting access to online updates, you need to finish the registration process. To proceed, click the *Continue* button.

To change the registration or subscription information for this system, you can log in to the Novell Customer Center at any time using the same credentials that you use to log in to your Novell Login account. You can access the Novell Customer Center at http://www.novell.com/center.

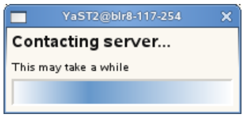
If you do not yet have a Novell Login account, please create one and make sure that you use the same e-mail address that you used when registering this system.

To create the Novell Login account, access the Novell web site at http://www.novell.com/createaccount.

For your convenience, you will be sent a follow up e-mail with this information.

© 2008 Novell, Inc. All Rights Reserved.

After you click **Continue**, the following message is displayed with the Manual Interaction Required page. Wait until this message disappears and the Novell Customer Center Configuration Was Successful page displays.



Contacting server...

This may take a while

7 When you see the message that the Novell Customer Center was successful, click **OK**.

When the registration is successful, the server is registered in the Novell Customer Center and the installation sources for patches are configured on the server.

7.4 Updating the Server

After the server has been registered in the Novell Customer Center, you can apply updates via packages and 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 7.4.1, “Updating the Server Using the Command Line,” on page 171

You could also patch an OES server using the following methods: Section 7.8, “GUI Based Patching,” on page 173, , Section 7.7, “Patching From Behind a Proxy Server,” on page 173, and so on.

7.4.1 Updating the Server Using the Command Line

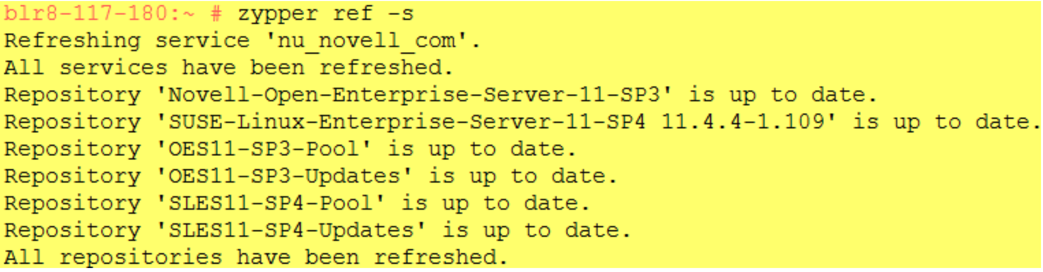
After you have registered the server in the Novell Customer Center, you can update the server by using commands at the command line. The following procedure specifies steps for updating the server with all available patches for SLES 11 SP4 and OES 11 SP3.

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
```



```
blr8-117-180:~ # zypper ref -s
Refreshing service 'nu_novell_com'.
All services have been refreshed.
Repository 'Novell-Open-Enterprise-Server-11-SP3' is up to date.
Repository 'SUSE-Linux-Enterprise-Server-11-SP4 11.4.4-1.109' is up to date.
Repository 'OES11-SP3-Pool' is up to date.
Repository 'OES11-SP3-Updates' is up to date.
Repository 'SLES11-SP4-Pool' is up to date.
Repository 'SLES11-SP4-Updates' is up to date.
All repositories have been refreshed.
```

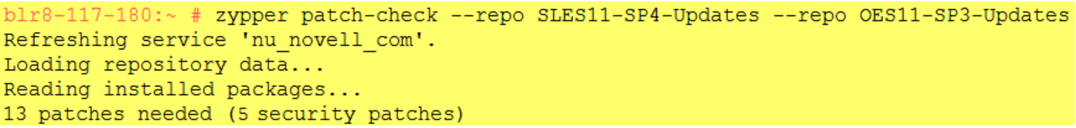
2b See whether updates are available for SLES 11 SP4 and OES 11 SP3:

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

For example,

```
zypper patch-check --repo SLES11-SP4-Updates --repo OES11-SP3-Updates
```

Updates available



```
blr8-117-180:~ # zypper patch-check --repo SLES11-SP4-Updates --repo OES11-SP3-Updates
Refreshing service 'nu_novell_com'.
Loading repository data...
Reading installed packages...
13 patches needed (5 security patches)
```

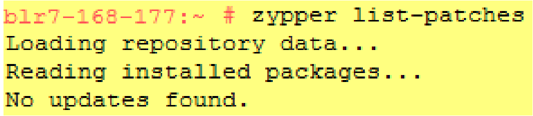
2c Update the server with all available SLES11 and OES 11 patches:

```
zypper up -t patch -r SLES11-SP4-Updates -r OES11-SP3-Updates
```

NOTE: When you install CIFS package using the command line (patch install, rpm upgrade, zypper updates and so on), you will get the 16024 Add method error. You can ignore this error as it does not cause disruption to any service.

Cause: While installing a newer CIFS version, the setup might try to pull in few NMAS methods that are existing on your server. This would be seen only when the patches are updated from the command line interface. The NMAS methods present in the server are retained and are not overwritten.

2d Repeat Step 2b and Step 2c until no more updates are available.



```
blr7-168-177:~ # zypper list-patches
Loading repository data...
Reading installed packages...
No updates found.
```

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.

For more information on zypper, see SDB:Zypper usage 11.3 (http://en.opensuse.org/SDB:Zypper_usage_11.3).

7.5 Verifying That Your Repository Subscriptions Are Up-to-Date

When an OES 11 SP3 server is updated properly, the update repository list is refreshed to include Updates entries for your OES 11 and SLES 11 versions.

To verify that you have updates from both update repositories:

1. At a terminal prompt on the server you have updated, enter the following command:

   ```
   zypper lr
   ```

   The list of repositories should include update repositories for your SLES 11 and OES 11 versions. For example, after updating an OES 11 server, the repositories listing should include both `SLES11-SP4-Updates` and `OES11-SP3-Updates` as subscribed update repositories.
2. After the repository list contains the correct entries, update your server by repeating the pertinent instructions in Section 7.4, “Updating the Server,” on page 171.

7.6 Frequently Asked Questions about Updating

This section contains the following information:

- Section 7.6.1, “Do I apply all the patches in the catalogs? How do I know which patches to apply?,” on page 173

7.6.1 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.

7.7 Patching From Behind a Proxy Server

See TID 3132246 (http://www.novell.com/support/viewContent.do?externalId=3132246&sliceId=2).

7.8 GUI Based Patching

The method of installing patches using the GUI is same for both OES 11 SP3 and SLES 11 SP4. For more information, see Installing Patches in the SLES 11 SP4 Administration Guide.

7.9 Quick Path Updating

This section contains the following Quick Path steps for patching an OES 11 server:

- Section 7.9.1, “Do Not Use zypper up without the -t Option,” on page 173
- Section 7.9.2, “Command Line Quick Path for Updating OES 11 SP3,” on page 174

7.9.1 Do Not Use zypper up without the -t Option

Do not use the `zypper up` command by itself to update an OES server. Always use the `-t patch` option as described in Section 7.9.2, “Command Line Quick Path for Updating OES 11 SP3,” on page 174.

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.

7.9.2 Command Line Quick Path for Updating OES 11 SP3

1 Make sure you have the following:

- A Novell Customer Center account

  If you don’t have one, create it at http://www.novell.com/register. This is the same account that you use for Bugzilla.

- Activation Codes for both SLES 11 SP4 and OES 11 SP3
- A valid installation source
- An established connection to the Internet
- All of the services installed that you need on the server.
- Enough disk space in `/var/cache/zypp/` where the update process downloads all the updates to.

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

- A backup of the current data on the server.

2 Register the server in the Novell Customer Center (one time only).

2a Log in to the server as `root` or su to `root`.

2b At the command line, enter

```
suse_register -a email=email_address -a regcode-
sles=SLES11_registration_code -a regcode-oes=oes11_registration_code
```

For example,

```
suse_register -a email=joe@example.com -a regcode-sles=4adab769abc68 -a
regcode-oes=30a74ebb94fa
```

2c Verify that the server is registered by checking to see whether you have the service types and catalogs needed for updates.

To verify the service types, enter:

```
zypper sl
```

To verify that you have the catalogs you need, enter:

```
zypper lr
```

3 Update the server with all available updates:

3a Refresh all services by entering:

```
zypper ref -s
```

3b See whether updates are available by entering:

```
zypper lu -r SLES11-SP4-Updates -r OES11-SP3-Updates
```

3c Update the server with all available SLES 11 SP4 and OES 11 SP3 patches by entering:

```
zypper up -t patch -r SLES11-SP4-Updates -r OES11-SP3-Updates
```

3d Repeat Step 3b and Step 3c until there are no more SLES 11 SP4 or OES 11 SP3 patches.

When there are no more patches, continue with Step 3e.

3e If the update requires a server reboot, do so when intimated by the system.

Rebooting the server activates the new kernel and ensures that OES services that need restarting after patching are restarted.

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 SLES11-SP4-Updates -r OES11-SP3-Updates
```

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

```
zypper pch SLES11-SP4-Updates OES11-SP3-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 SLES11-SP4-Updates -r OES11-SP3-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 oes11-CASA-3904-0
  ```

- 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 11 services are restarted.

7.10 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 2.7.7 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 `/etc/init.d/novell-tomcat6 restart` command.

7.11 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-tomcat6 restart` or `/etc/init.d/novell-tomcat6 restart` command. This loads all the latest libraries.

8 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 11 SP3 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 Automated Installation (http://www.suse.com/documentation/sles11/book_sle_deployment/data/cha_deployment_autoinst.html) in the SUSE Deployment Guide (http://www.suse.com/documentation/sles11/book_sle_deployment/data/cha_deployment_autoinst.html).

This section contains the following information:

8.1 Prerequisites

You need at least the following components to install an OES 11 SP3 server by using AutoYaST:

- ❐ A server with OES 11 SP3 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 178.

□ 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 184.

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

For more information, see “Setting Up an Installation Source” on page 184.

8.2 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 8.2.1, “Fixing an Automatically Created Control File,” on page 178.
- You can create or modify a control file by using the AutoInstallation module in YaST. For procedures, see Section 8.2.2, “Using the AutoInstallation Module to Create the Control File,” on page 179.

  This system depends on existing modules that are usually used to configure a computer after OES 11 is installed on a server.

8.2.1 Fixing an Automatically Created Control File

Review the following issues and solutions to fix the automatically created control file.

- **Issue 1:** If you install all OES Services through AutoYaST, Apache does not run.

  Solution: Reboot the server when the installation is complete; or, when you create the profile or control file, deselect the Print Server pattern in the Primary Functions category. If you have already created the control file, remove the following section:

```
- <printer>
  <cups_installation config:type="symbol">server< cups_installation>
  <default />
  <printcap config:type="list" />
  <server_hostname />
  <spooler>cups</spooler>
  </printer>
```

- **Issue 2:** The Certificate Authorities section of the control file is not created.

  Solution: You must insert the CA section manually.

  To add this information to the control file:

  1. Open YaST as `root`.
  2. Click **Miscellaneous** > **Autoinstallation**.
  3. Select **Security and Users** > **CA Management**, then click **Edit**.

4. In the **Common Name File** field, specify a name for the certificate. For example YaST_Default_CA(*hostname*).

5. Specify an e-mail name in the **Email** field.

6. Specify a password in the **Password** field.

7. Click **File > Save** to save the file. Ignore any error messages that you receive.

8. Click **View Source** to ensure that the CA entry was entered.

It should look similar to the following:

```
<ca_mgm>
    <CAName>YaST_Default_CA</CAName>
    <ca_commonName>YaST_Default_CA(hostname)</ca_commonName>
    <country>US</country>
    <importCertificate config:type="boolean">false</importCertificate>
    <locality></locality>
    <organization></organization>
    <organizationUnit></organizationUnit>
    <password>actual_password</password>
    <server_email>name@example.com</server_email>
    <state></state>
    <takeLocalServerName config:type="boolean">true</takeLocalServerName>
  </ca_mgm>
```

- **Issue 3:** If you install Novell Cluster Services, one package does not install correctly.

  Solution: Comment out the following line in the control file.

  ```
  <package>novell-cluster-services-kmp-smp</package>
  ```

  For example:

  ```
  <!--<package>novell-cluster-services-kmp-smp</package>-->
  ```

- **Issue 4:** 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>
  ```

8.2.2 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 11.

1 On a server that has OES 11 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 25. If the configuration contains the packages and selections you need, skip to Step 7. If not, continue with Step 6.

6 If necessary, change the package selections for the target servers:

6a In the Package Selection dialog box, click **Configure**.

6b On the Software Selection page, click **Patterns** in the **Filter** field.

6c Select the specific software items that you want to be added, then click **Accept**.

6d If you are prompted to accept the 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).

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) 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 Set a password for Certificate Authority management:

11a From the main window, click **Security and Users** > **CA Management** > **Configure**.

11b Type a password for the certificate in the **Password and Confirm Password** fields, then click **Finish**.

11c Verify that the Password status appears as **Set** on the **CA Management** page.

12 Configure OES Services:

12a 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 180. For more information about which modules are in each pattern, see "Deciding What Patterns to Install" on page 25.

Pattern	Other Module Dependencies
Novell AFP	◆ 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 Archive and Version Services	◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM) ◆ Novell Storage Services (NSS)
Novell Backup/Storage Management Services (SMS)	◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell CIFS	◆ Novell Backup / Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Storage Services (NSS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell Cluster Services (NCS)	◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell DHCP	◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell DNS	◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell Domain Services for Windows	◆ 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	◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)

Pattern	Other Module Dependencies
Novell FTP	◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell iFolder	◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell iManager	◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell iPrint	◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell iManager ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell Linux User Management (LUM)	◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Remote Manager (NRM)
Novell NCP Server / Dynamic Storage Technology	◆ Novell Backup/Storage Management Services (SMS) ◆ NetIQ eDirectory ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell NetStorage	◆ Novell Backup/Storage Management Services (SMS) ◆ Novell iManager ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell Pre-Migration Server	◆ Novell Backup / Storage Management Services (SMS) ◆ NetIQ eDirectory (without a replica) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell QuickFinder	◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM) ◆ Novell Remote Manager (NRM)
Novell Remote Manager (NRM)	◆ Novell Backup/Storage Management Services (SMS) ◆ Novell Linux User Management (LUM)

Pattern	Other Module Dependencies
Novell Samba	- Novell Backup/Storage Management Services (SMS) - Novell Linux User Management (LUM) - Novell Remote Manager (NRM)
Novell Storage Services (NSS)	- Novell Backup/Storage Management Services (SMS) - NetIQ eDirectory - Novell NCP Server - Novell Linux User Management (LUM) - Novell Remote Manager (NRM)

12b 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.

12c Verify that the settings for each module are what you want.

If not, click **Reset Configuration** and provide the corrected settings.

12d Repeat Step 12a through Step 12c until all the required modules have been configured, then continue with Step 13.

13 Save the file.:

13a Click **File** > **Save**.

13b Browse to a location that you want to save the file to.

13c 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/).

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

15 Proceed with “Setting Up an Installation Source” on page 184.

8.3 Setting Up an Installation Source

For OES 11 SP3, you must set up a separate directory for the SLES 11 SP4 software and the OES 11 SP3 software.

AutoYaST requires an installation source. You have several options. For an explanation of each, see “Network Based Installation” (http://doc.opensuse.org/projects/YaST/openSUSE11.3/autoinstall/Bootmanagement.html) and “The Auto-Installation Process” in *Automatic Linux Installation and Configuration with Yast2* (http://doc.opensuse.org/projects/YaST/openSUSE11.3/autoinstall/).

8.4 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.

8.4.1 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.

8.4.2 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).

```
<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 `OES11-SP3-addon_with_SLES11-SP4-x86_64-DVD.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>
```

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
```

5 Press Enter and the OES installation and configuration starts and completes without any user intervention.

9 Installing OES as a VM Host Server

You can install Novell Open Enterprise Server (OES) 11 as a VM host server for either the Xen or KVM virtualization services included with SLES 11. To understand why you might want your VM host server to have OES 11 installed, see "Why Install OES Services on Your VM Host?" in the *OES 11 SP3: Planning and Implementation Guide*.

IMPORTANT: Only Xen supports NetWare 6.5 SP8 running as a VM guest server. KVM does not.

Both Xen and KVM support OES 11 running as a VM guest server.

9.1 Installing the KVM Hypervisor and Tools

IMPORTANT: KVM requires a server that supports Intel Virtualization Technology (VT) with VT enabled.

The following instructions assume that you are installing OES 11 SP3 and the KVM hypervisor and tools on a SLES 11 SP4 server that you have previously installed. You can also install KVM at the same time as SLES.

For more information about KVM, see the *Virtualization with KVM* (http://www.suse.com/documentation/sles11/book_kvm/data/book_kvm.html) guide.

1. To install KVM, on the SLES 11 SP4 server desktop click **Computer > YaST > Virtualization > Install Hypervisor and Tools**.
2. Select **KVM**, click **Accept > Install**.
3. Click **Yes** to install a network bridge.

   After the software installs and configures, you are prompted to restart the machine. To avoid an interruption, you can do this in Step 15.
4. To install OES 11, under **Software**, click **Add-on Products**.
5. On the Installed Add-On Products page, click **Add**.
6. On the Media Type page, specify the type of your OES 11 installation media you are using and click **Next** and add the installation media.

   For more information, see Section 3.5, "Specifying the Add-On Product Installation Information," on page 48.
7. On the Software Selections page, scroll down to the **OES Services** category.

   Only the following are supported on a VM host server:

   - Novell iPrint
   - Novell Linux User Management (LUM)

- Novell Storage Management Services (SMS)
- Novell Cluster Services (NCS)

  You can select any of these services that you want to be available on the host server, or you can leave all of the services deselected. In either case, the server will be configured as an OES server.

8. If you selected any of the supported OES services, Novell Remote Manager (NRM) is also selected. Click the green check mark by NRM to deselect NRM and prevent it from being installed. NRM is not a supported OES service on a VM host server.
9. Click **Accept**.

   OES 11 is installed.
10. On the Configured LDAP Servers page, specify the tree name, admin name, and password for the eDirectory tree into which you are installing the host server.

    IMPORTANT: If you didn't select any OES services, the Novell Open Enterprise Server Configuration page appears instead. In that case, the Configured LDAP Servers page is accessible via the **LDAP Configuration for Open Enterprise Services** link.
11. Click **Add** and specify the IP address of a server in the tree that has eDirectory installed on it, then click **Next**.
12. On the Novell Open Enterprise Server Configuration page, click **Next**.
13. On the Installation Completed page, click **Finish**.
14. On the Novell Customer Center page, select **Registration Code** and click **Next**. Register your OES 11 server.

    For more information, see Chapter 7, "Updating (Patching) an OES 11 SP3 Server," on page 165.
15. Shut down, and then restart the server.

The server is now prepared to function as a KVM VM host server. For instructions on starting and running the server, see the *Virtualization with KVM* (http://www.suse.com/documentation/sles11/book_kvm/data/book_kvm.html) guide.

9.2 Installing the Xen Hypervisor and Tools

The following instructions assume that you are installing OES 11 SP3 and the Xen hypervisor and tools on a SLES 11 SP4 server that you have previously installed.

NOTE: You can also install Xen and OES 11 SP3 at the same time as SLES either using the integrated SLES 11 SP4 with OES media or using OES 11 SP3 add-on media. For either of these later options, the instructions that follow require slight but straight-forward adjustments.

For more information about Xen, see the *Virtualization with Xen* (http://www.suse.com/documentation/sles11/book_xen/data/book_xen.html) guide.

1. To install Xen, on the SLES 11 SP4 server desktop click **Computer > YaST > Virtualization > Install Hypervisor and Tools**.
2. Select **Xen**, click **Accept > Install**.
3. Click **Yes** to install a network bridge.

   After the software installs and configures, you are prompted to restart the machine. To avoid an interruption, you can do this in Step 15.

4 To install OES 11, under **Software**, click **Add-on Products**.

5 On the Installed Add-On Products page, click **Add**.

6 On the Media Type page, specify the type of your OES 11 installation media you are using and click **Next** and add the installation media.

For more information, see Section 3.5, “Specifying the Add-On Product Installation Information,” on page 48.

7 On the Software Selections page, scroll down to the **OES Services** category.

Only the following are supported on a VM host server:

- Novell iPrint
- Novell Linux User Management (LUM)
- Novell Storage Management Services (SMS)
- Novell Cluster Services (NCS)

You can select any of these services that you want to be available on the host server, or you can leave all of the services deselected. In either case, the server will be configured as an OES server.

8 If you selected any of the supported OES services, Novell Remote Manager (NRM) is also selected. Click the green check mark by NRM to deselect NRM and prevent it from being installed. NRM is not a supported OES service on a VM host server.

9 Click **Accept**.

OES 11 is installed.

10 On the Configured LDAP Servers page, specify the tree name, admin name, and password for the eDirectory tree into which you are installing the host server.

IMPORTANT: If you didn’t select any OES services, the Novell Open Enterprise Server Configuration page appears instead. In that case, the Configured LDAP Servers page is accessible via the **LDAP Configuration for Open Enterprise Services** link.

11 Click **Add** and specify the IP address of a server in the tree that has eDirectory installed on it, then click **Next**.

12 On the Novell Open Enterprise Server Configuration page, click **Next**.

13 On the Installation Completed page, click **Finish**.

14 On the Novell Customer Center page, select **Registration Code** and click **Next**. Register your OES 11 server.

For more information, see Chapter 7, “Updating (Patching) an OES 11 SP3 Server,” on page 165.

15 Shut down, and then restart the server.

16 To run the server as a Xen host, you must select the boot option that includes the Xen kernel . Alternatively, you can modify the boot loaded in YaST to load the Xen kernel by default.

9.3 Upgrading an OES 2 Xen VM Host Server to OES 11

The upgrade process of a Xen VM host server is exactly the same as upgrading a regular OES 2 server to OES 11, with one important difference. After the server is updated, the Xen Hypervisor might have an incorrect network configuration that prevents Xen from running.

SUSE has improved the network configuration in SLES 11. If you install SLES 11 SP4 and configure Xen, you get a bridged setup through YaST. However, if you upgrade from SLES 10 to SLES 11, the upgrade does not configure the bridged setup automatically. Until the bridged setup is configured for SLES 11, your Xen VM guest servers will not run. Be sure to set up the bridge using YaST as outlined in Section 9.4, “Setting Up Bridging After the Upgrade,” on page 190.

NOTE: If you have an advanced network configuration, refer to the SLES documentation for instructions on configuring your network settings during the upgrade. The instructions in this section assume a single network interface.

9.4 Setting Up Bridging After the Upgrade

After the upgrade completes and the server has all patches applied, do the following:

1. On the desktop, click **Computer > YaST**.
2. Click **Virtualization > Install Hypervisor and Tools**.
3. Select **Xen** and click **Accept**.
4. If prompted to install packages, click **Install**.
5. When prompted to configure a network bridge, click **Yes**.
6. When the hypervisor and tools installation is completed, click **OK**.
7. Click **YaST > Virtualization > VirtualMachineManager**.
8. Click **File > Add Connection > Connect**.

   Your VM guests are now able to be run.

10 Installing, Upgrading, or Updating OES on a VM

In Novell Open Enterprise Server (OES), you can install OES 11 SP3 as a guest operating system on the following servers:

- An OES 11 SP3 server that has been set up as a Xen-based host server

  See Chapter 9, “Installing OES as a VM Host Server,” on page 187.
- A SUSE Linux Enterprise Server (SLES) 11 SP4 Linux server running KVM.

  See the *Virtualization with KVM* (http://www.suse.com/documentation/sles11/book_kvm/data/book_kvm.html) guide.
- A SUSE Linux Enterprise Server (SLES) 11 SP4 Linux server running Xen.

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

For general information on the virtualization technology in SLES 11 SP4, see the SLES 11 documentation (http://www.suse.com/documentation/sles11/).

This section documents the system requirements, installation instructions, upgrade and migration instructions, and issues associated with setting up OES 11 SP3 on a Xen-based virtual machine.

10.1 System Requirements

To create an OES 11 SP3 VM guest, you need a SLES 11 SP4 or OES 11 SP3 server that is set up as a VM host server.

10.1.1 OES 11 SP3 VM Host Considerations

When you set up a virtual machine host for OES 11 SP3 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 > Network Services > NTP Time 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 11 SP3 virtual machine, you need a minimum of 2 GB of memory (1 GB for the host plus 1GB MB for the OES 11 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 11 SP3 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 11 SP3 cannot run as a paravirtualized guest on SLES 10 SP4 or earlier 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 up to 2E64 sectors (8388608 petabytes (PB) based on the 512-byte sector size.

For information, see "Device Size" in the *OES 11 SP3: NSS File System Administration Guide for Linux*.

10.1.3 Setup Instructions

As mentioned in Section 10.1, "System Requirements," on page 191, you can use either a SLES 11 SP4 server or an OES 11 SP3 server as your VM host server.

For setup procedures, see the following information:

- **SLES 11 SP4:** See the *Virtualization with KVM* (http://www.suse.com/documentation/sles11/book_xen/data/book_xen.html) and the *Virtualization with Xen* (http://www.suse.com/documentation/sles11/book_xen/data/book_xen.html)guides.
- **OES 11 SP3:** "Chapter 9, "Installing OES as a VM Host Server," on page 187."

10.2 Prerequisites

Before creating an OES 11 SP3 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 8, “Using AutoYaST to Install and Configure Multiple OES Servers,” on page 177.
- 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 193
- Section 10.3.2, “Preparing the Installation Source Files,” on page 193

10.3.1 Downloading the Installation Software

For information on downloading the following ISO image files, see the Novell Open Enterprise Server 11 Download Instructions (http://www.novell.com/documentation/oes11/esd/di_oes11.html).

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

ISO Image File	DVD Label
`OES11-SP3-addon-x86_64-DVD1.iso`	*Novell Open Enterprise Server 11 SP3 Media 1*
`SLES-11-SP4-DVD-x86_64-GM-DVD1.iso`	*SUSE Linux Enterprise Server 11 SP4 DVD*

10.3.2 Preparing the Installation Source Files

To create an OES 11 SP3 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 *SUSE Linux Enterprise Server 11 Deployment Guide* (http://www.suse.com/documentation/sles11/book_sle_deployment/data/sec_deployment_remoteinst_instserver.html).

10.4 Installing an OES 11 SP3 VM Guest

Creating an OES 11 SP3 virtual machine requires you to complete the following major tasks.

- Section 10.4.1, “Specifying Options for Creating an OES 11 SP3 VM Guest,” on page 194
- Section 10.4.2, “Specifying the Installation Mode,” on page 195
- Section 10.4.3, “Specifying the Add-On Product Installation Information,” on page 196
- Section 10.4.4, “Completing the OES 11 SP3 VM Guest Installation,” on page 197

10.4.1 Specifying Options for Creating an OES 11 SP3 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 most recent version of OES shown, then click **Forward**. The Summary page is displayed.

NOTE: Detailed explanations of the Summary page settings are available in "Virtualization: Configuration Options and Settings (http://www.suse.com/documentation/sles11/book_xen/data/cha_xen_config.html)" in the *Virtualization with Xen guide (http://www.suse.com/documentation/sles11/book_xen/data/book_xen.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 11 SP3 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 11 SP3 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 11 SP4 from a downloaded ISO image file, click **DVD**, browse to the SLES 11 SP4 image file, then click **Open > OK > Apply**.

11 If you are installing OES 11 SP3 from a downloaded ISO image file, click DVD, browse to the OES 11 SP3 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, make sure that the SLES 11 SP4 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 11 SP4 network installation source.

  You specify a network installation source for OES 11 SP3 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 usessh=1
  sshpassword=password
  ```
- **13e** Click **Apply**.

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

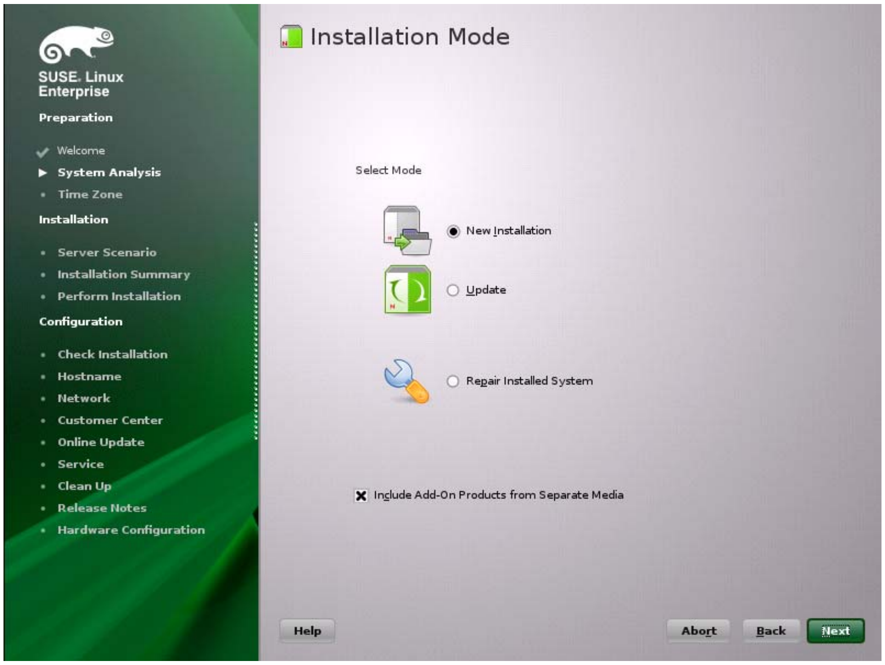
15 Continue with Section 10.4.2, “Specifying the Installation Mode,” on page 195.

10.4.2 Specifying the Installation Mode

1 When the **Installation Mode** screen displays, select the following menu options:

- **New Installation**

- **Include Add-On Products from Separate Media**



Installation Mode

Select Mode

● New Installation

○ Update

○ Repair Installed System

☒ Include Add-On Products from Separate Media

2 Click **Next**.

3 Continue with Section 10.4.3, “Specifying the Add-On Product Installation Information,” on page 196.

10.4.3 Specifying the Add-On Product Installation Information

When the Add-On Product Installation page displays:

1 Click **Add**.

2 If you are installing OES 11 SP3 from an ISO image file:

  2a On the Add-On Product Media page, click **Specify URL**, then click **Next**.

  2b In the URL field, type

```
hd:///?device=/dev/xvdc/
```

  2c Click **OK**.

  2d Skip to Step 4.

3 If you are installing from a network installation source, click the appropriate protocol for your situation, then click **Next** and supply the required information.

4 Read and accept the Novell Open Enterprise Server 11 license agreement, then click **Next**.

5 Confirm that the Add-On Product Installation page shows the correct path to the OES media, then click **Next**.

6 Continue with “Completing the OES 11 SP3 VM Guest Installation.”

10.4.4 Completing the OES 11 SP3 VM Guest Installation

1 Follow the on-screen prompts, using the information contained in the following sections:

1a Section 3.6, “Setting Up the Clock and Time Zone,” on page 48.

1b Section 3.7, “Specifying the Installation Settings for the SLES Base and OES Installation,” on page 48.

1c Section 3.8, “Specifying Configuration Information,” on page 55.

During the configuration portion of the installation, you might see additional prompts concerning hardware detection of the network cards, DSL, PPPoE DSL, ISDN cards, and modems.

When you specify the time source during the eDirectory configuration, use the same time source as the eDirectory tree you are installing the server into.

After the installation, enable the virtual machine’s Independent Wall Clock setting and reboot the virtual machine so it can synchronize its time correctly. For more information on this configuration issue, “Virtual Machine Clock Settings (http://www.suse.com/documentation/sles11/book_xen/data/sec_xen_guests_suse_time.html)” in the *Virtualization with Xen guide (http://www.suse.com/documentation/sles11/book_xen/data/book_xen.html)*.

1d Section 3.9, “Finishing the Installation,” on page 106.

During the hardware configuration, graphics and sound cards are not recognized when installing OES 11 SP3 as a VM guest.

2 Complete the server setup by following the procedures in “Chapter 6, “Completing OES Installation or Upgrade Tasks,” on page 159.”

10.5 Upgrading an OES VM Guest to OES 11 SP3

IMPORTANT: To upgrade an OES VM paravirtualized guest to OES 11 SP3, you must install using files on the network. Physical media upgrades and using ISO image files are not supported methods.

OES 11 SP3 cannot run as a paravirtualized guest on SLES 10 SP4 or earlier hosts.

Performing a down-server upgrade on a Xen VM guest running on a SLES 11/OES 11 SP3 VM host is very much like upgrading a physical machine

- Section 10.5.1, “Before You Start the Upgrade Process,” on page 197
- Section 10.5.2, “Starting the Upgrade,” on page 197

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 11 SP3,” on page 116 and Section 5.3, “Meeting the Upgrade Requirements,” on page 117.

10.5.2 Starting the Upgrade

1 In Virtual Machine Manager, shut down the OES 2 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 2**, 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 11 SP4 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 Section 5.4.5, "Selecting the Installation Mode Options," on page 126 and continue from there.

10.6 Managing a Virtual Machine Running OES 11 SP3

Managing a virtual machine running OES 11 SP3 is the same as managing virtual machines running other operating systems. See the instructions for your virtualization platform:

- "*Managing a Virtualization Environment* (http://www.suse.com/documentation/sles11/book_xen/data/cha_xen_manage.html)" in the *Virtualization with Xen guide* (http://www.suse.com/documentation/sles11/book_xen/data/book_xen.html).
- The *Virtualization with KVM guide* (http://www.suse.com/documentation/sles11/book_kvm/data/book_kvm.html).

10.7 Setting Up an OES 11 SP3 VM Guest to Use Novell Storage Services (NSS)

When you install OES 11 SP3 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 LVM2 (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 11 SP3: NSS File System Administration Guide for Linux*.

11 Installing and Managing NetWare on a Xen-based VM

IMPORTANT: NetWare 6.5 SP8 has been modified to run in paravirtual mode on a Xen virtual machine. Running NetWare in fully virtualized mode on a Xen host server or on a KVM host server is not supported.

You can install NetWare as a virtual machine guest (VM guest) operating system on the following servers:

- A SUSE Linux Enterprise Server (SLES) 11 SP4 Linux server

  See "Setting Up a Virtual Machine Host" (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/cha_xen_virtualization_vhost_setup.html) in the *Virtualization with Xen* guide (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/book_virtualization_xen.html).
- An OES 11 server that has been set up as a Xen-based host server

  See "Chapter 9, "Installing OES as a VM Host Server," on page 187."

For general information on the Xen virtualization technology in SLES 11 SP4, see the *Virtualization with Xen* guide (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/book_virtualization_xen.html).

NOTE: To get started with third-party virtualization platforms, such as Hyper-V from Microsoft and the different VMware product offerings, refer to the documentation for the product that you are using.

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

- Section 11.1, "Introduction," on page 199
- Section 11.2, "Support Information," on page 200
- Section 11.3, "Preparing to Install a NetWare VM Guest Server," on page 201
- Section 11.4, "Installing Virtualized NetWare," on page 204
- Section 11.5, "Managing NetWare on a Virtual Machine," on page 209
- Section 11.6, "If VM Manager Doesn't Launch on a Xen VM Host Server," on page 211

11.1 Introduction

To simplify the process of installing virtualization software, the SLES 11 SP4 software includes **Xen Virtual Machine Host Server** as a primary server function that you can select when installing SLES 11 SP4 as a virtualization host server.

Selecting this pattern installs the Xen host server software, which enables the server to boot the Xen version of the SLES 11 SP4 operating system kernel. It also installs utilities for preparing and creating virtual machines.

After the host server is up and running, you can then create a virtual machine and install NetWare 6.5 SP8 as a guest operating system.

11.2 Support Information

- Section 11.2.1, “OES Registration Is Required for Support,” on page 200
- Section 11.2.2, “Supported Configurations and Features,” on page 200
- Section 11.2.3, “Unsupported Configurations and Features,” on page 200

11.2.1 OES Registration Is Required for Support

Virtualized NetWare in Xen is an OES product feature. Support for NetWare on a Xen virtual machine is available only to registered OES customers.

11.2.2 Supported Configurations and Features

The following configurations and features are supported for NetWare VM guest servers.

- NetWare 6.5 SP7 and later running in paravirtual mode.
- The graphical paravirtualized frame buffer and the text-based console interface.
- Running on 32-bit, 32-bit PAE, and 64-bit hypervisors.
- Running in 32-bit PAE compatibility mode on 64-bit platforms.
- Up to 16 block devices.
- Up to 32 virtual CPUs.
- The pause and resume functionality.
- The `xm shutdown` command.
- The `shutdown` command in Virtual Machine Manager.
- Allocated memory from 1 GB to 8 GB.
- VCPU cover commitment, pinning, and capping.

11.2.3 Unsupported Configurations and Features

The following configurations and features are not supported for NetWare VM guest servers.

- NetWare in full virtualization mode.
- NetWare 6.5 SP6 and earlier running on a virtual machine.
- VCPU hotplug.
- Network or block device hotplug.
- Virtual memory resizing.
- Direct access to physical devices.
- The save, restore, and migrate commands.
- Some Novell Remote Manager debugging features.

11.3 Preparing to Install a NetWare VM Guest Server

- Section 11.3.1, “Planning for VM Host Servers,” on page 201
- Section 11.3.2, “Planning for NetWare VM Guest Servers,” on page 202
- Section 11.3.3, “You Must Use Timesync for Time Synchronization,” on page 203
- Section 11.3.4, “Disabling the Alt+Esc Shortcut on the Host,” on page 203

11.3.1 Planning for VM Host Servers

- “Meeting Server Hardware and Software Requirements” on page 201
- “Deciding Whether to Run OES Services on VM Host Servers” on page 201

Meeting Server Hardware and Software Requirements

To accommodate NetWare VM guest servers, your VM host servers must:

❒ Meet the criteria specified in “Setting Up a Virtual Machine Host” (http://www.suse.com/documentation/sles11/book_xen/data/cha_xen_vhost.html) in the *Virtualization with Xen* (http://www.suse.com/documentation/sles11/book_xen/data/book_xen.html) guide.

❒ Have enough memory (RAM) on the physical machine for:

- The SLES 11 operating system (512 MB)
- Any of the supported OES services that you install on the VM host (512 MB)
- Each NetWare virtual machine that you plan to run concurrently (1 GB to 8 GB)

For example, if you are installing one NetWare VM guest server on a SLES 10 VM host server, you need a minimum of 2 GB of memory: 1 GB for the VM host server and 1 GB for the NetWare VM guest server. For optimal performance, you should allocate as much memory as possible for each NetWare VM guest, up to 8 GB each.

❒ Have enough disk space on the host server for creating and running the VM guest servers.

The default disk space for a NetWare VM guest server is 10 GB. You might need more or less space, depending on what you will use the guest server for and what its storage configuration will be. You might want to locate your virtual machines on a separate partition or even on a separate storage device. For example, you might create a `/vm` partition on a separate drive installed in the server. For additional information, see “Storage Planning” on page 202.

Deciding Whether to Run OES Services on VM Host Servers

You should also decide whether to install OES 11 and one or more of its supported services on your VM host servers.

To ensure that optimal resources are available to the virtual machines, each VM host server should be dedicated to running the Xen virtualization software as much as possible. However, there are several good reasons why you might want to choose to install the supported OES services on the host server itself. For more information, see “Why Install OES Services on Your VM Host?” in the *OES 11 SP3: Planning and Implementation Guide*.

11.3.2 Planning for NetWare VM Guest Servers

Before creating NetWare virtual machines, you need to plan for the following:

- “RAM Planning” on page 202
- “Storage Planning” on page 202
- “Network Planning” on page 202
- “eDirectory Planning” on page 203

RAM Planning

To ensure the best performance by your NetWare VM guests, you should plan for the optimal RAM configuration of each NetWare VM guest server. As a general rule, the more RAM you assign to a NetWare guest server (up to 8 GB), the better the server performance is. For specific planning information, see “Optimizing Server Memory” in the *NW 6.5 SP8: Server Memory Administration Guide*.

Storage Planning

The first disk space that you allocate while creating the Xen virtual machines is used by the NetWare VM guest for the `sys:` volume. The partition where this is created should be formatted as an Ext2 partition (see “Xen VMs Need Ext2 for the System /Boot Volume” in the *OES 11 SP3: Planning and Implementation Guide*).

You can add other disk space as virtual devices for NSS pools and volumes. For best performance in a Xen virtual environment, NSS pools and volumes on NetWare should be created on virtual devices that live on SCSI devices, Fibre Channel devices, or iSCSI devices on the host server, or on partitions that are on those types of devices.

SATA or IDE disks have slower performance because special handling is required when working through the Xen driver to ensure that data writes are committed to the disk in the order intended before the driver reports back.

For more information on NSS disk storage, see “Using NSS in a Virtualization Environment” in the *OES 11 SP3: NSS File System Administration Guide for Linux*.

Network Planning

Each Xen guest VM is assigned one virtualized network card by default. You can create additional cards if desired.

You must obtain one static IP address for each virtualized network card you plan to create on your NetWare VM guest servers. OES 11 does not support dynamically assigned (DHCP) IP addresses.

eDirectory Planning

You can place a NetWare virtual machine in an existing tree or as the first server in a new tree. However, the performance of virtualized NetWare doesn't match a physical NetWare installation. In most cases, it is probably preferable to add your NetWare virtual machine to an existing tree located on a physical NetWare server, particularly if the tree is large.

Also, because virtualized servers might be started and stopped more often than they would normally be on physical servers, we recommend that the master replica (usually the first server in a tree) be placed on a system that is running at all times. For more information about master replicas, see "Managing Partitions and Replicas" in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

11.3.3 You Must Use Timesync for Time Synchronization

Because of known issues with Xen and the NTP NLM, you must use Timesync as the time synchronization method for NetWare VM guests running on Xen VM hosts. Otherwise, time drift causes problems for your NetWare VM guests.

Keeping accurate time is a critical function for servers in an eDirectory tree. The reported time must be synchronized across the network to provide the expiration dates and time stamps necessary for ordering eDirectory events.

NetWare VM guest servers synchronize time in the same ways that NetWare physical servers do. In other words, the clock on the VM host server has no influence on the NetWare VM guest server's time.

IMPORTANT: To ensure that your NetWare VM guest is configured correctly, be sure to follow the instructions in "Configuring Time Synchronization" (specifically Step 4) in the *NW65 SP8: Installation Guide*, and configure the NetWare VM guest to get time from the same time source as the eDirectory tree it is joining. If the time source specified is an NTP server, be sure to select the NTP option next to the source's DNS name or IP address. This enables Timesync to communicate with the NTP time source.

11.3.4 Disabling the Alt+Esc Shortcut on the Host

Alt+Esc is used on a NetWare server to switch between console screens, but on SLES 11 it moves between open windows. To provide the expected behavior for the virtualized NetWare server, you must disable the shortcut for SLES 11.

1. On the host server as the `root` user, click **Computer** > **Control Center**.
2. Click **Personal** > **Shortcuts**.
3. Under the **Window Management** category, click **Move between windows immediately**, then press the Backspace key to disable the shortcut.
4. Click **Close**.
5. Close the Control Center.

11.4 Installing Virtualized NetWare

This section provides the instructions for installing NetWare 6.5 SP8 as a guest OS.

- Section 11.4.1, “Preparing the Installation Media,” on page 204
- Section 11.4.2, “Creating a Xen Virtual Machine and Installing a NetWare VM Guest Server,” on page 204

11.4.1 Preparing the Installation Media

You must use the DVD installation files to install a NetWare VM guest on a Xen VM host server. (Xen on SLES 11 doesn’t support DVD swapping.)

The installation media must appear as a local disk to the virtual machine, but it can be physically located in either of the following locations:

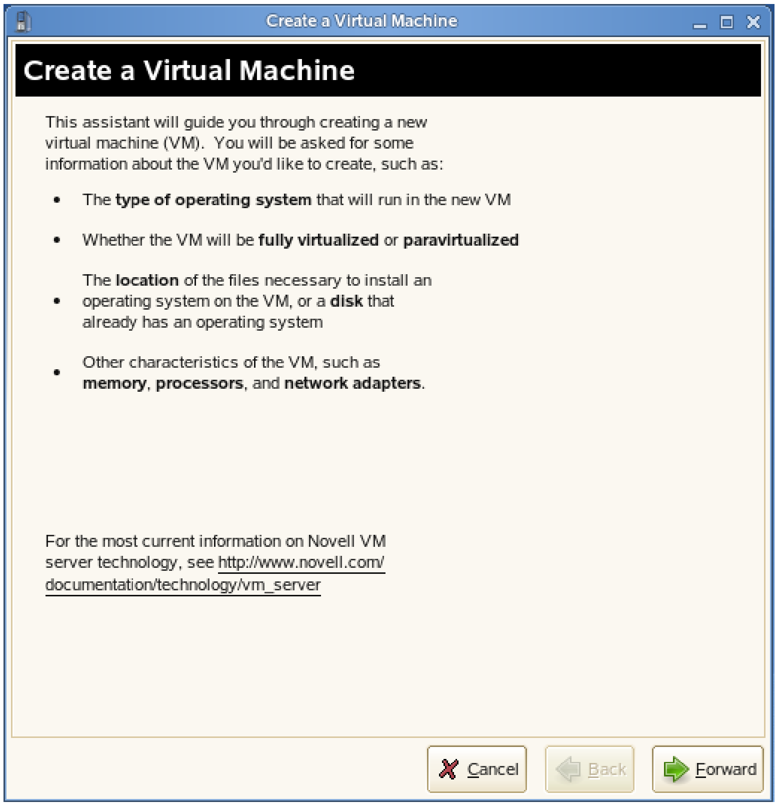
- On a DVD in the host’s physical DVD reader.
- As the DVD ISO image file copied to the Xen VM host server desktop.

The following steps are for downloading to the VM host server’s desktop and can be adapted as necessary for the other locations listed above.

1. Use the Firefox browser on the VM host server to access the Novell NetWare 6.5 SP8 Download page (http://download.novell.com/Download?buildid=dpIR3H1ymhk~) and download the `NW65SP8_OVL_DVD.iso` file to the server’s desktop (or another location of your choosing).
2. After the file downloads, continue with Section 11.4.2, “Creating a Xen Virtual Machine and Installing a NetWare VM Guest Server,” on page 204.

11.4.2 Creating a Xen Virtual Machine and Installing a NetWare VM Guest Server

1. Open YaST, then click **Virtualization** > **Create Virtual Machines**.



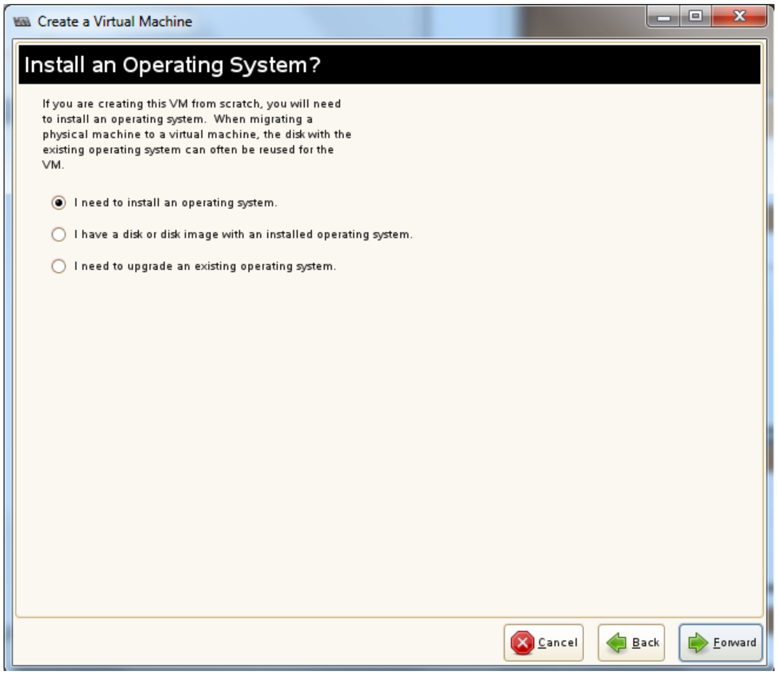
Create a Virtual Machine

This assistant will guide you through creating a new virtual machine (VM). You will be asked for some information about the VM you'd like to create, such as:

- The **type of operating system** that will run in the new VM
- Whether the VM will be **fully virtualized** or **paravirtualized**
- The **location** of the files necessary to install an operating system on the VM, or a **disk** that already has an operating system
- Other characteristics of the VM, such as **memory**, **processors**, and **network adapters**.

For the most current information on Novell VM server technology, see http://www.novell.com/documentation/technology/vm_server

2 Read the Create a Virtual Machine welcome page, then click **Forward**.



Install an Operating System?

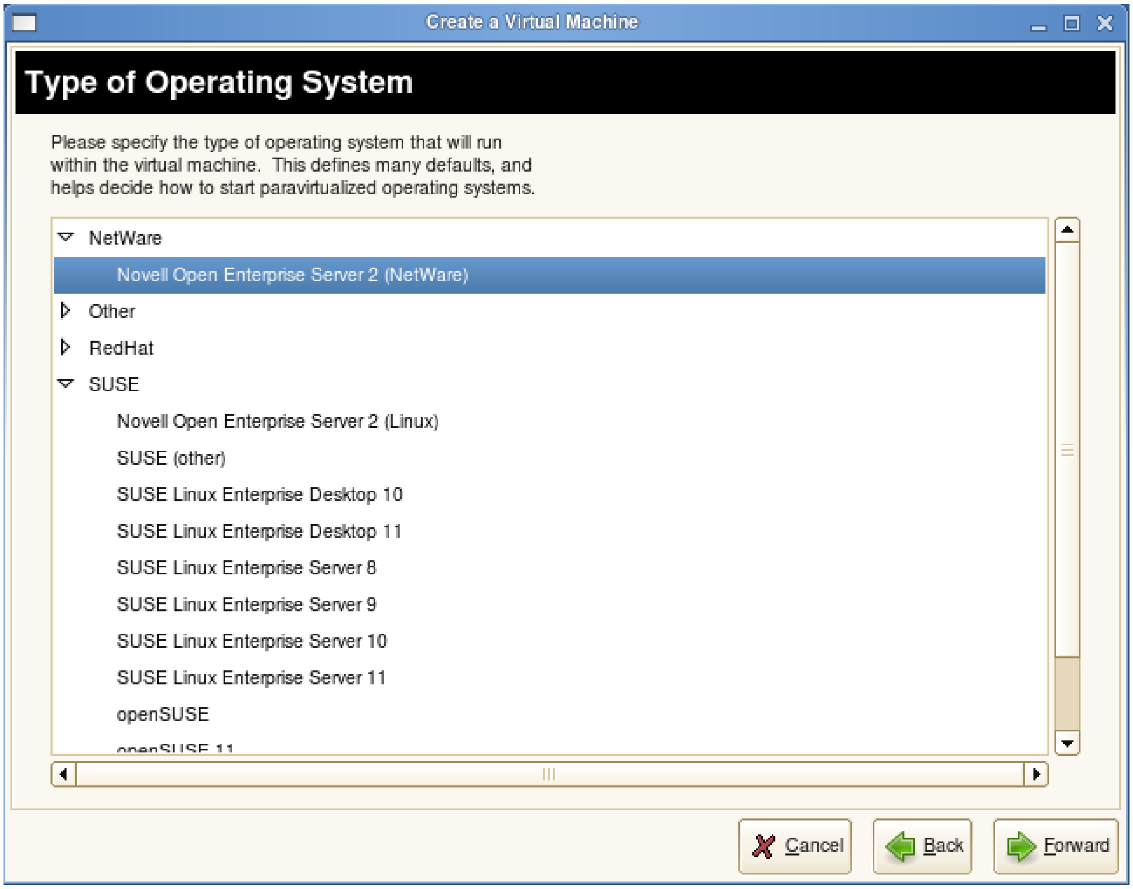
If you are creating this VM from scratch, you will need to install an operating system. When migrating a physical machine to a virtual machine, the disk with the existing operating system can often be reused for the VM.

● I need to install an operating system.

○ I have a disk or disk image with an installed operating system.

○ I need to upgrade an existing operating system.

3 Select **I need to install an operating system**, then click **Forward**.



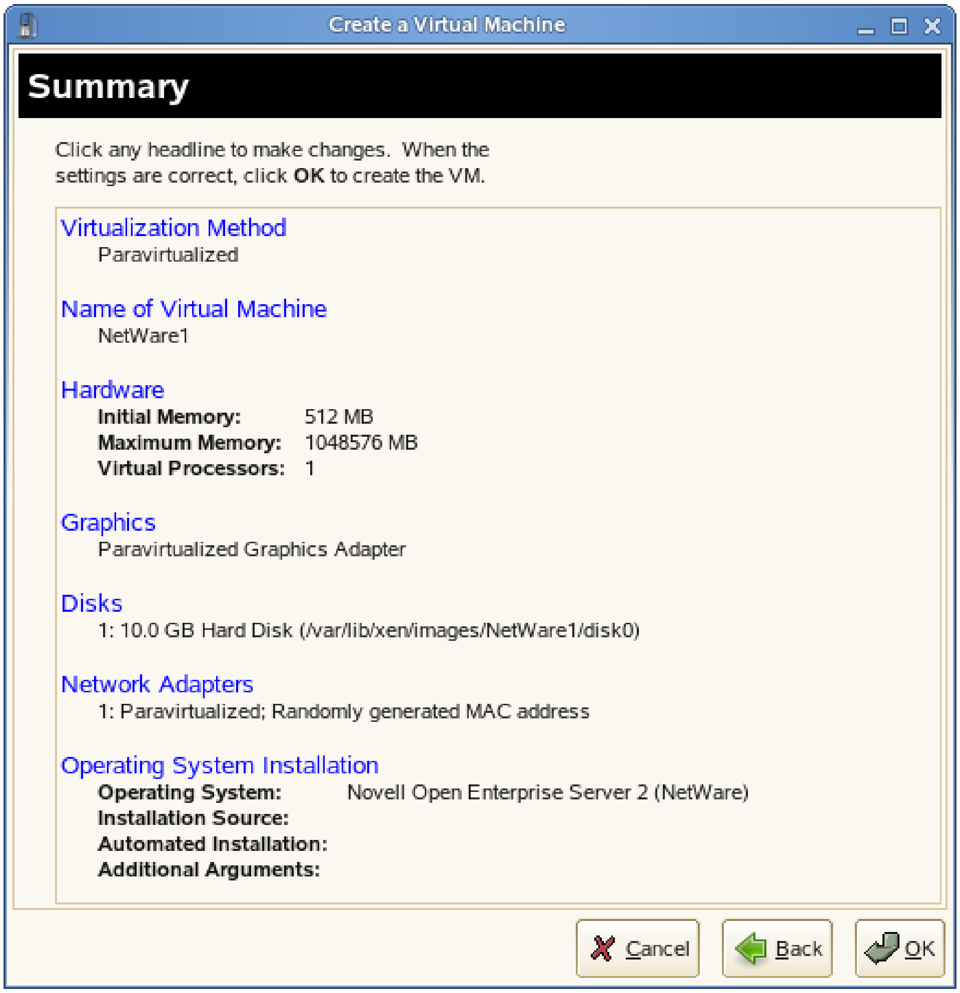
Type of Operating System

Please specify the type of operating system that will run within the virtual machine. This defines many defaults, and helps decide how to start paravirtualized operating systems.

- NetWare
  - Novell Open Enterprise Server 2 (NetWare)
- Other
- RedHat
- SUSE
  - Novell Open Enterprise Server 2 (Linux)
  - SUSE (other)
  - SUSE Linux Enterprise Desktop 10
  - SUSE Linux Enterprise Desktop 11
  - SUSE Linux Enterprise Server 8
  - SUSE Linux Enterprise Server 9
  - SUSE Linux Enterprise Server 10
  - SUSE Linux Enterprise Server 11
  - openSUSE
  - openSUSE 11

4 Click the triangle next to **NetWare**, select **Novell Open Enterprise Server 2 (NetWare)**, then click **Forward**.

The Summary page appears, showing the settings to be used for the virtual machine.



Summary

Click any headline to make changes. When the settings are correct, click **OK** to create the VM.

Virtualization Method
Paravirtualized

Name of Virtual Machine
NetWare1

Hardware

Initial Memory: 512 MB
Maximum Memory: 1048576 MB
Virtual Processors: 1

Graphics
Paravirtualized Graphics Adapter

Disks
1: 10.0 GB Hard Disk (/var/lib/xen/images/NetWare1/disk0)

Network Adapters
1: Paravirtualized; Randomly generated MAC address

Operating System Installation

Operating System: Novell Open Enterprise Server 2 (NetWare)
Installation Source:
Automated Installation:
Additional Arguments:

5 Click **Name of Virtual Machine**.

Specify the name that you want displayed for this virtual machine in the Virtual Machine Manager.

For example, you might specify *hostname*_vm, where *hostname* is the host name of the server you are installing.

6 Click **Hardware**.

Change the initial memory setting to at least 1024 MB and the maximum setting to as much as 8 GB, depending on the RAM available on your host server.

Add additional virtual processors if desired.

7 Click **Disks**.

The Virtual Disks dialog box lets you create one or more virtual disks that the NetWare 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 NetWare install allocates 500 MB for a DOS partition and 4 GB for the `sys:` volume. The default disk size of 10 GB leaves about 5.5 GB for other partitions.

7a Specify the hard disk space you want to be available to the virtual machine.

7b Click **Apply**.

7c To create additional virtual disks, click the Harddisk icon in the Disks wizard.

8 If you want to change the location of the NetWare VM’s first virtual hard drive, select the default **Hard Disk** and click **Edit**. Then modify the path in the **Server** field to where you want the virtual disk located.

Make sure that you specify enough physical disk space on the host server’s hard drive and partition to accommodate the maximum size of the virtual disk.

9 If you want optimal performance, deselect the sparse file option. This creates a blank file of the selected size when you start the virtual machine installation.

10 Click **OK**.

11 If you are installing from a mounted DVD, click **DVD**, browse to `/dev/cdrom` or `/dev/dvd`, then click **Open > OK > Apply**.

or

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

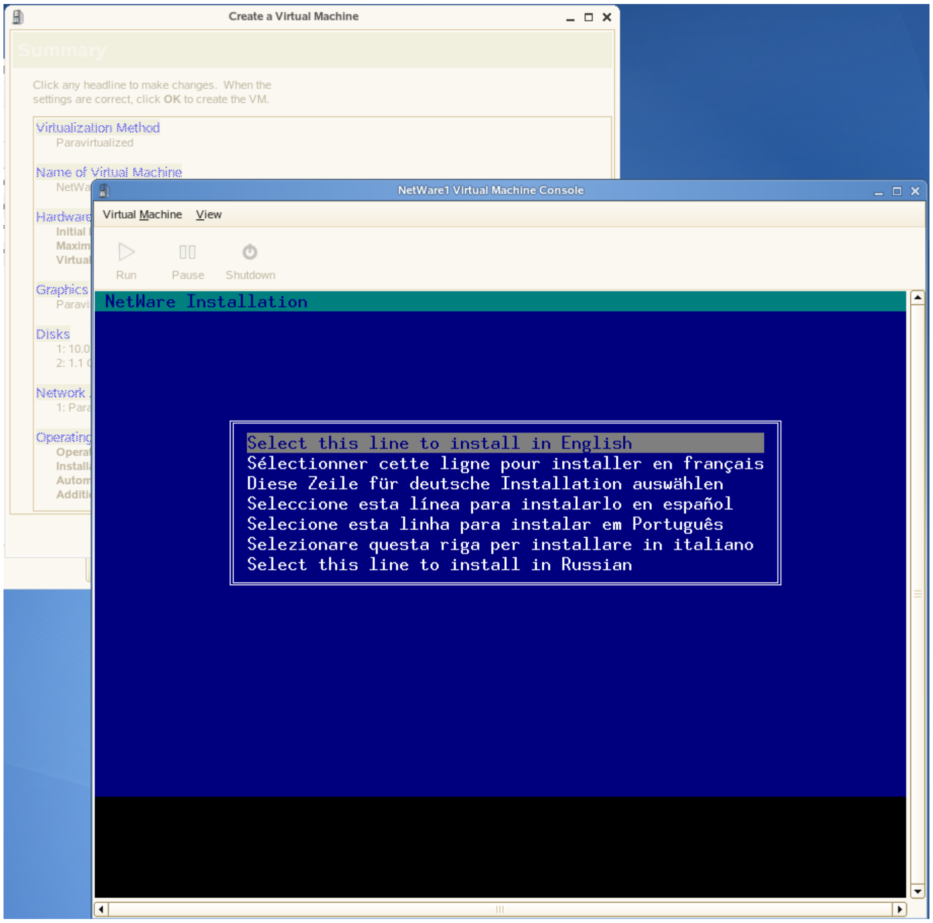
12 If you want multiple virtual network adapters, click **Network Adapters**.

Create virtual network adapters for the server.

The default setting is a single paravirtualized network adapter.

13 When you have the virtual machine settings the way you want them, click **OK** to proceed with the creation of the virtual machine and the installation of the virtual NetWare server.

A VNC viewer window appears, displaying the progress of the NetWare install program.



```
NetWare Installation

Select this line to install in English
Sélectionner cette ligne pour installer en français
Diese Zeile für deutsche Installation auswählen
Seleccione esta línea para instalarlo en español
Selecione esta linha para instalar em Português
Selezionare questa riga per installare in italiano
Select this line to install in Russian
```

14 Do the following:

14a Click inside the installation window to set the mouse pointer.

The mouse is not used on the first few screens, but you must set it now. Otherwise, the mouse and the keyboard might not work as expected when the GUI pages appear.

14b Enter all of the installation information as you would for a physical NetWare installation.

IMPORTANT: Do not close the VNC viewer window while the NetWare install program is running. Doing so prevents the installation from finishing properly.

11.5 Managing NetWare on a Virtual Machine

Virtualized NetWare is managed in the same way as if it were running on a physical machine. For information about managing your NetWare server, see the *NW 6.5 SP8: Server Operating System Administration Guide*. For additional information about managing NetWare servers in a virtualized environment, see “Running NetWare in a Virtualized Environment” in the “NW 6.5 SP8: Server Memory Administration Guide”.

- Section 11.5.1, “Using the Virtual Machine Manager,” on page 210
- Section 11.5.2, “Using the Command Line,” on page 210

11.5.1 Using the Virtual Machine Manager

Managing a NetWare virtual machine is simplified by using the Virtual Machine Manager utility, which is installed by default when you install the Xen virtualization software.

To start the Virtual Machine Manager, open a terminal prompt and enter `virt-manager`.

For more information, see "*Managing a Virtualization Environment* (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/cha_xen_virtualization_manage.html)" in the *Virtualization with Xen* guide (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/book_virtualization_xen.html).

11.5.2 Using the Command Line

Many NetWare administrators prefer to manage the server through the command line. If you want to use the command line, you should be aware of the following issues:

- "Terminal Size" on page 210
- "NetWare Debugger" on page 210
- "VNC Viewer" on page 210
- "The xm Commands" on page 210

Terminal Size

The terminal window might display only 80x24 characters. If you don't want to scroll to the command line, you need to resize the terminal.

NetWare Debugger

If pressing Alt+Shift+Shift+Esc doesn't launch the debugger, you can enter `386debug` at the command line.

VNC Viewer

In the VNC Viewer, pressing F8 displays a pop-up utility menu. Press F8 twice to pass single F8 to the remote side.

The xm Commands

- You can also manage the NetWare virtual machine, and all other virtual machines running on the Xen hypervisor, by using the `xm` command line tools. For more information, see "The xm Command (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/sec_xen_virtualization_xm.html)" in the *Virtualization with Xen* guide (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/book_virtualization_xen.html).
- To make a break in NetWare from a terminal, enter `xm sysrq` *`x c`*, where *x* is the domain ID and *c* is any keyboard character.

11.6 If VM Manager Doesn't Launch on a Xen VM Host Server

If the option to launch the VM Manager for installing a NetWare guest is not available, the most likely cause is that the Xen kernel is not running on the Xen VM host server. See *The Boot Loader Program* (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/sec_xen_config_bootloader.html) in the *Virtualization with Xen* guide (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/book_virtualization_xen.html).

12 Switching to SHA-2 SSL Certificates

Major browser vendors are taking steps to phase out SHA-1 signed certificates. OES certificates signed with SHA-1 should be replaced with certificate signed with SHA-2 to avoid warning messages to be displayed in browsers.

- Section 12.1, "Configuring SHA-2 Certificate," on page 213
- Section 12.2, "Verifying the Certificates with SHA-2 Signature," on page 214

12.1 Configuring SHA-2 Certificate

- Section 12.1.1, "CA Server," on page 213
- Section 12.1.2, "Other Servers," on page 213
- Section 12.1.3, "Servers Running on eDirectory 8.8.7 or OES 11 SP1 or Earlier," on page 214

12.1.1 CA Server

1 Apply patch on the OES server where CA is hosted in the tree.

2 Restart the eDirectory service.

```
rcndsd restart
```

3 Delete the existing CA in tree and create a new CA with SHA-2 signing algorithm. For more information, see the TID on Configuring eDirectory to mint certificates with a SHA-2 signature (7016877).

4 Restart the eDirectory service.

Run the following command to recreate the eDirectory server certificates with SHA-2 algorithm.

```
rcndsd restart
```

5 Reboot the server.

IMPORTANT: Ensure that eDirectory service is restarted before rebooting the server.

All the OES services will now use the new eDirectory certificates.

12.1.2 Other Servers

1 Apply patch on the OES server.

2 Restart the eDirectory service.

Run the following command to recreate the eDirectory server certificates with SHA-2 algorithm.

```
rcndsd restart
```

3 Reboot the server.

IMPORTANT: Ensure that eDirectory service is restarted before rebooting the server.

All the OES services will now use the new eDirectory certificates.

12.1.3 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 OES 11 SP3 server in the tree.

12.2 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 /etc/opt/novell/certs/SSCert.der -inform der -text -noout
  ```

13 Disabling OES 11 Services

Although you can uninstall Novell Open Enterprise Server 11 (OES) service RPMs through YaST, we do not recommend it because so many modules have interdependencies. Uninstalling services can leave the server in an undesirable state. Instead, we recommend disabling the service.

1. Log in as `root` and start YaST.
2. Click **System** > **System Services (Runlevel)**.
3. Select **Expert Mode**.
4. Select the *applicable_service_name,* then click **Set/Reset** > **Disable the service**.
5. Repeat Step 4 for each service you want to disable.
6. Click **Finish** to exit the YaST Runlevel tool.

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 Novell iManager 2.7.4 Administration Guide.

14 Reconfiguring eDirectory and OES Services

If the eDirectory database becomes corrupt, you need to reconfigure eDirectory and the OES services. This section outlines the steps to be performed, depending on the role of the server with regard to your eDirectory tree.

If a backup of the eDirectory database is not available, you can contact Novell Support or perform the following procedures:

- Section 14.1, “Cleaning Up the eDirectory Server,” on page 217
- Section 14.2, “Reconfiguring the eDirectory Server through YaST,” on page 219
- Section 14.3, “Reconfiguring OES Services,” on page 219
- Section 14.4, “Re-configuring iManager,” on page 223

14.1 Cleaning Up the eDirectory Server

IMPORTANT: The instructions in this section have been tested and approved, but it is impossible to anticipate all customer scenarios and the complications that might arise in them.Therefore, we urge that you only proceed when you have problems with eDirectory that aren't resolved by performing regular eDirectory maintenance tasks, or when Novell Technical Support recommends that you do.

- Section 14.1.1, “Before You Clean Up,” on page 217
- Section 14.1.2, “Reconfiguring the Replica Server,” on page 218
- Section 14.1.3, “Reconfiguring the CA Server,” on page 218
- Section 14.1.4, “Cleaning Up eDirectory,” on page 218

14.1.1 Before You Clean Up

- Before the cleanup, make a note of the following eDirectory configuration parameters:
  - eDirectory tree name
  - Replica server IP
  - eDirectory admin context
  - eDirectory server context
  - IP address of servers running NTP and SLP services
- If you are cleaning the master replica server, ensure that you make a read-write replica as a master. For more information, see Section 14.1.2, “Reconfiguring the Replica Server,” on page 218.
- If the reconfiguration is performed on a CA server, transfer the role of CA server to another server or create a new CA server. If you don’t do this, the CA does not work. For more information, see Section 14.1.3, “Reconfiguring the CA Server,” on page 218.

14.1.2 Reconfiguring the Replica Server

1 If the corrupted server is a master replica, make any other replica into the master replica.

For more information, refer to Managing Partitions and Replicas (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a2iiiik.html) in the *NetIQ eDirectory 8.8 Administration Guide*.

2 Clean up the replica server.

For more information, see Section 14.1.4, “Cleaning Up eDirectory,” on page 218.

3 Reconfigure the replica server.

For more information, see Section 14.2, “Reconfiguring the eDirectory Server through YaST,” on page 219.

4 On successful reconfiguration of the replica server, continue with Section 14.3, “Reconfiguring OES Services,” on page 219.

14.1.3 Reconfiguring the CA Server

1 If the corrupted server is a CA server, transfer the CA server role to another server or create a new CA server.

For more information, refer to Moving the Organizational CA to a Different Server (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) in the *Novell Certificate Server 3.3.2 Administration Guide*.

2 Clean up the server.

For more information, see Section 14.1.4, “Cleaning Up eDirectory,” on page 218.

3 Reconfigure the server.

For more information, see Section 14.2, “Reconfiguring the eDirectory Server through YaST,” on page 219.

4 After successfully reconfiguring the server, continue with Section 14.3, “Reconfiguring OES Services,” on page 219.

14.1.4 Cleaning Up eDirectory

1 Use iManager to delete all the objects from the eDirectory tree.

2 Stop the ndsd daemon:

```
rcndsd stop
```

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 Section 17.7.1, Cleaning Up the Replica Ring (http://www.novell.com/documentation/edir88/edir88/?page=/documentation//edir88/edir88/data/agm7hq7.html) in the *NetIQ eDirectory 8.8 Administration Guide*.

14.2 Reconfiguring the eDirectory Server through YaST

The eDirectory reconfiguration can be done on the Root partition Master replica server, a Read-Write replica server, a server without a replica, or the CA server.

1. Open YaST.
2. Click **Open Enterprise Server > OES Install and Configuration.**
3. On the Software Selection Page, click **Accept**.

   The status of eDirectory service is displayed as **Reconfigure is disabled.**
4. To reconfigure, click **disabled** to change the status to **enabled.**
5. Click **eDirectory** to access the configuration dialog box.
6. Provide all the eDirectory configuration information that was noted in Section 14.1.1, "Before You Clean Up," on page 217:
   - **6a** Verify the eDirectory tree name and click **Next.**
   - **6b** Specify the admin password and click **Next**.
   - **6c** Specify the server context and click **Next**.
   - **6d** Specify the IP address of the Network Time Protocol Server.
   - **6e** (Conditional) If SLP was configured earlier, select **Configure SLP to use an existing Directory Agent**, then click **Add.**
   - **6f** Specify the SLP DA server IP address and click **Add.**
   - **6g** Click **Next**.
7. In the NetIQ Modular Authentication Service (NMAS) window, click **Next**.
8. Verify the listed configuration information and click **Next**.

   eDirectory is configured and installation is successfully completed.
9. Click **Finish**.

14.3 Reconfiguring OES Services

After you have successfully configured eDirectory, some of the OES services are started by default, some services require a manual start, some services require the eDirectory objects to be re-created, and some services must be reconfigured.

***Table 14-1** Services*

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

- Section 14.3.1, “Re-creating eDirectory Objects,” on page 220
- Section 14.3.2, “Services Requiring Reconfiguration,” on page 221
- Section 14.3.3, “Manually Starting Services,” on page 222

14.3.1 Re-creating eDirectory Objects

- “Novell Storage Service” on page 220
- “NCP Server” on page 221

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 Quick Reference (http://www.novell.com/documentation/oes11/stor_nss_lx/?page=/documentation/oes11/stor_nss_lx/data/boswzl1.html) in the *NSS Administration Guide*.

1 Re-create the eDirectory object for each NSS pool:

1a Start NSSMU by entering the following command at the command prompt:

```
nssmu
```

1b Select **Pools** and press Enter to list all the NSS pools.

1c Select a pool that needs to be re-created and press F4.

1d Select **Yes** when you are prompted to delete and re-create an NDS pool object.

The selected NDS pool object is re-created.

1e Repeat from Step 1c for each NDS pool object that needs to be re-created.

2 Re-create the eDirectory object for each NSS volume:

2a In NSSMU, select **Volumes** and press Enter to list all the NSS volumes.

2b Select a volume and press F4.

2c Select **Yes** when you are prompted to delete and re-create the NDS volume object.

The selected volume object is re-created.

2d Repeat from Step 2b for each NDS volume object that needs to be re-created.

3 (Conditional) If the eDirectory object for _ADMIN volume exists, execute the following command:

```
rcadminfs restart
```

NCP Server

Use the NCP server console (NCPCON) utility to delete and re-create the eDirectory objects for the NCP volumes. For more information on the NCPCON utility, see NCP Server Console Utility (http://www.novell.com/documentation/oes11/file_ncp_lx/?page=/documentation/oes11/file_ncp_lx/data/ba2un44.html) in the *NCP Server for Linux Administration Guide.*

IMPORTANT: If restoration of the eDirectory database is not possible, simply delete the NCP server object.

1 Delete the eDirectory object of the NCP volume by entering the following command:

```
ncpcon remove volume SYS
```

2 Re-create the eDirectory object of the NCP volume by entering the following command:

```
ncpcon create volume SYS /usr/novell/sys
```

14.3.2 Services Requiring Reconfiguration

- "Novell DNS" on page 221
- "Novell CIFS" on page 222
- "Novell SLP" on page 222
- "NMAS" on page 222

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 219 for more information.

NMAS

The NMAS login method is selected during eDirectory reconfiguration. See Step 7 on page 219 for more information.

14.3.3 Manually Starting Services

Re-create the eDirectory objects of NCP and NSS volumes as directed in the Section 14.3.1, “Re-creating eDirectory Objects,” on page 220, before starting the following services manually:

Table 14-2 *Manually Restarting Services*

Service Name	Starting the Service
Novell AFP	`rcnovell-afptcpd start`
Novell Cluster Service (NCS)	`rcnovell-ncs start`

Archive and Version Service	`rcadminfs start`
	`rcnovell-ark start`

NetStorage	`rcnovell-xregd start`
	`rcnovell-xsrvd start`

QuickFinder	Generate the index again from QuickFinder Administration.
Samba	Start the Samba service through iManager
Novell DHCP	`rcnovell-dhcpd start`

Service Name	Starting the Service

iPrint	`rcnovell-ipsmd start`
	`rcnovell-idsd start`

iManager	After completing the OES installation, if iManager is installed without using YaST, Tomcat must be started manually.
	`/etc/init.d/novell-tomcat6 start`
	`rcapache2 restart`

NTP	`rcntpd restart`

14.4 Re-configuring iManager

In case iManager is not configured properly or there has been an interruption during iManager installation, use the following procedure to reconfigure iManager.

IMPORTANT: Before executing this reconfiguration procedure, ensure to backup all the custom tasks in iManager from `\var\opt\novell\imanager\nps\portal\modules\custom`. You can restore them after the reconfiguration. For more information on backing up and restoring the custom tasks, see Exporting Custom Tasks and Importing Custom Tasks under section Plug-In Studio of the Novell iManager 2.7.7 Administration Guide.

To reconfigure:

1. Ensure that the OES server is registered to NCC, and you have applied all the latest patches available in the patch channel using the zypper up command. For more information on patching using the zypper command, see Chapter 7, "Updating (Patching) an OES 11 SP3 Server," on page 165.
2. After patching, ensure that the following path exists along with all the iManager plugins that you want to install: `/var/opt/novell/iManager/nps/packages`.

   NOTE: The reconfiguration script installs only the iManager plug-ins that are available at `/var/opt/novell/iManager/nps/packages`.
3. Run the following command to reconfigure iManager `/var/opt/novell/iManager/iManagerReconfiguration.sh tomcat6`.

15 Security Considerations

This section includes issues that you should consider when installing and configuring a Novell Open Enterprise Server (OES) 11 Linux server.

- Section 15.1, "Access to the Server During an Installation or Upgrade," on page 225
- Section 15.2, "Remote Installations Through VNC," on page 225
- Section 15.3, "Improperly Configured LDAP Servers," on page 225

15.1 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.

15.2 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 11 SP4 Deployment Guide* (http://www.suse.com/documentation/sles11/book_sle_deployment/data/cha_deployment_remoteinst.html).

15.3 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 8.8 SP8 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 8.8 SP8 Administration Guide*.

16 Troubleshooting

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

16.1 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 Serer and Group objects
- Certificates (IP AG, SSL Certificate IP, DNS AG, and SSL Certificate DNS)

16.2 eDirectory User Password Screen Does Not Show Up During an Upgrade

When you upgrade an OES 2 server to OES 11 SP3, the eDirectory pattern will not be selected as part of the product listing and the eDirectory user password screen will not show up.

To resolve this issue follow any of these methods:

1. Before starting an upgrade, ensure to install the following packages in the OES 2 server:
   - nici64
   - novell-dclient-32bit
   - novell-nmas-libspmclnt-32bit
   - novell-NDSbase-32bit
   - novell-edirectory-tsands-32bit
2. During an upgrade, in the Installation Settings Screen, search and select the packages listed above and then proceed with the upgrade.
3. If you are upgrading using AutoYaST, ensure to add the packages listed above as part of the autoup.xml file. Add them to the <software> section and then proceed with the upgrade.

```
<software>
      <packages config:type="list">
            <package>novell-NDSbase-32bit</package>
            <package>novell-edirectory-tsands-32bit</package>
            <package>novell-nmas-libspmclnt-32bit</package>
            <package>nici64</package>
            <package>novell-dclient-32bit</package>
      </packages>
</software>
```

16.3 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.

16.4 iManager not Configured or Installed Properly

If iManager is not configured properly or there has been an interruption during iManager installation, see Section 14.4, “Re-configuring iManager,” on page 223 to reconfigure iManager.

16.5 eDirectory Restart Results in an Error Message on a Non-DSfW Server

On a non- DSfW Server, if you restart eDirectory, the following error message is received: “Method load failed: libxadnds.so.2: cannot open shared object file: No such file or directory.”

This is because three NMAS methods (IPCExternal, Kerberos, and Negotiate) fail to load on the server. These NMAS methods that are specific to DSfW are part of the `novell-xad-nmas-methods` rpm and depend on the libraries from the `novell-xad-framework` rpm. Since the `novell-xad-framework` rpm is part of the DSfW pattern and is installed only on a DSfW server, you receive this error message on a non-DSfW server.

If you receive this error message, you can ignore this message as these DSfW NMAS methods do not function in a non-DSfW server and do not impact any eDirectory functionality.

16.6 The DEFAULT SLP Scope Gets added to the slp.conf File During an Upgrade to OES 11 SP3

When you upgrade an OES server that is configured as an SLP DA to OES 11 SP3, 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 11 SP3 to future OES releases.

16.7 zlib-devel and zlib-devel-32bit Package Conflict During the Channel Upgrade to OES 11 SP3

The zlib-devel and zlib-devel-32bit package conflict occurs during the following upgrade path:

- Upgrading an OES 2 SP3 server that has C/C++ Compiler and Tools pattern installed to OES 11 SP2 using media upgrade.
- Upgrading the resultant OES 11 SP2 server to OES 11 SP3 using the channel upgrade.

Cause: These packages (zlib-devel and zlib-devel-32bit) are no longer available in the SLES 11 base.

Resolution: When you are prompted about the package conflict, uninstall them.

16.8 The change_proxy_pwd.sh Script Fails to Synchronize Password

Whenever the common proxy user password is not synchronized across CASA, 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 CASA. 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 CASA, 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 CASA 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.

16.9 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-SP3-Pool/sle-11-x86_64]]></media_url>
     <product>Open_Enterprise_Server</product>
     <product_dir></product_dir>
  </listentry>
</add_on_products>
```

16.10 The POODLE Security Vulnerability

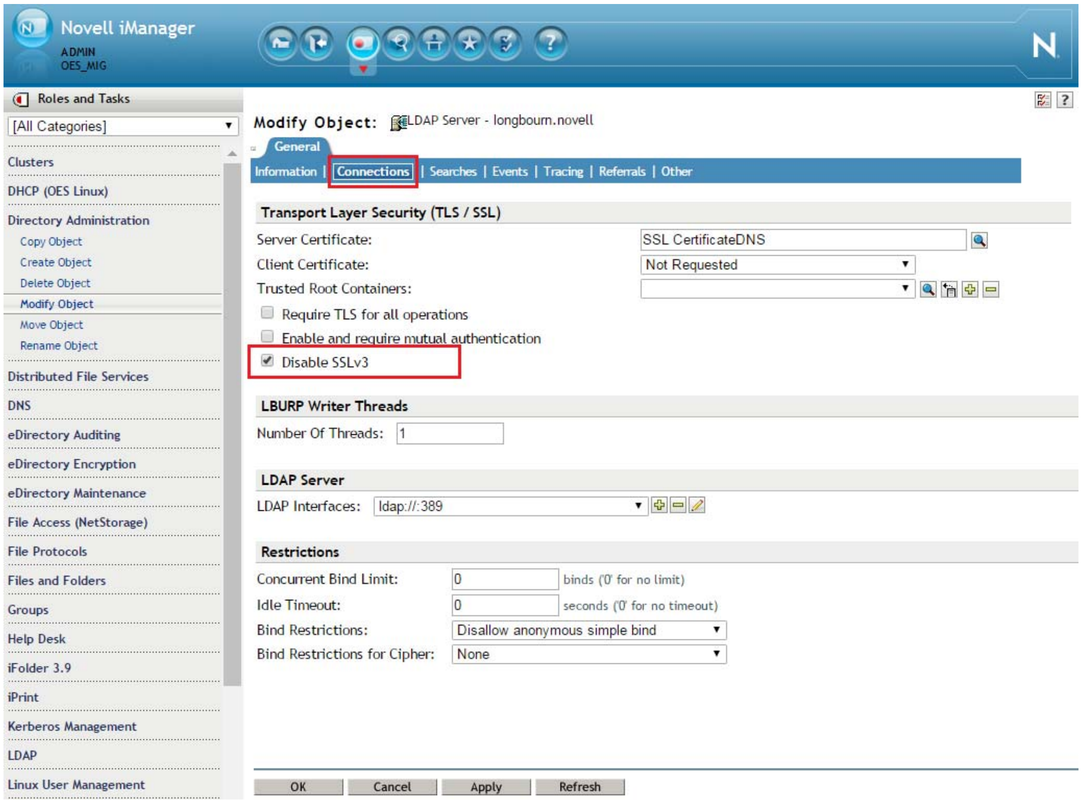
LDAPS in eDirectory allow SSLv3 for secure communication, and SSLv3 has been found to have protocol vulnerability as per CVE-2014-3566. Ensure that you disable SSLv3 to prevent POODLE security vulnerability.

SSLv3 can be disabled by any of the following methods:

- To disable SSLv3 through iManager, do the following:
  1. Log in to iManager as an administrator.
  2. In **Roles and Tasks** pane, click **Directory Administration** > **Modify Object**.

     The Modify Object page is displayed.
  3. Click 🔍 icon to select the LDAP server object and click OK.

     The Modify Object configuration page is displayed.



Modify Object: LDAP Server - longbourn.novell

Transport Layer Security (TLS / SSL)

Server Certificate: SSL CertificateDNS

Client Certificate: Not Requested

Trusted Root Containers:

☐ Require TLS for all operations

☐ Enable and require mutual authentication

☑ Disable SSLv3

LBURP Writer Threads

Number Of Threads: 1

LDAP Server

LDAP Interfaces: ldap://:389

Restrictions

Concurrent Bind Limit: 0 binds ('0' for no limit)

Idle Timeout: 0 seconds ('0' for no timeout)

Bind Restrictions: Disallow anonymous simple bind

Bind Restrictions for Cipher: None

  4. Go to **General** > **Connections** property tab.
  5. In Transport Layer Security (TLS/SSL) section, select **Disable SSLv3** option.
  6. Click Apply and then click OK.
- SSLv3 can also be disabled through LDAP. To disable SSLv3, set number 128 to the `ldapBindRestrictions` attribute on the LDAP server object. For example, if the current value is 49, replace the value with 128.

NOTE: This SSLv3 configuration should be done on each LDAP server object.

A OES 11 File and Data Locations

This section contains information about the general rules and conventions that Novell 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) 11 components follow Linux Standard Base (LSB) requirements regarding file location. Efforts to do this are detailed here.

- Section A.1, “General Rules,” on page 233
- Section A.2, “Exceptions,” on page 234

A.1 General Rules

Where possible, product design has followed these rules:

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

`/opt/novell/bin`	Executable files that are used by multiple products or are intended to be executed by an end user.
`/opt/novell/`*`product`*`/sbin`	Executable files that are used only by a product and are not executed by an end user.
`/opt/novell/lib`	Shared libraries that are used by multiple products and shared or static libraries that are part of an SDK.
`/opt/novell/include`	Header files for SDKs, typically in a product subdirectory.
`/opt/novell/lib64`	Contains 64-bit shared libraries.

- **/etc/opt/novell:** Generally contains host-specific configuration data.

  If a product has a single configuration file, it is named *`product or service`*`.conf`.

  If a product uses multiple configuration files, they are placed in a subdirectory named for the product or service.
- **/etc/opt/novell/*service_name*:** Contains various OES service configuration files.
- **/var/opt/novell:** Contains all variable data.

  Variable data (data that changes during normal run time operations) is stored in a product or service subdirectory.
- **/var/opt/novell/log:** Generally contains log files.

  If a product or service has a single log file, it is stored in a file with the product or service name.

  If a product or service has multiple log files, they are stored in a subdirectory named for the product or service.
- **/var/log:** Contains the log messages and the YaST logs.
- All files and directories that could not follow the above rules have the prefix *novell-* where possible.

A.2 Exceptions

Some files must reside in nonstandard locations for their products to function correctly. Two examples are init scripts, which must be in `/etc/init.d`, 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 11 SP4 AutoYaST (https://www.suse.com/documentation/sles11/singlehtml/book_autoyast/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 8.4, “Cloning an OES Server Post OES Installation and Configuration,” on page 185 section. All the passwords stored in the `autoinst.xml` file will be in clear text.

B.1 arkmanager

Attribute Name	Description
db_port	The MySQL database port number. Example: <db_port>5432</db_port>
db_username	The MySQL database user name. Example: <db_username>arkuser</db_username>

Attribute Name	Description
dbpassword	The MySQL database password. Example: <dbpassword>SAM23#$</dbpassword>

B.2 edirectory

Attribute Name	Description
casa_store	Always set this to 'yes' so that the proxy credentials are stored in CASA. Example: <casa_store>yes</casa_store>
cert_mutual	Set this to 'yes' when you want to implement the Certificate Mutual login method. It implements the Simple Authentication and Security Layer (SASL) EXTERNAL mechanism, which uses SSL certificates to provide client authentication to eDirectory through LDAP. Example: <cert_mutual>no</cert_mutual>
challenge_response	Set this to 'yes' when you want to enable the Challenge-Response login method. It works with the Identity Manager password self-service process. This method allows either an administrator or a user to define a password challenge question and a response, which are saved in the password policy. Then, when users forget their passwords, they can reset their own passwords by providing the correct response to the challenge question. Example: <challenge_response>yes</challenge_response>
create_server_object	Set this to 'Yes' when you want to create a DNS server object. Example: <create_server_object>yes</create_server_object>
dib_location	Specify the path of the nds databse. Example: <dib_location>/var/opt/novell/eDirectory/data/dib</dib_location>
digest_md5	Set this to 'yes' when you want to implement the the Digest MD5 login method. It implements the Simple Authentication and Security Layer (SASL) DIGEST-MD5 mechanism as a means of authenticating the user to eDirectory through LDAP. Example: <digest_md5>no</digest_md5>
domain_name	Specify the DSfW DNS domain name. The value of this tag and xad_domain_name tag should be same. Example: <domain_name>acme.com</domain_name>
existing_dns_ip	Specify the existing DNS server IP address. Example: <existing_dns_ip>192.168.1.1</existing_dns_ip>
group_context	Specify the DNS DHCP group object context. Example: <group_context>ou=OESSystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</group_context>

Attribute Name	Description
host_name	Specify the host name of the current server where the installation is being done. Example: <host_name>acme-208</host_name>
http_port	Specify the HTTP port of the eDirectory server where the installation is being done. Example: <http_port config:type="integer">8028</http_port>
https_port	Specify the HTTPS port of the current eDirectory server. Example: <https_port config:type="integer">8030</https_port>
install_secretstore	Set to 'yes' when you want to install the secret store. Example: <install_secretstore>yes</install_secretstore>
install_universalstore	Set to 'yes' when you want to install the universal store. Example: <install_universalstore>no</install_universalstore>
ldap_basedn	Specify the DNSs server's CN name. This is required only in case of DSfW server. Example: <ldap_basedn>ou=OESSystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</ldap_basedn>
ldap_server	Specify the IP address of the DNS LDAP server. Example: <ldap_server>192.168.1.1</ldap_server>
locator_context	Specify the DNS locator object context where the DNS servers or zones are present. Example: <locator_context>ou=OESSystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</locator_context>
migrate_option	Always set this to 'no' as the migrate NKDC realm to DSfW domain is discontinued. Example: <migrate_option>no</migrate_option>
nds	Set to this to 'yes' when you want to use the NDS login method that provides secure password challenge-response user authentication to eDirectory. Example: <nds>yes</nds>
ntp_server_list	Specify reliable NTP servers IP addresses. Example: <ntp_server_list config:type="list"> <listentry>192.168.1.5</listentry> </ntp_server_list>
overwrite_cert_files	Set this to 'yes' when you want eDirectory to automatically back up the currently installed certificate and key files and replace them with files created by the eDirectory Organizational CA (or Tree CA). Example: <overwrite_cert_files>yes</overwrite_cert_files>

Attribute Name	Description
replica_server	Specify the IP address of the master eDirectory server. Example: <replica_server>192.168.1.5</replica_server>
runtime_admin	Specify the common proxy user context of the DNS. Example: <runtime_admin>cn=OESCommonProxy_host1,ou=OESSystemObjects,dc=acme,dc=com</runtime_admin>
runtime_admin_password	Specify the common proxy DNS password. Example: <runtime_admin_password>SAM23#$</runtime_admin_password>
sasl_gssapi	Set this to 'yes' when you want to implement the SASL GSSAPI login method. It implements the Generic Security Services Application Program Interface (GSSAPI) authentication using the Simple Authentication and Security Layer (SASL) that enables users to authenticate to eDirectory through LDAP using a Kerberos ticket. Example: <sasl_gssapi>no</sasl_gssapi>
server_context	Specify the eDirectory server context where there eDirectory server object needs to be created. Example: <server_context>ou=wdc,o=acme</server_context>
server_object	Specify the eDirectory server object name that has the object name and context. Example: <server_object>cn=DNS_edir-acme-208,ou=OESSystemObjects,dc=labs,dc=wdc,dc=acme,dc=com</server_object>
simple_password	Set this to 'yes' when you want to implement the Simple Password NMAS login method. It provides password authentication to eDirectory. The Simple Password is a more flexible but less secure alternative to the NDS password. Simple Passwords are stored in a secret store on the user object. Example: <simple_password>no</simple_password>
slp_backup	Set this to 'yes' when you want the SLP server to periodically back up all registrations. This works only when the server is configured as a DA (Directory Agent). Example: <slp_backup>yes</slp_backup>
slp_backup_interval	Specify the SLP backup time in seconds. The default is (900 seconds or 15 minutes). If the server is configured as Director Agent, this value will be used. Example: <slp_backup_interval>900</slp_backup_interval>
slp_da	Specify the list of IP addresses of the SLP Directory Agents. Example: <slp_da config:type="list"> <listentry>198.162.1.1</listentry> </slp_da>

Attribute Name	Description
slp_dasync	Set this to 'yes' when you want to enable SLPD to sync service registration between SLP Das on startup. If the server is configured as Director Agent, this value be used. Example: <slp_dasync>no</slp_dasync>
Slp_mode	Specify the SLP mode to multicast, da, or da_server. By default, it is set to multicast. Example: <slp_mode>da</slp_mode>
slp_scopes	This is a comma delimited list of strings indicating the only scopes a UA or SA is allowed when making requests or registering or the scopes a DA must support. The default value is DEFAULT. Example: <slp_scopes>DEFAULT</slp_scopes>
tls_for_simple_binds	Set this to 'yes' when you require TLS for SIMPle binds with passwords. Example: <tls_for_simple_binds>yes</tls_for_simple_binds>
tree_type	Specify the type of eDirectory tree: new or existing. Example: <tree_type>new</tree_type>
use_secure_port	Set this to 'yes' when you want the DNS to use the secure port for communication in an DSfW environment. Example: <use_secure_port>yes</use_secure_port>
xad_admin_password	Specify the DSfW domain administrator password. Example: <xad_admin_password>SAM23#$</xad_admin_password>
xad_config_dns	Set this to 'yes' when you want to configure this domain controller also as a DNS server. Example: <xad_config_dns>yes</xad_config_dns>
xad_convert_existing_container	Set this to 'yes' for name mapped installations. In named mapped installations, the DSfW domain is mapped to an already existing eDirectory partition in the eDirectory tree. Example: <xad_convert_existing_container>no</xad_convert_existing_container>
xad_domain_name	Specify the DSfW DNS domain name. The value of this tag and domain_name tag should be same. Example: <xad_domain_name>acme.com</xad_domain_name>
xad_domain_type	Specify the DSfW domain type: forest, domain or controller. ◆ Forest: Use it for the first domain in the DSfW forest. ◆ Domain: Use it for the subsequent child domain(s) in the DSfW forest. ◆ Controller: Use it for subsequent domain controller(s) for any DSfW domain in the DSfW forest. Exmple: <xad_domain_type>forest</xad_domain_type>

Attribute Name	Description
xad_existing_container	Specify the eDirectory partition that the DSfW domain is being mapped to. This is effective only when the xad_convert_existing_container tag is set to 'yes'. Example: <xad_existing_container>ou=OESSystemObjects, o=acme</xad_existing_container>
xad_forest_root	Specify the forest root domain name in the DSfW forest. Example: <xad_forest_root>acme.com</xad_forest_root>
xad_ldap_admin_context	Specify the eDirectory tree admin context. In a name-mapped installation, for all the modes of DSfW installation, this tag will point to the (existing) eDirectory tree's tree administrator. Example: cn=admin,ou=admins,o=acme. <xad_ldap_admin_context>cn=admin,ou=admins,o=acme</xad_ldap_admin_context> In a non-name mapped installation, the forest root domain administrator is also the eDirectory tree administrator. For all the modes of installation, this tag will point to the forest root domain administrator. For example, for the forest root domain acme.com, the default forest domain administrator will be <xad_ldap_admin_context>cn=administrator,cn=users,dc=acme,dc=com</xad_ldap_admin_context> For example, for the child domain sales.example.com, the default forest domain administrator will be <xad_ldap_admin_context>cn=administrator,cn=users,dc=example,dc=com</xad_ldap_admin_context>
xad_ldap_admin_password	Specify the eDirectory tree administrator password. Example: <xad_ldap_admin_password>SAM23#$</xad_ldap_admin_password>
xad_netbios	Specify the NetBIOS name of the DSfW domain. Example: <xad_netbios>EXAMPLE</xad_netbios>
xad_parent_domain	Specify the DSfW domain name of immediate DSfW parent domain. For example, for a domain sales.acme.com, the value will be, <xad_parent_domain>acme.com</xad_parent_domain>
xad_parent_domain_address	Specify the IP address of any one of the parent DSfW domain controller. For example, for the domain sales.acme.com, specify the IP address of the DSfW DC hosting the domain acme.com. <xad_parent_domain_address>192.168.1.1</xad_parent_domain_address>
xad_parent_domain_admin_context	Specify the immediate DSfW parent domain's administrator context. For example, for the domain sales.acme.com, <xad_parent_domain_address>cn=administrator,cn=users,dc=acme,dc=com</xad_parent_domain_address>
xad_parent_domain_admin_password	Specify the immediate DSfW parent domain's administrator password. Example: <xad_parent_domain_admin_password>SAM23#$</xad_parent_domain_admin_password>

Attribute Name	Description
xad_replicate_partitions	Always set this to 'yes'. This indicates that the replicas of the configuration and schema partitions will be added to the local domain controller. Example: <xad_replicate_partitions>yes</xad_replicate_partitions>
xad_retain_policies	Set this to 'yes' when you want to retain the existing NMAS universal password policies. Example: <xad_retain_policies>yes</xad_retain_policies> **NOTE:** If set to 'no', the DSfW configuration will override the existing password policies if any.
xad_service_configured	Always specify this value to 'yes' when you want to configure DSfW. Example: <xad_service_configured>yes</xad_service_configured>
xad_site_name	Specify the site name to which this domain controller should be associated with. Otherwise the default value should be 'Default-First-Site-Name'. Example: <xad_site_name>Default-First-Site-Name</xad_site_name>
xad_wins_server	Specify 'yes' when you want to configure the DSfW domain controller as WINS server. Example: <xad_wins_server></xad_wins_server> **NOTE:** Only one domain controller in a DSfW domain should be designated as WINS server.

B.3 imanager

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

B.4 iprint

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

B.5 ncpserver

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

B.6 ncs

NOTE: Novell Cluster Services does not support using autoyast to configure cluster nodes for new clusters or existing clusters. If you create an autoyast file from a cluster node, you must remove or comment out the NCS section before you use it to build or rebuild a server. After the server is up and running successfully, you can manually configure the node for clustering by using the OES Install and Configuration option in YaST2.

Attribute Name	Description
cluster_dn	Specify the Fully Distinguished Name (FDN) of the cluster in comma-delimited typeful format. Each of the intermediate containers must already exist. The cluster name must be unique in that path. Example: <cluster_dn>cn=clus134,ou=ncs,o=acme</cluster_dn>
cluster_ip	Specify the IP address (in IPv4 format) assigned to the cluster. This is the Master IP Address that provides a single point for cluster access, configuration, and management. The cluster IP address is bound to the master node and remains with the master node regardless of which server is the master. The cluster IP address is required to be on the same IP subnet as the nodes in the cluster. Example: <cluster_ip>192.168.1.1</cluster_ip>
config_type	Specify whether the node is being configured for a "New Cluster" or an "Existing Cluster". Example: <config_type>Existing Cluster</config_type>
ldap_servers	Specify the IP address (in IPv4 format, comma-delimited with no spaces) of one or more LDAP servers in the tree that you want NCS on this server to use for LDAP (eDirectory) communications. If you specify multiple LDAP servers, the local LDAP server is recommended to be the first IP address in the list. The LDAP servers must have a master replica or a Read/Write replica of eDirectory. Example: <ldap_servers>192.168.1.1,192.168.1.2</ldap_servers>

Attribute Name	Description
proxy_user	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: - 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. Example: <proxy_user>cn=OESCommonProxy_avalon,o=acme</proxy_user>
proxy_user_password	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. Example: <proxy_user_password>SAM23#$</proxy_user_password>
sbd_dev	If this is the first node in the cluster (that is, you specified a <config_type>New Cluster</config_type>), you typically specify a device to use for the SBD (split-brain detector). The device must already be initialized and marked as Shareable for clustering. Specify the leaf node name of the device, such as sdc. If the <sbd_dev> tag is not used, the SBD is not created. Example: <sbd_dev>sdc</sbd_dev>
sbd_dev2	If this is the first node in the cluster and you are creating an SBD, you can mirror the SBD by specifying a second device to use for the mirror. The device must already be initialized and marked as Shareable for clustering. Specify the leaf node name of the device, such as sdd. Example: <sbd_dev2>sdd</sbd_dev2>
sbd_size	Specify a size in MB to use for the SBD. A single size value applies to the SBD and its mirror (if specified). The size must be at least 8 MB. A minimum size of 20MB is recommended. To use the maximum size (all free space on the device), specify a size of "-1". If you mirror the SBD, the maximum size is limited to the lesser of the free space available on either device. Specify only a value with no units. Example: - For Default size: <sbd_size>8</sbd_size> - For 1024 MB (1 GB): <sbd_size>1024</sbd_size> - For Maximum size: <sbd_size>-1</sbd_size>
server_name	Specify the hostname of the server where you are configuring. Example: NCS.<server_name>avalon</server_name>

Attribute Name	Description
start	Specify whether to start NCS automatically after the configuration completes by specifying a start value of "Now". To start the NCS manually, specify "Later". Example: <start>Now</start>

B.7 netstorage

Attribute Name	Description
xtier_proxy_context	Specify the LDAP context for xtier proxy user. Example: <xtier_proxy_context>cn=OESCommonProxy_wdc34,o=acme</xtier_proxy_context>
xtier_proxy_password	Specify the password for xtier proxy user. Example: <xtier_proxy_password>SAM23#$</xtier_proxy_password>
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.8 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>

Attribute Name	Description
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.9 novell-cifs

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

Attribute Name	Description
use_casa_for_credentials	Set to 'yes' when you want to store the CIFS proxy user credentials in the local CASA store. Setting it to 'no' will store the credentials in an encrypted file locally. It is recommended to use CASA to store the CIFS Proxy user credentials. Example: <use_casa_for_credentials>yes</use_casa_for_credentials>
server_context	Specify the context of the local NCP server. Example: <server_context>ou=wdc,o=acme</server_context>
cifs_edir_contexts	Specify a list of CIFS User contexts that are searched when the CIFS user enters a user name for authentication. The server searches through each context in the list until it finds the user object. Example: <cifs_edir_contexts config:type="list"> <listentry>ou=wdc,o=acme</listentry> <listentry>ou=prv,o=acme</listentry> </cifs_edir_contexts>
subtree_search	Set this value to 'yes' when you want to enable the subtree search feature. Example: <subtree_search>no</subtree_search>
usercontext_rights	Set this to 'yes' for CIFS proxy user to grant search rights over user contexts. This is required for subtree search feature. Example: <usercontext_rights>yes</usercontext_rights>

B.10 novell-dhcp

Attribute Name	Description
certificate_authority	Specify the path of the LDAP CA file that contains the CA certificate. Example: <certificate_authority>/etc/opt/novell/certs/ca.pem</certificate_authority>
check_method	Specify what checks to perform on server certificate in a SSL/TLS session. Specify any one of the following options: ◆ Never: The server does not ask the client for a certificate. ◆ Allow: The server requests for a client certificate but if a certificate is not provided or a wrong certificate is provided, the session still proceeds normally. ◆ Try: The server requests for the certificate, if none is provided, the session proceeds normally. If a certificate is provided and it cannot be verified, the session is immediately terminated. ◆ Hard: The server requests for a certificate and a valid certificate must be provided, otherwise the session is immediately terminated. Example: <check_method>never</check_method>

Attribute Name	Description
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>
ldap_method	Specify static or dynamic. ◆ Static, when you do not want the DHCP server to query the LDAP server for host details. ◆ Dynamic, when you want the DHCP server to query for host details front the LDAP server for every request. Example: <ldap_method>static</ldap_method>
ldap_referrals	Set this to 'yes' when you want to enable LDAP referral. Example: <ldap_referrals>yes</ldap_referrals>
ldap_server	Specify the IP address of the LDAP server. Example: <ldap_server>192.168.1.2</ldap_server>
ldap_user	Specify the DHCP common proxy user context. Example: <ldap_user>cn=OESCommonProxy_host1,ou=OESSystemObjects,dc=sales,dc=wdc,dc=acme,dc=com</ldap_user>
ldap_user_password	Specify the common proxy DHCP password. Example: <ldap_user_password>SAM23#$</ldap_user_password>
locator_context	Specify the DHCP locator context. Example: <locator_context>ou=OESSystemObjects.dc=sales.dc=wdc.dc=acme.dc=com</locator_context>

Attribute Name	Description
server_context	Specify the DHCP server context. Example: <server_context>ou=OESSystemObjects.dc=sales.dc=wdc.dc=acme.dc=com</server_context>
server_object_name	Specify the DHCP server object name. Example: <server_object_name>DHCP_acme-208</server_object_name>
use_secure_port	Set it to 'yes' when you want to use a secure port for communicating with the LDAP server. Example: <use_secure_port>yes</use_secure_port>
use_secure_port_config	Set this to 'yes' when you want to use a secure port for DHCP configuration. Example: <use_secure_port_config>yes</use_secure_port_config>

B.11 novell-dns

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

Attribute Name	Description
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.12 novell-ifolder3

Attribute Name	Description
admin_alias	Specify the iFolder administrator name. Example: <admin_alias>/admin</admin_alias>
alternate_ldap_admin	Specify the admin user for the alternate LDAP source. Example: <alternate_ldap_admin>cn=admin,o=acme</alternate_ldap_admin>
alternate_ldap_admin_password	Specify the admin password for the alternate LDAP source. Example: <alternate_ldap_admin_password>SAM23#$</alternate_ldap_admin_password>
alternate_ldap_port	Specify the LDAP port for the alternate LDAP source. Example: <alternate_ldap_port>389</alternate_ldap_port>
alternate_secure_ldap_port	Specify the LDAP secure port for the alternate LDAP source. Example: <alternate_secure_ldap_port>636</alternate_secure_ldap_port>
data_path	Specify the iFolder data store path where all the iFolder related data is stored like database, managed iFolder data and unmanaged iFolder data. Example: <data_path>/var/simias/data</data_path>
do_server_config	Set it to 'yes' when you want to perform server configuration. Example: <do_server_config>yes</do_server_config>
do_webacc_config	Set it to 'yes' when you want to perform web access configuration. Example: <do_webacc_config>yes</do_webacc_config>

Attribute Name	Description
do_webadmin_config	Set it to 'yes' when you want to perform web administration configuration. Example: <do_webadmin_config>yes</do_webadmin_config>
groups_plugin	Set it to 'yes' when you want to enable LDAP groups plugin. Example: <groups_plugin>no</groups_plugin>
ifolder_admin_context	Specify the LDAP context where the iFolder administrator context is present. Example: <ifolder_admin_context>cn=admin,o=acme</ifolder_admin_context>
ifolder_admin_password	Specify the LDAP password for the admin context used as <ifolder_admin_context> tag. Example: <ifolder_admin_password>SAM23#$</ifolder_admin_password>
ifolder_port	Specify the HTTP port in which iFolder service has to listen. Example: <ifolder_port config:type="integer">443</ifolder_port>
ldap_proxy_user	Specify the LDAP proxy user DN used by iFolder for administrator related operations. It can be the OES common proxy as well. Example: <ldap_proxy_user>cn=OESCommonProxy_wdcwgpcminstall34,o=acme</ldap_proxy_user>
ldap_search_context	Specify a list of LDAP context that is used for the iFolder user authentication. Example: <ldap_search_context config:type="list"> <listentry>ou=wdc,o=acme</listentry> </ldap_search_context>
ldap_server	Specify the LDAP server IP address or DNS name used by the iFolder server. Example: <ldap_server>192.168.1.1</ldap_server>
master_address	Specify the iFolder Master server IP address or DNS name. Example: <master_address>192.168.1.1</master_address>
naming_attribute	Specify the LDAP attribute used as the unique identifier for login. Example: <naming_attribute>cn</naming_attribute>
private_url	Specify the URL or IP address used by the iFolder server or multi-server configuration. This is also used for Web Access/Admin to communicate. Example: <private_url>164.99.100.34</private_url>
proxy_password	Specify the LDAP proxy password. If OES common proxy is used, then specify the password of the common proxy. Example: <proxy_password>SAM23#$</proxy_password>

Attribute Name	Description
public_url	Specify the URL or IP address used by the iFolder clients to communicate with the iFolder server. Example: <public_url>164.99.100.34</public_url>
recovery_path	Specify the path in the server where the Encryption key recovery file is stored. Example: <recovery_path>/var/simias/data/simias</recovery_path>
server_name	Specify the name of the iFolder server. This can be the DNS name of the IP used or the local server name. Example: <server_name>acme-208</server_name>
slave_server	Set it to 'yes' when the configuration is for a slave server. Example: <slave_server>no</slave_server>
system_description	Specify a description that explains the current server's role. Example: <system_description>iFolder Enterprise System Sales Team</system_description>
system_name	Specify the name given to the iFolder System Domain. Example: <system_name>AcmeiFolder</system_name>
use_alternate_ldap_server	Set it to 'yes' if an alternate LDAP server is present. Example: <use_alternate_ldap_server>no</use_alternate_ldap_server>
use_ldap_ssl	Set it to 'yes' if LDAP communication is via SSL-enabled protocol. Example: <use_ldap_ssl>yes</use_ldap_ssl>
use_ssl	Represents if the iFolder communication is via SSL, non-ssl or both. Example: ◆ To use SSL: <use_ssl>SSL</use_ssl> ◆ To use non SSL: <use_ssl>NONSSL</use_ssl> ◆ To use both: <use_ssl>BOTH</use_ssl>
web_acc_connect_port	Specify the port for web Access. Example: <web_acc_connect_port config:type="integer">443</web_acc_connect_port>
web_acc_logout_url	Specify the URL to redirect when a Web Access log out occurs. So that the session, used by Access Manager enabled products, can be safely terminated. Example: <web_acc_logout_url></web_acc_logout_url>
web_acc_server_ip	Specify the IP or DNS used by the Web Access server. Example: <web_acc_server_ip>192.168.1.1</web_acc_server_ip>
web_acc_use_ssl	Set it to 'yes' if Web Access should use SSL for communication with the iFolder server. Example: <web_acc_use_ssl>yes</web_acc_use_ssl>

Attribute Name	Description
web_acc_use_ssl_browser	Set it to 'yes' if browser should use SSL for communication with the Web Access. Example: <web_acc_use_ssl_browser>yes</web_acc_use_ssl_browser>
web_admin_connect_port	Specify the port used by the Web Administration server. Example: <web_admin_connect_port config:type="integer">443</ web_admin_connect_port>
web_admin_logout_url	Specify the URL to redirect when a Web Administration log out occurs. So that the session, used by Access Manager enabled products, can be safely terminated. Example: <web_admin_logout_url></web_admin_logout_url>
web_admin_server_ip	Specify the IP or DNS used by the Web Admin server. Example: <web_admin_server_ip>164.99.100.34</web_admin_server_ip>
web_admin_use_ssl	Set it to 'yes' if Web Administration should use SSL for communication with the iFolder server. Example: <web_admin_use_ssl>yes</web_admin_use_ssl>
web_admin_use_ssl_browser	Set it to 'yes' if browser should use SSL for communication with the Web Administration. Example: <web_admin_use_ssl_browser>yes</ web_admin_use_ssl_browser>
web_alias	Specify the Apache alias used by the Web Access or Web Administration. Example: <web_alias>/ifolder</web_alias>

B.13 novell-lum

Attribute Name	Description
admin_group	Specify the admin group name. The admin group will be created if it does not exist and will be LUM-enabled. The admin user that is used to configure the LUM service will be added to this admin group and this group will be associated with the workstation object. Example: <admin_group>cn=admingroup,o=acme</admin_group>
alternate_ldap_servers_list1	Specify a list of the IP addresses of the local eDirectory servers that you are connecting to. Example: <alternate_ldap_servers_list1 config:type="list"> <listentry>192.168.1.1</listentry> <listentry>192.168.1.2</listentry> </alternate_ldap_servers_list1>

Attribute Name	Description
alternate_ldap_servers_list2	Specify one or more external LDAP servers. Ensure to specify the IP address of a valid LDAP server that is up and running. Example: <alternate_ldap_servers_list2 config:type="list"> <listentry>192.168.1.3</listentry> <listentry>192.168.1.4</listentry> </alternate_ldap_servers_list2>
ldap_server	Specify the IP address of the LDAP server. Example: <ldap_server>164.99.100.38</ldap_server>
lum_enabled_services	If you want the LUM-enabled users to accees the following services, set the value of those tags to 'yes': FTP, GDM, Gnome Screensaver, Gnomesu pam, Login, SFCB, SSHD and SU. Example: <lum_enabled_services> <ftp>no</ftp> <gdm>no</gdm> <gnome-screensaver>no</gnome-screensaver> <gnomesu-pam>no</gnomesu-pam> <login>no</login> <sfcb>yes</sfcb> <sshd>no</sshd> <su>no</su> </lum_enabled_services>
partition_root	Specify the context where UNIX Config Object will be created. Example: <partition_root>o=acme</partition_root>
proxy_user	Specify the LUM proxy user FQDN, in LDAP format, used for searching LUM users in eDirectory at login time. Example: <proxy_user>cn=ldapsproxy,o=acme</proxy_user> If you are using common proxy for LUM, mention the user FQDN of the common proxy as shown below. <proxy_user>cn=OESCommonProxy_localhostname,o=acme</proxy_user>
proxy_user_password	Specify the password for the LUM proxy user. Example: <proxy_user_password>SAM23#$</proxy_user_password>
restrict_access	Set it to 'yes' if you want to restrict read and write access for users other than the owners of the home directories. Example: <restrict_access>yes</restrict_access>

Attribute Name	Description
ws_context	Specify the workstation context. Computers running Linux User Management (LUM) are represented by Unix Workstation objects in eDirectory. The object holds the set of properties and information associated with the target computer, such as the target workstation name or a list of eDirectory groups that have access to the target workstation. Example: <ws_context>o=novell</ws_context>

B.14 novell-quickfinder

Attribute Name	Description
lum_enable	Set this to 'yes' if the admin user is LUM-enabled. If LUM-enabled, then the user should be an eDirectory user, else it will be a local user on the server. Example: <lum_enable>yes</lum_enable>
qf_user_name	Specify the QuickFinder user name context. Example: <qf_user_name>cn=admin,o=acme</qf_user_name>
qf_user_password	Specify the QuickFinder user password. Example: <qf_user_password>SAM23#$</qf_user_password>
shadow_access	Set this to 'yes' if you want to enabled shadow access. QuickFinder uses the Pluggable Authentication Modules (PAM) to authenticate users. Because QuickFinder is run as a servlet under Tomcat, it has the same rights to the system as the Tomcat user (wwwrun). In order for QuickFinder to authenticate, the wwwrun user must be added to the shadow group which gives it read rights to the shadow file. If you do not want the wwwrun user added to the shadow group, then authentication to QuickFinder Manager and rights-based searches will be turned off. Example: <shadow_access>yes</shadow_access>

B.15 novell-samba

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

Attribute Name	Description
ldap_server	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. Example:<ldap_server>192.168.1.1</ldap_server>

Attribute Name	Description
netbios_name	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. Example: <netbios_name>avalon-W</netbios_name>
proxy_user_context proxy_user_is_new proxy_user_password	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. ◆ 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. Example (new user): ◆ <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>
user_context	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. Example: <user_context>cn=Users.dc=labs.dc=wdc.dc=acme.dc=com</user_context>

B.16 nss

Attribute Name	Description
ldap_server	Specify the IP address of the LDAP server. Example: <ldap_server>192.168.1.34</ldap_server>
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.17 oes-ldap

Attribute Name	Description
admin_context	Specify the LDAP Server Administrator context. Example: <admin_context>cn=admin,o=acme</admin_context>
admin_password	Specify the LDAP Server server Administrator password. Example: <admin_password>SAM23#$</admin_password>
ldap_servers	Specify the details of the list of LDAP servers in a particular tree. ◆ ip_address: Specify the IP address of the LDAP server. ◆ ldap_port: Specify the LDAP non-secure port number. ◆ ldaps_port: Specify the LDAP secure port number. Example: <ldap_servers config:type="list"> <listentry> <ip_address>164.99.100.38</ip_address> <ldap_port config:type="integer">389</ldap_port> <ldaps_port config:type="integer">636</ldaps_port> </listentry> </ldap_servers>
proxy_context	Specify the FQDN of the default common proxy user. Example: <proxy_context>cn=OESCommonProxy_wdcsales34,o=acme</proxy_context>
proxy_password	Specify the common proxy user password. Example: <proxy_password>SAM23#$</proxy_password>

Attribute Name	Description
tree_name	Specify the eDirectory tree name. Example: <tree_name>sales_wdc_acme</tree_name>
use_common_proxy	Set it to 'yes' when you want to use the default common proxy. Example: <use_common_proxy>yes</use_common_proxy>
xad_tree_admin_context	Specify domain tree admin FQDN context. Example: <xad_tree_admin_context></xad_tree_admin_context>
xad_tree_admin_password	Specify domain tree admin password. Example: <xad_tree_admin_password>SAM23#$</xad_tree_admin_password>

B.18 sms

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

C Documentation Updates

This section summarizes the changes made to this guide since the initial release of Novell Open Enterprise Server 11.

July 2016 (OES 11 SP3)

Includes document updates to new features as mentioned in Section 1.1, "What's New (OES 11 SP3)," on page 11.

January 2016 (OES 11 SP2)

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. This patch (eDirectory 8.8 SP8 Patch 6 Hot Patch 1) contains bug fixes that enables the servers to easily switch to SHA-2 signed certificates. For more information, see Section 12.1, "Configuring SHA-2 Certificate," on page 213.

December 2014 (OES 11 SP2)

A troubleshooting section on resolving the POODLE security vulnerability has been added for the December 2014 OES patches. For more information, see Section 16.10, "The POODLE Security Vulnerability," on page 231 under Chapter 16, "Troubleshooting," on page 227.

August 2014 (OES 11 SP2)

A new section Section 7.11, "Restarting the OES Instance of Tomcat After Applying a Tomcat Update," on page 176 has been added under Chapter 7, "Updating (Patching) an OES 11 SP3 Server," on page 165.

June 2014 (OES 11 SP2)

A new troubleshooting section has been added (Section 16.9, "OES Installation Fails Due to Encrypted OES Media URL in the autoinst.xml File," on page 230).

January 2014 (OES 11 SP2)

Chapter or Section Changed	Summary of Changes
Initial OES 11 SP2 Release	◆ Includes document updates to new features as mentioned in Section 1.3, "What's New (OES 11 SP2)," on page 11. ◆ Explanation about the AutoYaST tags related to OES have been included in Appendix B, "AutoYaST XML Tags," on page 235 ◆ Secure communication using digital certificates is explained in Section 6.5, "Implementing Digital Certificates in an OES Environment," on page 161