SUSE Linux Enterprise Server 15 SP7

Upgrade Guide

Upgrade Guide

SUSE Linux Enterprise Server 15 SP7

This book guides you through upgrades of SUSE Linux Enterprise Server. If you use SUSE Linux Enterprise Server as base system for other SLE products or extensions, also see their product documentation for upgrade information specific to this product or extension.

Contents

Preface

Available documentation

Online documentation

Our documentation is available online at https://documentation.suse.com. Browse or download the documentation in various formats.

> **Latest updates**
>
> The latest updates are usually available in the English-language version of this documentation.

SUSE Knowledgebase

If you run into an issue, check out the Technical Information Documents (TIDs) that are available online at https://www.suse.com/support/kb/. Search the SUSE Knowledgebase for known solutions driven by customer need.

Release notes

For release notes, see https://www.suse.com/releasenotes/.

In your system

For offline use, the release notes are also available under `/usr/share/doc/release-notes` on your system. The documentation for individual packages is available at `/usr/share/doc/packages`.

Many commands are also described in their *manual pages*. To view them, run **man**, followed by a specific command name. If the **man** command is not installed on your system, install it with **sudo zypper install man**.

Improving the documentation

Your feedback and contributions to this documentation are welcome. The following channels for giving feedback are available:

Service requests and support

For services and support options available for your product, see https://www.suse.com/support/.

To open a service request, you need a SUSE subscription registered at SUSE Customer Center. Go to https://scc.suse.com/support/requests, log in, and click *Create New*.

Bug reports

Report issues with the documentation at https://bugzilla.suse.com/.

To simplify this process, click the *Report an issue* icon next to a headline in the HTML version of this document. This preselects the right product and category in Bugzilla and adds a link to the current section. You can start typing your bug report right away.

A Bugzilla account is required.

Contributions

To contribute to this documentation, click the *Edit source document* icon next to a headline in the HTML version of this document. This will take you to the source code on GitHub, where you can open a pull request.

A GitHub account is required.

> ### *Edit source document* only available for English
>
> The *Edit source document* icons are only available for the English version of each document. For all other languages, use the *Report an issue* icons instead.

For more information about the documentation environment used for this documentation, see the repository's README.

Mail

You can also report errors and send feedback concerning the documentation to `doc-team@suse.com`. Include the document title, the product version, and the publication date of the document. Additionally, include the relevant section number and title (or provide the URL) and provide a concise description of the problem.

Documentation conventions

The following notices and typographic conventions are used in this document:

- `/etc/passwd`: Directory names and file names
- *PLACEHOLDER*: Replace *PLACEHOLDER* with the actual value
- PATH: An environment variable

- **ls**, `--help`: Commands, options, and parameters

- `user`: The name of a user or group

- `package_name`: The name of a software package

- `Alt`, `Alt`–`F1`: A key to press or a key combination. Keys are shown in uppercase as on a keyboard.

- *File*, *File > Save As*: menu items, buttons

- ⬚x86_64▶This paragraph is only relevant for the AMD64/Intel 64 architectures. The arrows mark the beginning and the end of the text block.◀

  ⬚zseries;power▶This paragraph is only relevant for the architectures `IBM Z` and `POWER`. The arrows mark the beginning and the end of the text block.◀

- *Chapter 1, "Example chapter"*: A cross-reference to another chapter in this guide.

- Commands that must be run with `root` privileges. You can also prefix these commands with the **sudo** command to run them as a non-privileged user:

  ```
  #command>sudocommand
  ```

- Commands that can be run by non-privileged users:

  ```
  >command
  ```

- Commands can be split into two or multiple lines by a backslash character (\) at the end of a line. The backslash informs the shell that the command invocation will continue after the end of the line:

  ```
  >echo a b \
  c d
  ```

- A code block that shows both the command (preceded by a prompt) and the respective output returned by the shell:

  ```
  >command
  output
  ```

- Notices

Warning notice

Vital information you must be aware of before proceeding. Warns you about security issues, potential loss of data, damage to hardware, or physical hazards.

Important notice

Important information you should be aware of before proceeding.

Note notice

Additional information, for example about differences in software versions.

Tip notice

Helpful information, like a guideline or a piece of practical advice.

- Compact Notices

Note

Additional information, for example about differences in software versions.

Tip

Helpful information, like a guideline or a piece of practical advice.

Support

Find the support statement for SUSE Linux Enterprise Server and general information about technology previews below. For details about the product lifecycle, see https://www.suse.com/lifecycle.

If you are entitled to support, find details on how to collect information for a support ticket at https://documentation.suse.com/sles-15/html/SLES-all/cha-adm-support.html.

Support statement for SUSE Linux Enterprise Server

To receive support, you need an appropriate subscription with SUSE. To view the specific support offers available to you, go to https://www.suse.com/support/ and select your product.

The support levels are defined as follows:

L1

Problem determination, which means technical support designed to provide compatibility information, usage support, ongoing maintenance, information gathering and basic troubleshooting using available documentation.

L2

Problem isolation, which means technical support designed to analyze data, reproduce customer problems, isolate a problem area and provide a resolution for problems not resolved by Level 1 or prepare for Level 3.

L3

Problem resolution, which means technical support designed to resolve problems by engaging engineering to resolve product defects which have been identified by Level 2 Support.

For contracted customers and partners, SUSE Linux Enterprise Server is delivered with L3 support for all packages, except for the following:

- Technology previews.
- Sound, graphics, fonts, and artwork.
- Packages that require an additional customer contract.
- Some packages shipped as part of the module *Workstation Extension* are L2-supported only.
- Packages with names ending in `-devel` (containing header files and similar developer resources) will only be supported together with their main packages.

SUSE will only support the usage of original packages. That is, packages that are unchanged and not recompiled.

Technology previews

Technology previews are packages, stacks, or features delivered by SUSE to provide glimpses into upcoming innovations. Technology previews are included for your convenience to give you a chance to test new technologies within your environment. We would appreciate your feedback. If you test a technology preview, please contact your SUSE representative and let them know about your experience and use cases. Your input is helpful for future development.

Technology previews have the following limitations:

- Technology previews are still in development. Therefore, they may be functionally incomplete, unstable, or otherwise *not* suitable for production use.
- Technology previews are *not* supported.
- Technology previews may only be available for specific hardware architectures.
- Details and functionality of technology previews are subject to change. As a result, upgrading to subsequent releases of a technology preview may be impossible and require a fresh installation.
- SUSE may discover that a preview does not meet customer or market needs, or does not comply with enterprise standards. Technology previews can be removed from a product at any time. SUSE does not commit to providing a supported version of such technologies in the future.

For an overview of technology previews shipped with your product, see the release notes at https://www.suse.com/releasenotes.

Chapter 1. Lifecycle and support

1.1. Terminology

This section uses several terms. To understand the information, read the definitions below:

Backporting

> Backporting is the act of adapting specific changes from a newer version of software and applying it to an older version. The most commonly used case is fixing security holes in older software components. Usually it is also part of a maintenance model to supply enhancements or (less commonly) new features.

Delta RPM

> A delta RPM consists only of the binary diff between two defined versions of a package, and therefore has the smallest download size. Before being installed, the full RPM package is rebuilt on the local machine.

Downstream

> A metaphor of how software is developed in the open source world (compare it with *upstream*). The term *downstream* refers to people or organizations like SUSE who integrate the source code from upstream with other software to build a distribution which is then used by end users. Thus, the software flows downstream from its developers via the integrators to the end users.

Extension, Add-on product

> Extensions and third party add-on products provide additional functionality of product value to SUSE Linux Enterprise Server. They are provided by SUSE and by SUSE partners, and they are registered and installed on top of the base product SUSE Linux Enterprise Server.

LTSS

> LTSS is the abbreviation for Long Term Service Pack Support, which is available as an extension for SUSE Linux Enterprise Server.

Major release, General Availability (GA) version

> The major release of SUSE Linux Enterprise (or any software product) is a new version which brings new features and tools, decommissions previously deprecated components and comes with backward-incompatible changes. Major releases for example are SUSE Linux Enterprise 12 or 15.

Migration

Updating to a Service Pack (SP) by using the online update tools or an installation medium to install the respective patches. It updates all packages of the installed system to the latest state.

Migration target

A compatible product to which a system can be migrated, containing the version of the products/extensions and the URL of the repository. Migration targets can change over time and depend on installed extensions. It is possible to select multiple migration targets.

Module

Modules are fully supported parts of SUSE Linux Enterprise Server with a different lifecycle. They have a clearly defined scope and are delivered via online channel only. Registering at the SUSE Customer Center, RMT (Repository Mirroring Tool), or SUSE Multi-Linux Manager is a prerequisite for being able to subscribe to these channels.

Package

A package is a compressed file in `rpm` format that contains all files for a particular program, including optional components like configuration, examples, and documentation.

Patch

A patch consists of one or more packages and may be applied by means of delta RPMs. It may also introduce dependencies to packages that are not installed yet.

Service Pack (SP)

A service pack combines several patches into a form that is easy to install or deploy. Service packs are numbered and usually contain security fixes, updates, upgrades, or enhancements of programs.

Upstream

A metaphor of how software is developed in the open source world (compare it with *downstream*). The term *upstream* refers to the original project, author or maintainer of a software that is distributed as source code. Feedback, patches, feature enhancements, or other improvements flow from end users or contributors to upstream developers. They decide if the request will be integrated or rejected.

If the project members decide to integrate the request, it will show up in newer versions of the software. An accepted request will benefit all parties involved.

If a request is not accepted, it may be for different reasons. Either it is in a state that is not compliant with the project's guidelines, it is invalid, it is already integrated, or it is not in the interest or road map of the project. An unaccepted request makes it harder for upstream developers as they need to synchronize their patches with the upstream code. This practice is generally avoided, but sometimes it is still needed.

Update

Installation of a newer *minor* version of a package, which usually contains security or bug fixes.

Upgrade

Installation of a newer *major* version of a package or distribution, which brings *new features*. For a distinction between the upgrade options, see *the section called "Online and offline upgrade"*.

1.2. Product lifecycle

SUSE has the following product lifecycle:

- SUSE Linux Enterprise Server has a 13-year lifecycle: 10 years of general support and three years of extended support.
- SUSE Linux Enterprise Desktop has a 10-year lifecycle: seven years of general support and three years of extended support.
- Major releases are made every four years. Service packs are made every 12-14 months.

SUSE supports previous service packs for six months after the release of the new service pack. *Figure 1.1, "Major releases and service packs"* depicts some mentioned aspects.

Figure 1.1. Major releases and service packs
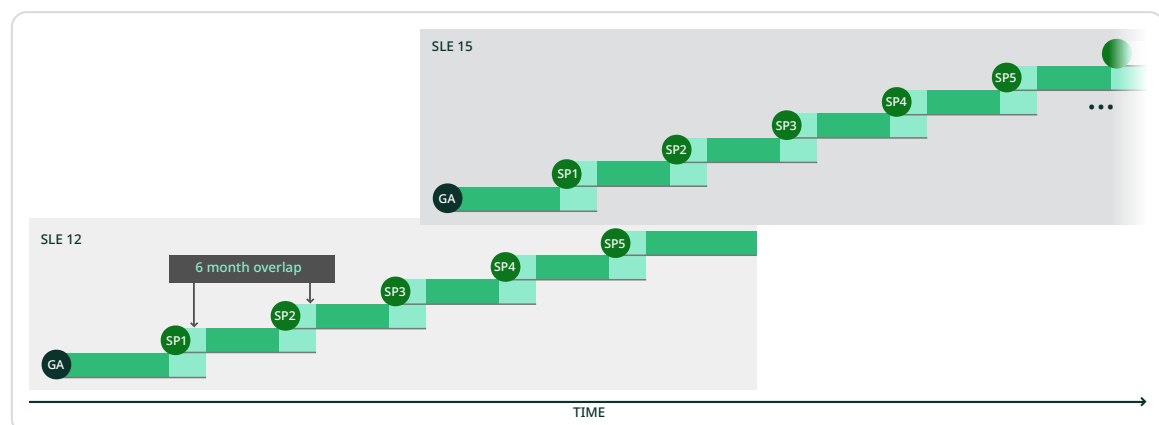
If you need additional time to design, validate and test your upgrade plans, Long Term Service Pack Support can extend the support you get by an additional 12 to 36 months in 12-month

increments. This gives you a total of 2 to 5 years of support on any service pack. For details, see *Figure 1.2, "Long term service pack support"*.

Figure 1.2. Long term service pack support

For more information, refer to https://www.suse.com/products/long-term-service-pack-support/.
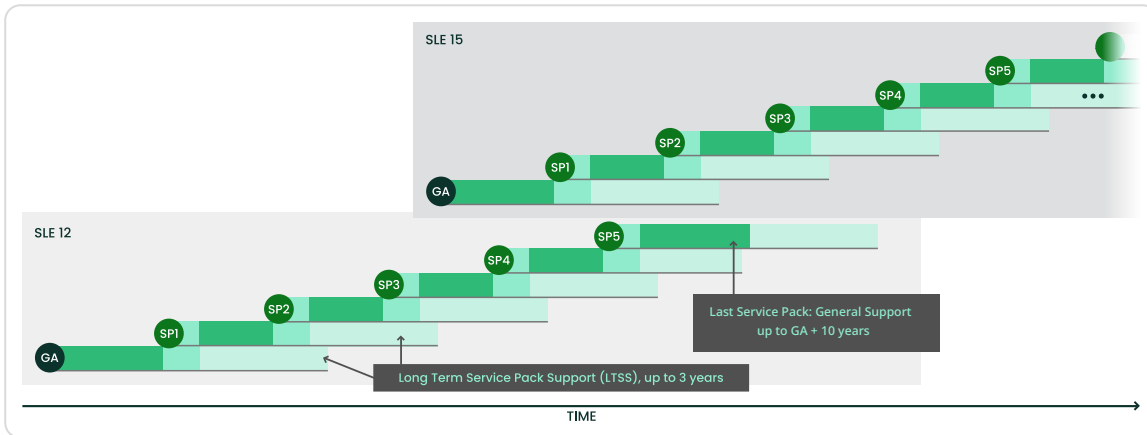
Refer to https://www.suse.com/lifecycle for more information about lifecycles, release frequency, and the overlay support period.

1.3. Module dependencies and lifecycles

For a list of modules, their dependencies, and lifecycles, see the *Modules and Extensions Quick Start*.

1.4. Generating periodic lifecycle report

SUSE Linux Enterprise Server can regularly check for changes in the support status of all installed products and send the report via e-mail in case of changes. To generate the report, install the `zypper-lifecycle-plugin` with **zypper in zypper-lifecycle-plugin**.

Enable the report generation on your system with **systemctl**:

```
>sudosystemctl enable lifecycle-report.timer
```

The recipient and subject of the report e-mail, and the report generation period can be configured in the file `/etc/sysconfig/lifecycle-report` with any text editor. The settings `MAIL_TO` and `MAIL_SUBJ` define the mail recipient and subject, while `DAYS` sets the interval at which the report is generated.

The report displays changes in the support status after the change occurred and not in advance. If the change occurs right after the generation of the last report, it can take up to 14 days until you are notified of the change. Take this into account when setting the `DAYS` option. Change the following configuration entries to fit your requirements:

```
MAIL_TO='root@localhost'
MAIL_SUBJ='Lifecycle report'
DAYS=14
```

The latest report is available in the file `/var/lib/lifecycle/report`. The file contains two sections. The first section informs about the end of support for used products. The second section lists packages with their support end dates and update availability.

1.5. Support levels

The range for extended support levels starts from year 10 and ends in year 13. These contain continued L3 engineering level diagnosis and reactive critical bug fixes. With these support levels, you will receive updates for trivially exploitable root exploits in the kernel and other root exploits directly executable without user interaction. Furthermore, they support existing workloads, software stacks, and hardware with limited package exclusion list. Find an overview in *Table 1.1, "Security updates and bug fixes"*.

Table 1.1. Security updates and bug fixes

	General Support for Most Recent Service Pack (SP)			General Support for Previous SP, with LTSS	Extended Support with LTSS
Feature	**Year 1-5**	**Year 6-7**	**Year 8-10**	**Year 4-10**	**Year 10-13**
Technical Services	Yes	Yes	Yes	Yes	Yes
Access to Patches and Fixes	Yes	Yes	Yes	Yes	Yes
Access to Documentation and Knowledge Base	Yes	Yes	Yes	Yes	Yes
Support for Existing Stacks and Workloads	Yes	Yes	Yes	Yes	Yes

Feature	General Support for Most Recent Service Pack (SP)			General Support for Previous SP, with LTSS	Extended Support with LTSS
	Year 1-5	Year 6-7	Year 8-10	Year 4-10	Year 10-13
Support for New Deployments	Yes	Yes	Limited (Based on partner and customer requests)	Limited (Based on partner and customer requests)	No
Enhancement Requests	Yes	Limited (Based on partner and customer requests)	Limited (Based on partner and customer requests)	No	No
Hardware Enablement and Optimization	Yes	Limited (Based on partner and customer requests)	Limited (Based on partner and customer requests)	No	No
Driver updates via SUSE SolidDriver Program (formerly PLDP)	Yes	Yes	Limited (Based on partner and customer requests)	Limited (Based on partner and customer requests)	No
Backport of Fixes from Recent SP	Yes	Yes	Limited (Based on partner and customer requests)	N/A	N/A
Security Updates[1]	All	All	All	Critical only	Critical only

	General Support for Most Recent Service Pack (SP)			General Support for Previous SP, with LTSS	Extended Support with LTSS
Feature	Year 1-5	Year 6-7	Year 8-10	Year 4-10	Year 10-13
Defect Resolution	Yes	Yes	Limited (Severity Level 1 and 2 defects only)	Limited (Severity Level 1 and 2 defects only)	Limited (Severity Level 1 and 2 defects only)

[1] For further information on the SUSE Linux Enterprise Update Policy, refer to the following knowledgebase article.

1.6. Registering and deregistering machines with SUSEConnect

On registration, the system receives repositories from the SUSE Customer Center (see https://scc.suse.com/) or a local registration proxy like SMT. The repository names map to specific URIs in the customer center. To list all available repositories on your system, use **zypper** as follows:

```
#zypper repos -u
```

This gives you a list of all available repositories on your system. Each repository is listed by its alias, name and whether it is enabled and will be refreshed. The option -u gives you also the URI from where it originated.

To register your machine, run SUSEConnect, for example:

```
#SUSEConnect -r REGCODE
```

To deregister your machine, you can use SUSEConnect too:

```
#SUSEConnect --de-register
```

To check your locally installed products and their status, use the following command:

```
#SUSEConnect -s
```

1.7. Enabling LTSS support

Long Term Service Pack Support (LTSS) extends the lifecycle of SUSE Linux Enterprise Server. It is available as an extension. For more information about LTSS, refer to https://www.suse.com/products/long-term-service-pack-support/

To enable the LTSS extension, perform the following steps:

1. Make sure your system is registered with a subscription that is eligible for LTSS. If the system is not yet registered, run:

```
>sudoSUSEConnect -r REGISTRATION_CODE -e EMAIL_ADDRESS
```

2. Make sure the LTSS extension is available for your system:

```
>sudoSUSEConnect --list-extensions | grep LTSS
SUSE Linux Enterprise Server LTSS 15 SP7 x86_64
Activate with: SUSEConnect -p SLES-LTSS/15.7/x86_64 -r ADDITIONAL REGCODE
```

3. Activate the module as instructed:

```
>sudoSUSEConnect -p SLES-LTSS/15.7/x86_64 -r REGISTRATION_CODE
```

1.8. Identifying the SLE version

If you need to identify the version of an SLE installation, check the content of the file `/etc/os-release`.

A machine readable XML output is available with **zypper**:

```
>zypper --no-remote --no-refresh --xmlout --non-interactive products -i
<?xml version='1.0'?>
<stream>
<product-list>
<product name="SLES" version="15" release="0" epoch="0" arch="x86_64"
vendor="SUSE" summary="SUSE Linux Enterprise Server 15" repo="@System"
productline="sles" registerrelease="" shortname="SLES15" flavor="" isbase="true"
installed="true"><endoflife time_t="0" text="0"/><registerflavor/
><description>SUSE Linux Enterprise offers [...]</description></product>
</product-list>
</stream>
```

Chapter 2. Upgrade paths and methods

2.1. Upgrading versus fresh installation

Upgrades between two major releases of SUSE Linux Enterprise Server are supported by SUSE. Whether it is better to upgrade or perform a fresh installation depends on your specific scenario. While upgrades involve less work, fresh installations ensure you benefit from all the new features of a release such as disk layout changes, specific file system features, and other improvements. To get the most out of your system, SUSE therefore recommends fresh installations in most scenarios.

In both cases—upgrade as well as a fresh installation—customers need to check if system settings and default values still fit their requirements.

For updates from one service pack of a specific release to another one of the same codestream, SUSE recommends to do it in-place, and not to perform a fresh installation. Nevertheless, there may be reasons and scenarios for a customer to perform a fresh installation in this case, too. The decision as to which is more suitable can only be made by the customer.

2.2. Online and offline upgrade

SUSE supports the following upgrade and migration methods. For more information about the terminology, see *the section called "Terminology"*. The methods are:

Online

> Upgrades that are executed from the running operating system itself (system up and running state). Examples: online update with Zypper or YaST, connected through SUSE Customer Center or Repository Mirroring Tool (RMT), Salt Policy via SUSE Multi-Linux Manager.

> For details, see *Chapter 5, Upgrading online*.

> When migrating between Service Packs of the same major release, we suggest following *the section called "Upgrading with the online migration tool (YaST)"* or *the section called "Upgrading with Zypper"*.

Offline

> Upgrading offline implies that the operating system to be upgraded is *not* running (system down state). Instead, the installer for the target operating system is booted (for example, from the installation media, via network or via local boot loader), and performs the upgrade.

> For details, see *Chapter 4, Upgrading offline*.

SUSE Multi-Linux Manager clients

If your machine is managed by SUSE Multi-Linux Manager, update it as described in the SUSE Multi-Linux Manager documentation. The *Client Migration* procedure is described in the *SUSE Multi-Linux Manager Upgrade Guide*, available at https://documentation.suse.com/multi-linux-manager/.

2.3. Supported upgrade and migration paths to SLES 15 SP7

Before you perform any migration, read *Chapter 3, Preparing the upgrade*.

Cross-architecture upgrades are not supported

Cross-architecture upgrades, such as upgrading from a 32-bit version of SUSE Linux Enterprise Server to the 64-bit version, or upgrading from big endian to little endian are *not* supported!

Specifically, SLE 11 on POWER (big endian) to SLE 15 SP7 on POWER (new: little endian!) is *not* supported.

Also, since SUSE Linux Enterprise 15 is 64-bit only, upgrades from any 32-bit SUSE Linux Enterprise 11 systems to SUSE Linux Enterprise 15 and later are *not* supported.

To make a cross-architecture upgrade, you need to perform a new installation.

Skipping service packs

The easiest upgrade path is consecutively installing all service packs. For the SUSE Linux Enterprise 15 product line (GA and the subsequent service packs), skipping from one to any other service pack is technically possible, but not officially supported. For a supported upgrade path, only up to two service packs may be skipped, and your system needs to be on a supported tier before launching the upgrade (fully upgraded LTSS when out of regular support). For example, upgrading from SLE 15 SP1 to 15 SP4 is *not* supported, as SP1 is out of regular support before SP4 is released. However, the upgrade from SLE 15 SP1 LTSS to 15 SP4 or SP3 LTSS is supported.

Figure 2.1. Overview of supported upgrade paths
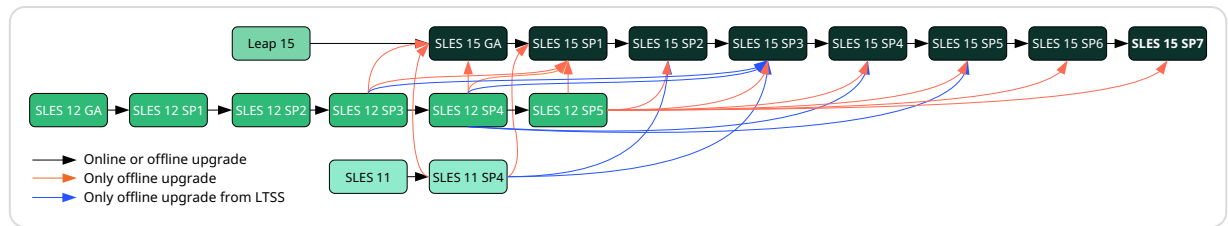
Upgrading databases

The upgrade paths described here apply only to SUSE Linux Enterprise as the operating system of a machine, not to all the applications it runs. If you have workloads such as PostgreSQL or MariaDB databases, intermediate OS upgrades may be required in order to upgrade your applications.

Before upgrading the operating system, consult the Release Notes for information about database versions. If a new major version is shipped, refer to *Chapter 3, Preparing the upgrade* for upgrade instructions.

Supported upgrade paths per version

Upgrading from SUSE Linux Enterprise Server 11

Upgrading from SLES 11 directly is not supported. You need at least SLES 11 SP4 and you can only upgrade to SLES 15 SP3 before you can proceed to SLES 15 SP7.

If you cannot do a fresh installation, first, upgrade your installed SLES 11 service pack to SLES 11 SP4. This upgrade is described in the *SLES 11 SP4 Deployment Guide*. Next, perform an offline upgrade to SLES 15 SP3. This upgrade is described in the *SLES 15 SP3 Deployment Guide*. Then, follow the instructions in this guide to upgrade to SLES 15 SP7.

Upgrading from SUSE Linux Enterprise Server 12 GA / SP1 / SP2 / SP3 / SP4

Upgrading from SLES 12 SP4 or older service packs directly is not supported. You need at least SLES 12 SP5 before you can proceed to SLES 15 SP7.

If you cannot do a fresh installation, first, upgrade your installed SLES 12 service pack to SLES 12 SP5. This upgrade is described in the *SLES 12 SP5 Deployment Guide*

Upgrading from SUSE Linux Enterprise Server 12 SP5

Upgrading from SLES 12 SP5 is only supported via an offline upgrade. Refer to *Chapter 4, Upgrading offline* for details.

Upgrading from SUSE Linux Enterprise Server 15 GA / SP1 / SP2 / SP3 / SP4 / SP5

Upgrading from SLES 15 GA, SP1, SP2, SP3, SP4, or SP5 directly is no longer supported. You need at least SLES 15 SP6 before you can proceed to SLES 15 SP7.

Upgrading from SUSE Linux Enterprise Server 15 SP1 / SP2 / SP3 with LTSS or ESPOS

Upgrading from SLES 15 SP1, SP2, or SP3 with LTSS or ESPOS directly is not supported. You need at least SLES 15 SP4 with LTSS or ESPOS before you can proceed to SLES 15 SP7.

First, upgrade your installed SLES 15 service pack to SLES 15 SP4. This upgrade is described in the *SLES 15 SP4 Upgrade Guide*. Then, follow the instructions in this guide to upgrade to SLES 15 SP7.

Upgrading from SUSE Linux Enterprise Server 15 SP4 / SP5 with LTSS or ESPOS

Upgrading from SLES 15 SP4 or SP5 with LTSS or ESPOS is supported both online and offline. Refer to *the section called "Online and offline upgrade"* for details.

Upgrading from SUSE Linux Enterprise Server 15 SP6

Upgrading from SLES 15 SP6 is supported both online and offline. Refer to *the section called "Online and offline upgrade"* for details.

Upgrading SUSE Linux Enterprise public cloud guests

For instructions on upgrading SLE guests in public clouds, see *Using the SUSE Distribution Migration System*.

Upgrading from openSUSE Leap 15.0 / 15.1 / 15.2 / 15.3 / 15.4 / 15.5

Upgrading from openSUSE Leap 15.0, 15.1, 15.2, 15.3, 15.4, or 15.5 directly is no longer supported. You need at least openSUSE Leap 15.6 before you can proceed to SLES 15 SP7.

Upgrading from openSUSE Leap 15.6 / 15.7

Upgrading from openSUSE Leap 15.6 or 15.7 is supported. See *the section called "Upgrading from openSUSE Leap to SUSE Linux Enterprise Server "*. Only the server installation of Leap is supported for an upgrade.

Extended Service Pack Overlap Support (ESPOS)

For some products, SUSE offers Extended Service Pack Overlap Support (ESPOS) under the same conditions as LTSS. For more information about ESPOS, refer to the documentation of the respective SUSE Linux Enterprise product and the Product Lifecycle Support Policies webpage.

Chapter 3. Preparing the upgrade

3.1. Make sure the system is up-to-date

Upgrading the system is only supported from the most recent patch level. Make sure the latest system updates are installed by either running **zypper patch** or by starting the YaST module *Online-Update*.

New 4096-bit signing key for SUSE Linux Enterprise 15

Mid 2023, the SUSE Linux Enterprise 15 product family switched over from a RSA 2048-bit signing key to a new RSA 4096-bit key. This change covers RPM packages, package repositories and ISO signatures. Old repositories that are not updated anymore and RPMs released up to the switch-over date, will remain signed with the old 2048-bit key.

If you update your system, the new key is automatically imported into the RPM keyring from the suse-build-key package on SLE 15 SP 4 and SP5 as well as the LTSS versions of SLE 15 SP1, SP2 and SP3.

If the key has not been imported yet, you can manually import it with:

```
>sudorpm --import /usr/lib/rpm/gnupg/keys/gpg-
pubkey-3fa1d6ce-63c9481c.asc
```

If you are running an older version of SLE or did not import the new key, you will be asked to trust it during the upgrade. Make sure the fingerprint matches:

```
pub   rsa4096/0xF74F09BC3FA1D6CE 2023-01-19 [SC] [expires:
2027-01-18]
Key fingerprint = 7F00 9157 B127 B994 D5CF  BE76 F74F 09BC 3FA1 D6CE
uid            SUSE Package Signing Key <build@suse.de>
```

Additionally, a reserve 4096-bit RSA key for disaster recovery purposes was imported:

```
pub   rsa4096/0xA1BFC02BD588DC46 2023-01-19 [SC] [expires:
2033-01-16]
Key fingerprint = B56E 5601 41D8 F654 2DFF  3BF9 A1BF C02B D588 DC46
uid            SUSE Package Signing Key (reserve key) <build@suse.de>
```

This key can be manually imported using:

```
>sudorpm --import /usr/lib/rpm/gnupg/keys/gpg-pubkey-
d588dc46-63c939db.asc
```

Both keys can also be found on the installation media and the SUSE website at https://www.suse.com/support/security/keys/.

3.2. Read the release notes

Find a list of all changes, new features, and known issues in the <u>release notes</u>. You can also find the release notes on the installation media in the `docu` directory.

The release notes usually only contain the changes between two subsequent releases. If you are skipping one or more Service Packs, check the release notes of the skipped Service Packs as well.

Consult the release notes to check whether the following applies:

- Your hardware needs special considerations
- Any currently used software packages have changed significantly
- Your installation requires special precautions

3.3. Make a backup

Before upgrading, back up your data by copying the existing configuration files to a separate medium (such as tape device, removable hard disk, etc.). This primarily applies to files stored in `/etc` and some directories and files in `/var` and `/opt`. You may also want to write the user data in `/home` (the `HOME` directories) to a backup medium.

Back up all data as `root`. Only `root` has sufficient permissions for all local files.

If you have selected *Update an Existing System* as the installation mode in YaST, you can choose to do a (system) backup at a later point in time. You can choose to include all modified files and files from the `/etc/sysconfig` directory. However, this is not a complete backup, as all the other important directories mentioned above are missing. Find the backup in the `/var/adm/backup` directory.

3.4. Check the available disk space

Software tends to grow from version to version. Therefore, take a look at the available partition space before updating. If you suspect you are running short of disk space, back up your data before increasing the available space by resizing partitions, for example. 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.

Automatic check for enough space in YaST

During the update procedure, YaST will check how much free disk space is available and display a warning to the user if the installation may exceed the available amount. In that case, performing the update may lead to an *unusable system*! Only if you know exactly what you are doing (by testing beforehand), you can skip the warning and continue the update.

3.4.1. Checking disk space on non-Btrfs file systems

Use the **df** command to list available disk space. For example, in *Example 3.1, "List with **df -h** "*, the root partition is /dev/sda3 (mounted as /).

Example 3.1. List with df -h

```
Filesystem      Size  Used Avail Use% Mounted on
    /dev/sda3          74G   22G   53G  29% /
    tmpfs            506M     0  506M   0% /dev/shm
    /dev/sda5          116G  5.8G  111G   5% /home
    /dev/sda1           44G    4G   40G   9% /data
```

3.4.2. Checking disk space on Btrfs root file systems

On a Btrfs file system, the output of **df** can be misleading, because in addition to the space the raw data allocates, a Btrfs file system also allocates and uses space for metadata.

Consequently a Btrfs file system may report being out of space even though it seems that plenty of space is still available. In that case, all space allocated for the metadata is used up. For details on how to check for used and available space on a Btrfs file system, see the section called "Checking for free space" in "Storage Administration Guide". For more information refer to **man 8 btrfs-filesystem** and https://btrfs.wiki.kernel.org/index.php/FAQ.

When using Btrfs for root file systems on your machine, make sure there is enough free space. Check the available space on all mounted partitions. In the worst case, an upgrade needs as much disk space as the current root file system (without /.snapshot) for a new snapshot.

The following recommendations have been proven:

- For all file systems, including Btrfs, you need enough free disk space to download and install big RPMs. The space of old RPMs is only freed after new RPMs are installed.

- For Btrfs with snapshots, you need as a minimum as much free space as your current installation takes. We recommend having twice as much free space as the current installation.

    If you do not have enough free space, you can try to delete old snapshots with **snapper**:

    ```
    #snapper list
        #snapper delete NUMBER
    ```

    However, this may not help in all cases. Before migration, most snapshots occupy only little space.

3.5. Listing installed packages and repositories

You can save a list of installed packages; for example, when doing a fresh install of a new major SLE release or reverting to the old version.

Note

Be aware that not all installed packages or used repositories are available in newer releases of SUSE Linux Enterprise. Some may have been renamed and others replaced. It is also possible that some packages are still available for legacy purposes while another package is used by default. Therefore, some manual editing of the files might be necessary. This can be done with any text editor.

1. Create a file named `repositories.bak.repo` containing a list of all used repositories:

```
#zypper lr -e repositories.bak
```

2. Also create a file named `installed-software.bak` containing a list of all installed packages:

```
#rpm -qa --queryformat '%{NAME}\n' > installed-software.bak
```

3. Back up both files. The repositories and installed packages can be restored with the following commands:

```
#zypper ar repositories.bak.repo
#zypper install $(cat installed-software.bak)
```

Number of packages increases with an update to a new major release

A system upgraded to a new major version (SLE *X+1*) may contain more packages than the initial system (SLE *X*). It will also contain more packages than a fresh installation of SLE *X+1* with the same pattern selection. Reasons for this are:

- Packages were split to allow a more fine-grained package selection. For example, 37 `texlive` packages on SLE 11 were split into over 3000 packages on SLE 15.

- When a package has been split, all new packages are installed in the upgrade case to retain the same functionality as the previous version. However, the new default for a fresh installation of SLE *X+1* may be to not install all packages.

- Legacy packages from SLE *X* may be kept for compatibility reasons.

- Package dependencies and the scope of patterns may have changed.

3.6. Disable the LTSS extension

If you upgrade a SUSE Linux Enterprise Server system with Long Term Service Pack Support (LTSS) to a version that is still under general support, the upgrade will fail with the error No

`migration available`. This happens because **`zypper migration`** tries to migrate *all* repositories, but there is no LTSS repository for the new version yet.

To fix this issue, disable the LTSS extension before the upgrade.

1. Check if the LTSS extension is enabled:

   ```
   >sudo SUSEConnect --list-extensions | grep LTSS
   SUSE Linux Enterprise Server LTSS 12 SP4 x86_64 (Installed)
   Deactivate with: SUSEConnect -d -p SLES-LTSS/12.4/x86_64
   ```

2. Disable the LTSS extension with the command from the **SUSEConnect** output above:

   ```
   >sudo SUSEConnect -d -p SLES-LTSS/12.4/x86_64
   Deregistered SUSE Linux Enterprise Server LTSS 12 SP4 x86_64
   To server: https://scc.suse.com/
   ```

3. Verify the LTSS repository is no longer present with **`zypper lr`**.

3.7. Migrate your PostgreSQL database

SUSE Linux Enterprise Server15 SP7 ships with the PostgreSQL database versions 15, 16 and 17. While version 17 is the default, versions 15 and 16 are still provided through the `Legacy` module for upgrades from earlier versions of SUSE Linux Enterprise Server. Additional versions are available through SUSE Package Hub.

Because of the required migration work of the database, there is no automatic upgrade process. As such, the switch from one version to another needs to be performed manually.

The migration process is conducted by the **`pg_upgrade`** command, which is an alternative method of the classic dump and reload. In comparison with the "dump and reload" method, **`pg_upgrade`** makes the migration less time-consuming.

The program files for each PostgreSQL version are stored in different, version-dependent directories. For example, in `/usr/lib/postgresql96/` for version 9.6, in `/usr/lib/postgresql10/` for version 10, and in `/usr/lib/postgres17/` for version 17. Note that the versioning policy of PostgreSQL has changed between the major versions 9.6 and 10. For details, see https://www.postgresql.org/support/versioning/.

The procedure below describes the database migration from version 16 to 17. When using a different version as start or target, replace the version numbers accordingly.

To perform the database migration, do the following:

1. Make sure the following preconditions are fulfilled:

   ◦ If not already done, upgrade any package of the old PostgreSQL version to the latest release through a maintenance update.

   ◦ Create a backup of your existing database.

- Install the packages for the new PostgreSQL major version. For SLE 15 SP7, this means installing `postgresql17-server` and all the packages it depends on.

- Install the package `postgresql17-contrib`, which contains the command **`pg_upgrade`**:

  ```
  #zypper in postgresql17-contrib
  ```

- Make sure you have enough free space in your PostgreSQL data volume, which is `/var/lib/pgsql/data` by default. If space is tight, try to reduce size with the following SQL command on each database (can take a long time!):

  ```
  VACUUM FULL;
  ```

2. Stop the PostgreSQL server:

   ```
   #systemctl stop postgresql.service
   ```

3. Rename your old data directory:

   ```
   #mv /var/lib/pgsql/data /var/lib/pgsql/data.old
   ```

4. Initialize your new database instance either manually with **`initdb`** or by starting and stopping PostgreSQL, which does it automatically:

   ```
   #systemctl start postgresql.service
   #systemctl stop postgresql.service
   ```

5. If you have changed your configuration files in the old version, consider transferring these changes to the new configuration files. This may affect the files `postgresql.auto.conf`, `postgresql.conf`,`pg_hba.conf` and `pg_ident.conf`. The old versions of these files are located in `/var/lib/pgsql/data.old/`, and the new versions can be found in `/var/lib/pgsql/data`.

   Note that copying the old configuration files is not recommended, because this may overwrite new options, new defaults and changed comments.

6. Start the migration process as user `postgres`:

   ```
   #su - postgres
   postgres > pg_upgrade \
    --old-datadir "/var/lib/pgsql/data.old" \
    --new-datadir "/var/lib/pgsql/data" \
    --old-bindir "/usr/lib/postgresql16/bin/" \
    --new-bindir "/usr/lib/postgresql17/bin/"
   postgres > exit
   ```

7. Start your new PostgreSQL 17 database instance:

   ```
   #systemctl start postgresql.service
   ```

8. Check if the migration was successful. The scope of the test depends on your use case, and there is no general tool to automate this step.

9. Remove any old PostgreSQL 16 packages and your old data directory:

```
#zypper search -s postgresql16| xargs zypper rm -u
#rm -rf /var/lib/pgsql/data.old
```

For more information about upgrading databases or using alternative methods such as logical replication, refer to the official PostgreSQL documentation at https://www.postgresql.org/docs/17/upgrading.html.

3.8. Migrate your MySQL or MariaDB database

As of SUSE Linux Enterprise 12, SUSE switched from MySQL to MariaDB. Before you start any upgrade, it is highly recommended to back up your database.

To perform the database migration, do the following:

1. Create a dump file:

   ```
   #mysqldump -u root -p --all-databases --add-drop-database >
   mysql_backup.sql
   ```

   By default, **mysqldump** does not dump the INFORMATION_SCHEMA or performance_schema database. For more details refer to https://mariadb.com/kb/en/mariadb-dumpmysqldump/.

2. Store your dump file, the configuration file /etc/my.cnf, and the directory /etc/mysql/ for later investigation (*not* installation!) in a safe place.

3. Perform the SUSE Linux Enterprise Server upgrade. After the upgrade, your former configuration file /etc/my.cnf will still be intact. You can find the new configuration in the file /etc/my.cnf.rpmnew.

4. Configure your MariaDB database to your needs. Do *not* use the former configuration file and directory, but use it as a reminder and adapt it.

5. Make sure you start the MariaDB server:

   ```
   #systemctl start mariadb
   ```

   If you want to start the MariaDB server on every boot, enable the service:

   ```
   #systemctl enable mariadb
   ```

6. Verify that MariaDB is running properly by connecting to the database:

   ```
   #mariadb -u root -p
   ```

3.9. Create non-MD5 server certificates for Java applications

As a security measure, MD5-based certificates are no longer supported in Java. If you have certificates created as MD5, re-create your certificates with the following steps:

1. Open a terminal and log in as root.

2. Create a private key:

```
#openssl genrsa -out server.key 1024
```

If you want a stronger key, replace 1024 with a higher number, for example, 4096.

3. Create a certificate signing request (CSR):

```
#openssl req -new -key server.key -out server.csr
```

4. Self-sign the certificate:

```
#openssl x509 -req -days 365 -in server.csr -signkey server.key -out
server.crt
```

5. Create the PEM file:

```
#cat server.key server.crt > server.pem
```

6. Place the files `server.crt`, `server.csr`, `server.key`, and `server.pem` in the respective directories where the keys can be found. For Tomcat, for example, this directory is `/etc/tomcat/ssl/`.

3.10. Shut down virtual machine guests

If your machine serves as a VM Host Server for KVM or Xen, make sure to properly shut down all running VM Guests prior to the update. Otherwise you may not be able to access the guests after the update.

3.11. Adjust your SMT client setup

If the machine you want to upgrade is registered as a client against an SMT server, take care to do the following:

Check if the version of the **clientSetup4SMT.sh** script on your host is up to date. **clientSetup4SMT.sh** from older versions of SMT cannot manage SMT 12 clients. If you apply software patches regularly on your SMT server, you can always find the latest version of **clientSetup4SMT.sh** at `<SMT_HOSTNAME>/repo/tools/clientSetup4SMT.sh`.

In case upgrading your machine to a higher version of SUSE Linux Enterprise Server fails, deregister the machine from the SMT server as described in *Procedure 3.1*. Afterward, restart the upgrade process.

Procedure 3.1. Deregistering a SUSE Linux Enterprise client from an SMT server

1. Log in to the client machine.

2. The following step depends on the current operating system of the client:

   ◦ For SUSE Linux Enterprise 11, execute the following commands:

```
>sudo suse_register -E
>sudo rm -f /etc/SUSEConnect
>sudo rm -rf /etc/zypp/credentials.d/*
>sudo rm -rf /etc/zypp/repos.d/*
>sudo rm -f /etc/zypp/services.d/*
>sudo rm -f /var/cache/SuseRegister/*
>sudo rm -f /etc/suseRegister*
>sudo rm -f /var/cache/SuseRegister/lastzmdconfig.cache
>sudo rm -f /etc/zmd/deviceid
>sudo rm -f /etc/zmd/secret
```

◦ For SUSE Linux Enterprise 12, execute the following commands:

```
>sudo SUSEConnect --de-register
>sudo SUSEConnect --cleanup
>sudo rm -f /etc/SUSEConnect
>sudo rm -rf /etc/zypp/credentials.d/*
>sudo rm -rf /etc/zypp/repos.d/*
>sudo rm -f /etc/zypp/services.d/*
```

3. Log in to the SMT server.

4. Check if the client has successfully been deregistered by listing all client registrations:

```
>sudo smt-list-registrations
```

5. If the client's host name is still listed in the output of this command, get the client's Unique ID from the first column. (The client might be listed with multiple IDs.)

6. Delete the registration for this client:

```
>sudo smt-delete-registration -g UNIQUE_ID
```

7. If the client is listed with multiple IDs, repeat the step above for each of its unique IDs.

8. Check if the client has now successfully been deregistered by re-running:

```
>sudo smt-list-registrations
```

3.12. Changes in AutoYaST profiles from SLE 12 to 15

To learn how to migrate your AutoYaST profiles, see Appendix D, Differences between AutoYaST profiles in SLE 12 and 15 in "AutoYaST Guide".

3.13. Upgrading a Subscription Management Tool (SMT) server

A server running SMT requires a special upgrade procedure. Please refer to Chapter 3, Migrate from SMT to RMT in "Repository Mirroring Tool Guide" in the Repository Mirroring Tool Guide.

3.14. Temporarily disabling kernel multiversion support

SUSE Linux Enterprise Server allows installing multiple kernel versions by enabling the respective settings in /etc/zypp/zypp.conf. Support for this feature needs to be temporarily disabled to upgrade to a service pack. When the update has successfully finished, multiversion support can be re-enabled. To disable multiversion support, comment the respective lines in /etc/zypp/zypp.conf. The result should look similar to:

```
#multiversion = provides:multiversion(kernel)
#multiversion.kernels = latest,running
```

To re-activate this feature after a successful update, remove the comment signs. For more information about multiversion support, refer to the section called "Enabling and configuring multiversion support" in "Administration Guide".

3.15. IBM Z: Adjust `zipl` for UEFI Secure Boot

When upgrading from SUSE Linux Enterprise Server 12, enabling UEFI Secure Boot during or after the upgrade with **yast bootloader** will fail with an error:

```
Error: Could not install Secure Boot IPL records: Missing
signature in image file /boot/zipl/image.prev
/sbin/zipl: Failed
/usr/sbin/grub2-install: error: `grub2-zipl-setup' failed.
```

This happens because `/boot/zipl` still contains the previous, unsigned kernel and initrd as fallback in case the new kernel does not boot. To avoid this error, edit `/etc/default/grub` and change SUSE_SECURE_BOOT=1 to SUSE_SECURE_BOOT=auto. This setting makes **zipl** write a signature for the new kernel but not yield an error for the old kernel. Then run **grub2-install** to re-install the boot loader.

Alternatively you can remove the obsolete kernel and initrd files from `/boot/zipl` manually. Only do so when you have already rebooted into the new kernel after the upgrade.

After the next SUSE Linux Enterprise 15 kernel update, you can switch back to SUSE_SECURE_BOOT=1 to ensure all kernels are signed.

For more information, refer to **man 8 zipl** and the IBM documentation at https://www.ibm.com/docs/en/linux-on-systems?topic=loader-parameters.

3.16. Adjust the `resume` boot parameter

On systems that have been installed with SUSE Linux Enterprise Server 12 or older, the default kernel command line in `/etc/default/grub` may contain a `resume` parameter using a device node name such as `/dev/sda1` to refer to the hibernation (suspend-to-disk) device. As device node names are not persistent and may change between reboots, fixing this is highly recommended. Otherwise, the upgraded system may hang on reboot.

1. Find the hibernation device:

   ```
   >sudogrep resume /etc/default/grub
   GRUB_CMDLINE_LINUX_DEFAULT="resume=/dev/sda1 splash=silent quiet showopts"
   ```

   The hibernation device is `/dev/sda1`. If the command returns nothing, hibernation is not configured.

2. Get the UUID for */dev/sda1*:

```
>sudoblkid /dev/vda1
/dev/vda1: UUID="a1d1f2e0-b0ee-4be2-83d5-78a98c585827" TYPE="swap"
PARTUUID="000134b5-01"
```

The UUID for `/dev/sda1` is `a1d1f2e0-b0ee-4be2-83d5-78a98c585827`.

3. Edit `/etc/default/grub` and adjust the `resume` parameter. Replace *`/dev/sda1`* with *`UUID=a1d1f2e0-b0ee-4be2-83d5-78a98c585827`*. The result will look like this:

```
GRUB_CMDLINE_LINUX_DEFAULT="resume=UUID=a1d1f2e0-
b0ee-4be2-83d5-78a98c585827 splash=silent quiet showopts"
```

4. Update the configuration of the grub boot manger:

```
>sudogrub2-mkconfig -o /boot/grub2/grub.cfg
```

If the system does not use hibernation, you can simply remove the `resume` parameter and update the boot configuration.

3.17. Upgrading on IBM Z

Upgrading a SUSE Linux Enterprise installation on IBM Z requires the **Upgrade=1** kernel parameter, for example via the parmfile. See the section called "The parmfile—automating the system configuration" in "Deployment Guide".

3.18. IBM POWER: Starting an X server

On SLES 12 for IBM POWER the display manager is configured not to start a local X server by default. This setting was reversed on SLES 12 SP1—the display manager now starts an X server.

To avoid problems during upgrade, the SUSE Linux Enterprise Server setting is not changed automatically. If you want the display manager to start an X server after the upgrade, change the setting of DISPLAYMANAGER_STARTS_XSERVER in `/etc/sysconfig/displaymanager` as follows:

```
DISPLAYMANAGER_STARTS_XSERVER="yes"
```

Chapter 4. Upgrading offline

4.1. Conceptual overview

Before upgrading your system, read *Chapter 3, Preparing the upgrade* first.

To upgrade your system, boot from an installation source, as you would do for a fresh installation. However, when the boot screen appears, you need to select *Upgrade* (instead of *Installation*). The upgrade can be started from:

- **Removable media**This includes media such as CDs, DVDs or USB mass storage devices. For more information, see *the section called "Starting the upgrade from an installation medium"*.
- **Network resource**You can either boot from the local medium and then select the respective network installation type, or boot via PXE. For more information, see *the section called "Starting the upgrade from a network source"*.

4.2. Starting the upgrade from an installation medium

The procedure below describes booting from a DVD, but you can also use another local installation medium like an ISO image on a USB mass storage device. The medium and boot method to select depends on the system architecture and on whether the machine has a traditional BIOS or UEFI.

Procedure 4.1. Manually upgrading to SUSE Linux Enterprise Server 15 SP7

1. Select and prepare a boot medium, see Part I, "Installation preparation" in "Deployment Guide".
2. Insert the Unified Installer DVD for SUSE Linux Enterprise Server15 SP7 and boot your machine. A *Welcome* screen is displayed, followed by the boot screen.
3. To force the installer to only install packages from the DVD and not from network sources, add the boot option `media_upgrade=1`.
4. Start up the system by selecting *Upgrade* in the boot menu.
5. Proceed with the upgrade process as described in *the section called "Upgrading SUSE Linux Enterprise"*.

4.3. Starting the upgrade from a network source

To start an upgrade from a network installation source, make sure that the following requirements are met:

Requirements for upgrading from a network installation source

Network installation source

A network installation source is set up according to Chapter 18, Setting up a network installation source in "Deployment Guide".

Network connection and network services

Both the installation server and the target machine must have a functioning network connection. Required network services are:

- Domain Name Service
- DHCP (only needed for booting via PXE, IP can be set manually during setup)
- OpenSLP (optional)

Boot medium

A bootable SUSE Linux Enterprise DVD, ISO image or functioning PXE setup. For details about booting via PXE, see the section called "Preparing the target system for PXE boot" in "Deployment Guide". Refer to Chapter 13, Remote installation in "Deployment Guide" for in-depth information on starting the upgrade from a remote server.

4.3.1. Manually upgrading via network installation source—booting from DVD

This procedure describes booting from a DVD as an example, but you can also use another local installation medium like an ISO image on a USB mass storage device. The way to select the boot method and to start up the system from the medium depends on the system architecture and on whether the machine has a traditional BIOS or UEFI. For details, see the links below.

1. Insert the Unified Installer DVD for SUSE Linux Enterprise Server15 SP7 and boot your machine. A *Welcome* screen is displayed, followed by the boot screen.

2. Select the type of network installation source you want to use (FTP, HTTP, NFS, SMB, or SLP). Usually you get this choice by pressing `F4`, but in case your machine is equipped with UEFI instead of a traditional BIOS, you may need to manually adjust boot parameters. For details, see Chapter 9, Boot parameters in "Deployment Guide" and Chapter 10, Installation steps in "Deployment Guide".

3. Proceed with the upgrade process as described in *the section called "Upgrading SUSE Linux Enterprise"*.

4.3.2. Manually upgrading via network installation source—booting via PXE

To perform an upgrade from a network installation source using PXE boot, proceed as follows:

1. Adjust the setup of your DHCP server to provide the address information needed for booting via PXE. For details, see Procedure 19.0, "" in "Deployment Guide".

2. Set up a TFTP server to hold the boot image needed for booting via PXE. Use the Installer DVD for SUSE Linux Enterprise Server15 SP7 for this or follow the instructions in the section called "Setting up a TFTP server" in "Deployment Guide".

3. Prepare PXE Boot and Wake-on-LAN on the target machine.

4. Initiate the boot of the target system and use VNC to remotely connect to the installation routine running on this machine. For more information, see the section called "Monitoring installation via VNC" in "Deployment Guide".

5. Proceed with the upgrade process as described in *the section called "Upgrading SUSE Linux Enterprise"*.

4.4. Upgrading SUSE Linux Enterprise

Before you upgrade your system, read *Chapter 3, Preparing the upgrade* first. To perform an automated migration, proceed as follows:

> **SUSE Customer Center and Internet connection**
>
> If the system you want to upgrade is registered with the SUSE Customer Center, make sure to have an Internet connection during the following procedure.

1. After you have booted (either from an installation medium or the network), select the *Upgrade* entry on the boot screen.

> **Wrong choice may lead to data loss**
>
> Make sure you select *Upgrade* at this point. If you select *Installation* by mistake, your data partition will be overwritten with a fresh installation.

   YaST starts the installation system.

2. On the *Welcome* screen, choose *Language* and *Keyboard*. Proceed with *Next*.

   YaST checks your partitions for already installed SUSE Linux Enterprise systems.

3. On the *Select for Upgrade* screen, select the partition to upgrade and click *Next*.

4. YaST mounts the selected partition and displays the license agreement for the upgraded product. To continue, accept the license.

5. On the *Previously Used Repositories* screen, adjust the status of the repositories. By default all repositories are removed. If you have not added any custom repositories, do not change the settings. The packages for the upgrade will be installed from DVD, and you can optionally enable the default online repositories in the next step.

   If you have custom repositories, you have two choices:

   ◦ Leave the repository in state Removed. Software that was installed from this repository will be removed during the upgrade. Use this method if no version of the repository that matches the new release is available.

   ◦ Update and enable the repository if it matches the new release. Change its URL by clicking the repository in the list, and then click *Change*. Enable the repository by checking *Toggle Status* until it is set to *Enable*.

   Do not keep repositories from the previous release, as the system may be unstable or not work at all. Then proceed by clicking *Next*.

6. The next step depends on whether the upgraded system is registered with the SUSE Customer Center or not.

   1. If the system is not registered with the SUSE Customer Center, YaST displays a pop-up message suggesting using a second installation medium, the SLE-15-SP7-Full-*ARCH*-GM-media1.iso image.

      If you do not have that medium, the system cannot be upgraded without registration.

   2. If the system is registered with the SUSE Customer Center, YaST will show possible migration targets and a summary.

      Select one migration target from the list and proceed with *Next*.

7. In the next dialog you can optionally add an additional installation medium. If you have additional installation media, activate the *I would like to install an additional Add On Product* option and specify the media type.

8. Review the *Installation Settings* for the upgrade.

9. If all settings are according to your wishes, start the installation and removal procedure by clicking *Update*.

   Upgrade failure on SMT clients

   If the machine to upgrade is an SMT client, and the upgrade fails, see *Procedure 3.1, "Deregistering a SUSE Linux Enterprise client from an SMT server"* and restart the upgrade procedure afterward.

10. After the upgrade process has finished successfully, perform the post-upgrade steps described in *Chapter 6, Finishing the upgrade*.

4.5. Upgrading with AutoYaST

The upgrade process can be executed automatically. For details, see the section called "Upgrade" in "AutoYaST Guide".

4.6. Upgrading with SUSE Multi-Linux Manager

SUSE Multi-Linux Manager is a server solution for providing updates, patches, and security fixes for SUSE Linux Enterprise clients. It comes with a set of tools and a Web-based user interface for management tasks. See https://www.suse.com/products/multi-linux-manager/ for more information about SUSE Multi-Linux Manager.

You can perform a system upgrade using SUSE Multi-Linux Manager. The AutoYaST technology allows upgrades from one major version to the next.

If your machine is managed by SUSE Multi-Linux Manager, update it as described in the SUSE Multi-Linux Manager documentation. The *Client Migration* procedure is described in the *SUSE Multi-Linux Manager Upgrade Guide*, available at https://documentation.suse.com/multi-linux-manager/.

4.7. Updating registration status after rollback

When performing a service pack upgrade, it is necessary to change the configuration on the registration server to provide access to the new repositories. If the upgrade process is interrupted or reverted (via restoring from a backup or snapshot), the information on the registration server is inconsistent with the status of the system. This may lead to you being prevented from accessing update repositories or to wrong repositories being used on the client.

When a rollback is done via Snapper, the system notifies the registration server to ensure access to the correct repositories is set up during the boot process. If the system was restored with another method, or the communication with the registration server fails, trigger the rollback on the client manually. An example for manually triggering a rollback can be that the server was not accessible because of network issues. To do a rollback, execute:

```
>sudo snapper rollback
```

We suggest always checking that the correct repositories are set up on the system, especially after refreshing the service using:

```
>sudo zypper ref -s
```

This functionality is available in the `rollback-helper` package.

4.8. Registering your system

If the system was not registered before running the upgrade you can register your system at any time using the *Product Registration* module in YaST.

Registering your systems has these advantages:

- Eligibility for support
- Availability of security updates and bug fixes
- Access to SUSE Customer Center

1. Start YaST and select *Software > Product Registration* to open the *Registration* dialog.

2. Provide the *E-mail* address associated with the SUSE account you or your organization uses to manage subscriptions. In case you do not have a SUSE account yet, go to the SUSE Customer Center home page (https://scc.suse.com/) to create one.

3. Enter the *Registration Code* you received with your copy of SUSE Linux Enterprise Server.

4. If one or more local registration servers are available on your network, you can choose one of them from a list.

5. To start the registration, proceed with *Next*.

   After successful registration, YaST lists extensions, add-ons, and modules that are available for your system. To select and install them, proceed with the section called "Managing modules and extensions in a running system" in "Deployment Guide".

Chapter 5. Upgrading online

5.1. Conceptual overview

SUSE releases new service packs for the SUSE Linux Enterprise family at regular intervals. To make it easy for customers to migrate to a new service pack and minimize downtime, SUSE supports migrating online while the system is running.

Starting with SLE 12, YaST Wagon has been replaced by YaST migration (GUI) and Zypper migration (command line). This has the following advantages:

- The system is always in a defined state until the first RPM is updated.
- Canceling is possible until the first RPM is updated.
- Simple recovery if there is an error.
- It is possible to do a "rollback" via system tools—no backup or restore needed.
- Use of all active repositories.
- The ability to skip a service pack

Online migration not supported for major releases

The online migration is *only* supported for migrating between service packs. Online migration is *not supported* for upgrading to new major releases. For details, see *Chapter 2, Upgrade paths and methods*.

Use the offline migration to upgrade to a new major release. For details, see *Chapter 4, Upgrading offline*.

Upgrading SUSE Multi-Linux Manager clients

If the system to upgrade is a SUSE Multi-Linux Manager client, it cannot be upgraded by YaST online migration or `zypper migration`. Use the *Client Migration* procedure instead. It is described in the *SUSE Multi-Linux Manager Upgrade Guide*.

5.2. Service pack migration workflow

A service pack migration can be executed by either YaST, `zypper`, or AutoYaST.

Before you can start a service pack migration, your system must be registered at the SUSE Customer Center or a local RMT server. SUSE Multi-Linux Manager can also be used.

Regardless of the method, a service pack migration consists of the following steps:

1. Find possible migration targets on your registered systems.
2. Select one migration target.
3. Request and enable new repositories.
4. Run the migration.

The list of migration targets depends on the products you have installed and registered. If you have an extension installed for which the new SP is not yet available, it could be that no migration target is offered to you.

The list of migration targets available for your host will always be retrieved from the SUSE Customer Center and depend on products or extensions installed.

5.3. Canceling service pack migration

A service pack migration can only be canceled at specific stages during the migration process:

1. Until the package upgrade starts, there are only minimal changes on the system, such as changes to services and repositories. Restore `/etc/zypp/repos.d/*` to revert to the previous state.
2. After the package upgrade starts, you can revert to the previous state by using a Snapper snapshot (see Chapter 10, System recovery and snapshot management with Snapper in "Administration Guide").
3. After the migration target was selected, SUSE Customer Center changes the repository data. To revert this state manually, use **SUSEConnect**`--rollback`.

5.4. Upgrading with the online migration tool (YaST)

To perform a service pack migration with YaST, use the *Online Migration* tool. By default, YaST does not install any packages from a third-party repository. If a package was installed from a third-party repository, YaST prevents packages from being replaced with the same package coming from SUSE.

> ### Reduce installation size
>
> When performing the Service Pack migration, YaST will install all recommended packages. Especially in the case of custom minimal installations, this may increase the installation size of the system significantly.
>
> To change this default behavior and allow only required packages, adjust the `solver.onlyRequires` option in `/etc/zypp/zypp.conf`.
>
> ```
> solver.onlyRequires = true
> ```
>
> Additionally, edit the file `/etc/zypp/zypper.conf` and change the `installRecommends` option.
>
> ```
> installRecommends=false
> ```
>
> This changes the behavior of all package operations, such as the installation of patches or new packages. To change the behavior of Zypper for a single invocation, use the parameter `--no-recommends`.

To start the service pack migration, do the following:

1. Deactivate all unused extensions on your registration server to avoid future dependency conflicts. If you forget an extension, YaST will later detect unused extension repositories and deactivate them.

2. If you are logged in to a GNOME session running on the machine you are going to update, switch to a text console. Running the update from within a GNOME session is not recommended. Note that this does not apply when being logged in from a remote machine (unless you are running a VNC session with GNOME).

3. Run YaST online update to get the latest package updates for your system.

4. Install the package `yast2-migration` and its dependencies (in YaST under *Software > Software Management*).

5. Restart YaST, otherwise the newly installed module will not be shown in the control center.

6. In YaST, choose *Online Migration* (depending on the version of SUSE Linux Enterprise Server that you are upgrading from, this module is categorized under either *System* or *Software*). YaST will show possible migration targets and a summary. If more than one migration target is available for your system, select one from the list.

7. Select one migration target from the list and proceed with *Next*.

8. If the migration tool offers update repositories, it is recommended to proceed with *Yes*.

9. If the online migration tool finds obsolete repositories from DVD or a local server, it is highly recommended to disable them. Obsolete repositories are for a previous service pack. Old repositories from SUSE Customer Center or RMT are removed automatically.

If the registration server does not offer migrations for a module or extension, its repository configuration will remain unchanged. This usually happens with 3rd party repositories such as the *NVIDIA Compute Module* that are not specific to a product version or service pack. If necessary, you can manually check the repository configuration after the migration.

10. Check the summary and proceed with the migration by clicking *Next*. Confirm with *Start Update*.

11. After the successful migration restart your system.

5.5. Upgrading with Zypper

To perform a service pack migration with Zypper, use the command-line tool **zypper**migration from the package `zypper-migration-plugin`.

> **Reduce installation size**
>
> When performing the Service Pack migration, YaST will install all recommended packages. Especially in the case of custom minimal installations, this may increase the installation size of the system significantly.
>
> To change this default behavior and allow only required packages, adjust the `solver.onlyRequires` option in `/etc/zypp/zypp.conf`.
>
> ```
> solver.onlyRequires = true
> ```
>
> Additionally, edit the file `/etc/zypp/zypper.conf` and change the `installRecommends` option.
>
> ```
> installRecommends=false
> ```
>
> This changes the behavior of all package operations, such as the installation of patches or new packages. To change the behavior of Zypper for a single invocation, use the parameter `--no-recommends`.

To start the service pack migration, do the following:

1. If you are logged in to a GNOME session running on the machine you are going to update, switch to a text console. Running the update from within a GNOME session is not recommended. Note that this does not apply when being logged in from a remote machine (unless you are running a VNC session with GNOME).

2. Register your SUSE Linux Enterprise machine if you have not done so:

   ```
   >sudoSUSEConnect --regcode YOUR_REGISTRATION_CODE
   ```

3. Start the migration:

   ```
   >sudozypper migration
   ```

Some notes about the migration process:

- If more than one migration target is available for your system, Zypper allows you to select one SP from the list. This is the same as skipping one or more SPs. Keep in mind, online migration for base products (SLES, SLED) remains available only between the SPs of a major version.

- By default, Zypper uses the option `--no-allow-vendor-change` which is passed to **zypper**dup. If a package was installed from a third-party repository, this option prevents packages from being replaced with the same package coming from SUSE.

- If Zypper finds obsolete repositories coming from DVD or a local server, it is highly recommended to disable them. Old SUSE Customer Center or RMT repositories are removed automatically.

4. Review all the changes, especially the packages that are going to be removed. Proceed by typing y (the exact number of packages to upgrade can vary on your system):

```
266 packages to upgrade, 54 to downgrade, 17 new, 8 to reinstall, 5 to
remove, 1 to change arch.
Overall download size: 285.1 MiB. Already cached: 0 B  After the operation,
additional 139.8 MiB will be used.
Continue? [y/n/? shows all options] (y):
```

Use the `Shift`–`Page Up` or `Shift`–`Page Down` keys to scroll in your shell.

5. After successful migration restart your system.

5.6. Upgrading with plain Zypper

If your system is not registered because you do not have access to the Internet or a registration server, migrating to a new service pack is not possible with YaST Migration or **zypper migration**. In this case you can still migrate to a new service pack with plain Zypper and some manual interactions.

> **!**
>
> **For unregistered systems only**
>
> This migration path to a new service pack is *only* supported for unregistered systems that do not have access to the Internet or a registration server. This may, for example, be the case for machines in a specially protected network. If you have a registered system, use YaST or Zypper migration.

Installation sources

This migration path requires that the system you are going to migrate has access to the installation sources. For example, this can be done by setting up an RMT server or an SLP server.

It is also required that the system has access to an up-to-date update repository for the installed product version.

1. If you are logged in to a graphical session running on the machine you are going to migrate, log out of that session and switch to a text console. Running the update from within a graphical session is not recommended. Note that this does not apply when being logged in from a remote machine (unless you are running a VNC session with X).

2. Update the package management tools:

   ```
   >sudozypper patch --updatestack-only
   ```

3. Make sure that all SUSE Linux Enterprise Server repository configuration files in `/etc/zypp/repos.d/` use the variable `$releasever`:

   ```
   >grep baseurl /etc/zypp/repos.d/*.repo
   /etc/zypp/repos.d/rmt.repo:baseurl=https://rmt.example.com/repo/SUSE/
   Products/SLE-15-SP5-Product-SLES/x86_64/product/
   /etc/zypp/repos.d/updates.repo:baseurl=https://updates.suse.com/SUSE/
   Products/SLE-Product-SLES/$releasever/x86_64/product[...]
   ```

   In this example, the file `updates.repo` uses the variable, while `rmt.repo` hardcodes the version string `15-SP5`. To replace all occurrences of `15-SP5` with `$releasever` across all repository configuration files, run:

   ```
   >sudosed -i 's/15-SP5/${releasever}/g' /etc/zypp/repos.d/*.repo
   ```

   If necessary, repeat this command with different version strings to ensure all repository configuration files get updated.

4. Check if all repositories are configured correctly:

   ```
   >sudozypper --releasever=15-SP7 repos -u
   ```

   You should now see `15-SP7` in the repository URLs. Note that some third-party repositories may be unversioned. It is assumed that they work for all SUSE Linux Enterprise Server releases.

5. Switch and refresh all repositories to 15 SP7:

   ```
   >sudozypper --releasever=15-SP7 refresh -f -s
   ```

   In case updating a repository fails, double-check whether you entered the wrong URL. If the problem cannot be fixed, it is recommended to disable the failing repository.

6. Test the migration:

```
>sudozypper --releasever=15-SP7 dup -D --no-allow-vendor-change --no-
recommends
```

The parameter `-D` will perform a dry run that simulates the migration without actually changing the system. If problems occur, fix them before proceeding.

The option `-no-allow-vendor-change` prevents third-party packages from replacing RPM packages from the base system. The option `--no-recommends` ensures that packages deselected during initial installation will not be added again.

7. Execute the full distribution upgrade:

```
>sudozypper --releasever=15-SP7 dup --no-allow-vendor-change --no-
recommends
```

With the above command, zypper downloads all packages in advance—which is more reliable if your Internet connection may fail. To download and install packages in heaps, run:

```
>sudozypper zypper --releasever=15-SP7 dup --no-allow-vendor-change --no-
recommends --download-in-heaps
```

When the distribution update is finished, SUSE Linux Enterprise Server sets the `$releasever` variable to the new version and you no longer need to specify it with the `--releasever` option.

8. Reboot your system after successful migration.

5.7. Rolling back a service pack

If a service pack does not work for you, SUSE Linux Enterprise supports reverting the system to the state before the service pack migration was started. Prerequisite is a Btrfs root partition with snapshots enabled (this has been the default since SLES 12). See Chapter 10, System recovery and snapshot management with Snapper in "Administration Guide" for details.

1. Get a list of all Snapper snapshots:

```
>sudo snapper list
```

Review the output to locate the snapshot that was created immediately before the service pack migration was started. The column *Description* contains a corresponding statement and the snapshot is marked as `important` in the column *Userdata*. Memorize the snapshot number from the column # and its date from the column *Date*.

2. Reboot the system. From the boot menu, select *Start boot loader from a read-only snapshot* and then choose the snapshot with the date and number you memorized in the previous step. A second boot menu (the one from the snapshot) is loaded. Select the entry starting with SLES 15 SP7 and boot it.

3. The system boots into the previous state with the system partition mounted read-only. Log in as `root` and check whether you have chosen the correct snapshot. Also make sure

everything works as expected. Note that since the root file system is mounted read-only, restrictions in functionality may apply.

In case of problems or if you have booted the wrong snapshot, reboot and choose a different snapshot to boot from—up to this point no permanent changes have been made. If the snapshot is correct and works as expected, make the change permanent by running the following command:

```
>sudo snapper rollback
```

Reboot the machine. On the boot screen, choose the default boot entry to reboot into the reinstated system.

4. Check if the repository configuration has been properly reset. Furthermore, check if all products are properly registered. If either one is not the case, updating the system at a later point in time may no longer work, or the system may be updated using the wrong package repositories.

   Make sure the system can access the Internet before starting this procedure.

   1. Refresh services and repositories by running

      ```
      >sudo zypper ref -fs
      ```

   2. Get a list of active repositories by running

      ```
      >sudo zypper lr
      ```

      Carefully check the output of this command. No services and repositories that were added for the update should be listed. For example, if you are rolling back from SLES 15 SP7 to SLES15 GA, the list must contain the SLES15-GA repositories, and not the SLES15-SP7 repositories.

      If wrong repositories are listed, delete them and, if necessary, replace them with the versions matching your product or service pack version. For a list of repositories for the supported migration paths refer to *the section called "Module dependencies and lifecycles"*. (Note that manual intervention should not be necessary, as the repositories should be updated automatically, but it is a best practice to verify and make any necessary corrections.)

   3. Last, check the registration status for all products installed by running

      ```
      >sudo SUSEConnect --status
      ```

      All products should be reported as being Registered. If this is not the case, repair the registration by running

      ```
      >sudo SUSEConnect --rollback
      ```

Now you have successfully reverted the system to the state that was captured immediately before the service pack migration was started.

5.8. Upgrading with SUSE Multi-Linux Manager

SUSE Multi-Linux Manager is a server solution for providing updates, patches, and security fixes for SUSE Linux Enterprise clients. It comes with a set of tools and a Web-based user interface for management tasks. See https://www.suse.com/products/multi-linux-manager/ for more information about SUSE Multi-Linux Manager.

SP Migration allows migrating from one Service Pack (SP) to another within one major version (for example, from SLES 15 GA to SLES 15 SP7).

If your machine is managed by SUSE Multi-Linux Manager, update it as described in the SUSE Multi-Linux Manager documentation. The *Client Migration* procedure is described in the *SUSE Multi-Linux Manager Upgrade Guide*, available at https://documentation.suse.com/multi-linux-manager/.

5.9. Upgrading from openSUSE Leap to SUSE Linux Enterprise Server

You can upgrade an openSUSE Leap installation to SUSE Linux Enterprise Server. To find out which Leap versions are supported for migration, refer to *the section called "Supported upgrade and migration paths to SLES 15 SP7 "*.

> **Not all openSUSE packages can be migrated**
>
> openSUSE provides more packages than SUSE Linux Enterprise Server. Most of the additional packages are available through SUSE Package Hub and will be migrated. Any additional packages that are not available through SUSE Package Hub will no longer receive updates after the migration and should therefore be removed afterward.
>
> Make sure that all packages you need for operating your system are available in the SUSE Linux Enterprise Server and SUSE Package Hub repositories. For more information about SUSE Package Hub, refer to https://packagehub.suse.com/.

5.9.1. Upgrading with `yast2 migration`

The following procedure is similar to *the section called "Upgrading with the online migration tool (YaST)"*, but requires some additional steps. Before executing this procedure on a production system, we recommend to first run it on a test system that replicates your production setup.

Procedure 5.1. Upgrading openSUSE Leap to SUSE Linux Enterprise Server with with `yast2 migration`

To migrate from openSUSE Leap to SUSE Linux Enterprise Server, perform the following steps:

1. Close all unused applications and switch to a TTY, for example by pressing `Ctrl`–`Alt`–`F1`.
   Then log in as `root`.

2. Install the `yast2-migration` and `rollback-helper` packages:

   ```
   #zypper in yast2-migration rollback-helper
   ```

3. Enable the `rollback-helper` service:

   ```
   #systemctl enable rollback
   ```

4. Register the system with the SUSE Customer Center:

   ```
   #yast2 registration
   ```

5. Perform the migration:

   ```
   #yast2 migration
   ```

   In case of package conflicts, YaST presents a list of resolutions to choose from.

6. Reboot the system:

   ```
   #reboot
   ```

You have now successfully migrated your system to SUSE Linux Enterprise Server. Continue with *Chapter 6, Finishing the upgrade* and remove orphaned packages to ensure you are running a fully supported SUSE Linux Enterprise installation.

If you run into a problem after the migration, you can revert the migration like a service pack upgrade. For instructions, refer to *the section called "Rolling back a service pack"*.

5.9.2. Upgrading with `yast2 migration_sle`

A simplified migration from openSUSE Leap to SUSE Linux Enterprise Server is available as a technology preview as of Leap 15.4.

Procedure 5.2. Upgrading openSUSE Leap to SUSE Linux Enterprise Server with `yast2 migration_sle`

To migrate from openSUSE Leap to SUSE Linux Enterprise Server, perform the following steps:

1. Close all unused applications (recommended).

2. Install the `yast2-migration-sle` and `rollback-helper` packages:

   ```
   >sudozypper in yast2-migration-sle rollback-helper
   ```

3. Enable the `rollback-helper` service:

```
>sudosystemctl enable rollback
```

4. Open YaST and select *Software > Online Migration* or run:

```
>sudoyast2 migration_sle
```

The wizard will guide you through the migration process. If there are pending updates, they can be installed before registering the system. To register, enter your registration code and e-mail address. To register with a local RMT server, provide its URL instead of the registration code and leave the e-mail address empty.

After the system is registered, the SUSE Linux Enterprise Server repositories will be added and the SLE packages will be installed to replace the openSUSE ones.

5. Reboot the system:

```
>sudoreboot
```

You have now successfully migrated your system to SUSE Linux Enterprise Server. Continue with *Chapter 6, Finishing the upgrade* and remove orphaned packages to ensure you are running a fully supported SUSE Linux Enterprise installation.

If you run into a problem after the migration, you can revert the migration like a service pack upgrade. For instructions, refer to *the section called "Rolling back a service pack"*.

Chapter 6. Finishing the upgrade

6.1. Check for old packages

Use **zypper packages** to check for orphaned and unneeded packages.

Orphaned Packages are no longer available in any of the configured package repositories. They can no longer get updated and become unsupported.

For a list of orphaned packages, run:

```
>zypper packages --orphaned
```

Unneeded packages are dependencies of packages that have been installed either explicitly by the user or implicitly as part a pattern or product, and that have been removed in the meantime. They are usually no longer needed and should be removed, too.

For a list of unneeded packages, run:

```
>zypper packages --unneeded
```

> **Tip**
>
> To avoid unneeded packages, use **zypper rm** with the `--clean-deps` option or YaST with *Options > Clean up when deleting packages* enabled.

You can combine both lists into one:

```
>zypper packages --orphaned --unneeded
```

Use these lists to determine which packages are still needed and which can be safely removed.

> **Do not remove packages you need**
>
> If packages are renamed or removed from a pattern or product, **zypper** may no longer consider them explicitly installed and mark them as unneeded, even though they are still crucial for your installation.
>
> Carefully review the list of packages you are removing.

To remove all orphaned and unneeded packages with a single command, run:

```
>sudozypper rm $(zypper --no-refresh packages --orphaned --unneeded | gawk
'{print $5}' | tail -n +5)
```

Exclude a single package or pattern from being uninstalled:

```
>sudozypper rm $(zypper --no-refresh packages --orphaned --unneeded | gawk
'{print $5}' | tail -n +5 | grep -v PACKAGE_TO_EXCLUDE)
```

Exclude multiple packages defined in a text file, separated by a newline:

```
>sudozypper rm $(zypper --no-refresh packages --orphaned --unneeded | gawk
'{print $5}' | tail -n +5 | grep -v -f /PACKAGES/TO/KEEP.txt)
```

6.2. Review your configuration files

Check for any `*.rpmnew` and `*.rpmsave` files. When an upgrade includes changes to a default configuration file that has been altered after package installation, instead of overwriting the file, one of these file types is created. While `*.rpmnew` contains the new default configuration and leaves your altered file untouched, `*.rpmsave` is a copy of your altered configuration that has been replaced by the new default file.

If you find any of these files, examine their content and merge desirable changes. You do not need to search the whole file system, only the `/etc` directory. Use the following command:

```
>find /etc/ -name "*.rpmnew" -o -name "*.rpmsave"
```

6.3. Enable the `Python 3` module

SUSE Linux Enterprise Server 15 uses Python 3.6 by default. Python 3.9 was added in SLES 15 SP3 as a more recent alternative. This version is no longer supported as of SLES 15 SP4. Instead, recent Python versions with important updates and security fixes are available through the `Python 3` module.

If you installed Python 3.9 under SUSE Linux Enterprise Server 15 SP3, enable the `Python 3` module with:

```
>sudoSUSEConnect -p sle-module-python3/15.7/x86_64.
```

Alternatively, you can return to the default Python version by removing 3.9 with `zypper remove -u python39`.

6.4. Reformat XFS v4 devices

SUSE Linux Enterprise Server supports the "on-disk format" (v5) of the XFS file system. The main advantages of this format are automatic checksums of all XFS metadata, file type support, and support for a larger number of access control lists for a file.

Note that this format is not supported by SUSE Linux Enterprise kernels older than version 3.12, by `xfsprogs` older than version 3.2.0, and GRUB 2 versions released before SUSE Linux Enterprise 12.

V4 is deprecated

XFS is deprecating file systems with the V4 format. This file system format was created by the command:

```
>sudo mkfs.xfs -m crc=0 DEVICE
```

The format was used in SLE 11 and older releases, and it currently creates a warning message by **dmesg**:

```
Deprecated V4 format (crc=0) will not be supported after September 2030
```

If you see the message above in the output of the **dmesg** command, it is recommended that you update your file system to the V5 format:

1. Back up your data to another device.
2. Create the file system on the device.

   ```
   >sudo mkfs.xfs -m crc=1 DEVICE
   ```

3. Restore the data from the backup on the updated device.

Chapter 7. Backports of source code

7.1. Reasons for backporting

Upstream developers are primarily concerned with advancing the software they develop. Often they combine fixing bugs with introducing new features which have not yet received extensive testing and which may introduce new bugs.

For distribution developers, it is important to distinguish between:

- bugfixes with a limited potential for disrupting functionality; and
- changes that may disrupt existing functionality.

Usually, distribution developers do not follow all upstream changes when a package has become part of a released distribution. Usually they stick instead with the upstream version that they initially released and create patches based on upstream changes to fix bugs. This practice is known as *backporting*.

Distribution developers generally will only introduce a newer version of software in two cases:

- when the changes between their packages and the upstream versions have become so large that backporting is no longer feasible, or
- for software that inherently ages badly, like anti-malware software.

SUSE uses backports extensively as we strike a good balance between several concerns for enterprise software. The most important of them are:

- Having stable interfaces (APIs) that software vendors can rely on when building products for use on SUSE's enterprise products.
- Ensuring that packages used in the release of SUSE's enterprise products are of the highest quality and have been thoroughly tested, both in themselves and as part of the whole enterprise product.
- Maintaining the various certifications of SUSE's enterprise products by other vendors, like certifications for Oracle or SAP products.
- Allowing SUSE's developers to focus on making the next product version, rather than spreading their focus thinly across a wide range of releases.
- Keeping a clear view of what is in a particular enterprise release, so that our support can provide accurate and timely information about it.

7.2. Reasons against backports

It is a general policy rule that no new upstream versions of a package are introduced into our enterprise products. This rule is not an absolute rule however. For certain types of packages, in

particular anti-virus software, security concerns weigh heavier than the conservative approach that is preferable from the perspective of quality assurance. For packages in that class, occasionally newer versions are introduced into a released version of an enterprise product line.

Sometimes also for other types of packages the choice is made to introduce a new version rather than a backport. This is done when producing a backport is not economically feasible or when there is a very relevant technical reason to introduce the newer version.

7.3. The implications of backports for interpreting version numbers

Because of the practice of backporting, one cannot simply compare version numbers to determine whether a SUSE package contains a fix for a particular issue or has had a particular feature added to it. With backporting, the upstream part of a SUSE package's version number merely indicates what upstream version the SUSE package is based on. It may contain bug fixes and features that are not in the corresponding upstream release, but that have been backported into the SUSE package.

One particular area where this limited value of version numbers when backporting is involved can cause problems is with security scanning tools. Some security vulnerability scanning tools (or particular tests in such tools) operate solely on version information. These tools and tests are therefore prone to generating "false positives" (when a piece of software is incorrectly identified as vulnerable) when backports are involved. When evaluating reports from security scanning tools, always check whether an entry is based on a version number or on an actual vulnerability test.

7.4. Checking for fixed bugs and backported features

Information about backported bug fixes and features is stored in several locations:

- The package's changelog:

  ```
  >rpm -q --changelog name-of-installed-package>rpm -qp --changelog packagefi
  le.rpmpackagefile.rpm
  ```

  The output briefly documents the change history of the package.

- The package changelog may contain entries like `bsc#1234` ("*B*ugzilla*S*use. *C*om") that refer to bugs in SUSE's Bugzilla tracking system or links to other bugtracking systems. Because of confidentiality policies, not all such information may be accessible to you.

- A package may contain a `/usr/share/doc/PACKAGENAME/README.SUSE` file which contains general, high-level information specific to the SUSE package.

- The RPM source package contains the patches that were applied during the building of the regular binary RPMs as separate files that can be interpreted if you are familiar with reading source code. See the section called "Installing or downloading source packages" in "Administration Guide" for installing sources of SUSE Linux Enterprise software. See the section called "Installing and compiling source packages" in "Administration Guide" for

building packages on SUSE Linux Enterprise. See the Maximum RPM book for details about software package builds for SUSE Linux Enterprise.

- For security bug fixes, consult the SUSE security announcements. These often refer to bugs through standardized names like `CAN-2005-2495` which are maintained by the Common Vulnerabilities and Exposures (CVE) project.

Appendix A. GNU licenses

This appendix contains the GNU Free Documentation License version 1.2.

A.1. GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall

subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

1. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

2. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

3. State on the Title page the name of the publisher of the Modified Version, as the publisher.

4. Preserve all the copyright notices of the Document.

5. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

6. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

7. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

8. Include an unaltered copy of this License.

9. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

10. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years

before the Document itself, or if the original publisher of the version it refers to gives permission.

11. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

12. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

13. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

14. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

15. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special

permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See https://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.