SUSE

SUSE Linux Enterprise Server 15 SP7

Release Notes

SUSE Linux Enterprise Server is a modern, modular operating system for both multimodal and traditional IT. This document provides a high-level overview of features, capabilities, and limitations of SUSE Linux Enterprise Server 15 SP7 and highlights important product updates.

These release notes are updated periodically. The latest version of these release notes is always available at https://www.suse.com/releasenotes. General documentation can be found at https://documentation.suse.com/sles/15-SP7.

Publication Date: 2026-10-01, Version: 15.7.20261001

Contents

1 About the release notes 3

2 SUSE Linux Enterprise Server 3

3 Modules, extensions, and related products 18

4 Installation and upgrade 20

5 Changes affecting all architectures 26

6 AMD64/Intel 64-specific changes (x86-64) 60

7 POWER-specific changes (ppc64le) 61

8 IBM Z-specific changes (s390x) 63

9 Arm 64-bit-specific changes (AArch64) 64

10 Removed and deprecated features and packages 69

11 Obtaining source code 71

12 Legal notices 71

13 Changelog for 15 SP7 73

14 Kernel parameter changes 81

1 About the release notes

These Release Notes are identical across all architectures, and the most recent version is always available online at https://www.suse.com/releasenotes.

Entries are only listed once but they can be referenced in several places if they are important and belong to more than one section.

Release notes usually only list changes that happened between two subsequent releases. Certain important entries from the release notes of previous product versions are repeated. To make these entries easier to identify, they contain a note to that effect.

However, repeated entries are provided as a courtesy only. Therefore, if you are skipping one or more service packs, check the release notes of the skipped service packs as well. If you are only reading the release notes of the current release, you could miss important changes.

2 SUSE Linux Enterprise Server

SUSE Linux Enterprise Server 15 SP7 is a multimodal operating system that paves the way for IT transformation in the software-defined era. It is a modern and modular OS that helps simplify multimodal IT, makes traditional IT infrastructure efficient and provides an engaging platform for developers. As a result, you can easily deploy and transition business-critical workloads across on-premises and public cloud environments.

SUSE Linux Enterprise Server 15 SP7, with its multimodal design, helps organizations transform their IT landscape by bridging traditional and software-defined infrastructure.

2.1 Interoperability and hardware support

Designed for interoperability, SUSE Linux Enterprise Server integrates into classical Unix and Windows environments, supports open standard interfaces for systems management, and has been certified for IPv6 compatibility.

This modular, general-purpose operating system runs on four processor architectures and is available with optional extensions that provide advanced capabilities for tasks such as real-time computing and high-availability clustering.

SUSE Linux Enterprise Server is optimized to run as a high-performance guest on leading hypervisors. This makes SUSE Linux Enterprise Server the perfect guest operating system for virtual computing.

2.2 What is new?

2.2.1 General changes in SLE 15

SUSE Linux Enterprise Server 15 introduces many innovative changes compared to SUSE Linux Enterprise Server 12. The most important changes are listed below.

Migration from openSUSE Leap to SUSE Linux Enterprise Server

SLE 15 SP2 and later support migrating from openSUSE Leap 15 to SUSE Linux Enterprise Server 15. Even if you decide to start out with the free community distribution, you can later easily upgrade to a distribution with enterprise-class support. For more information, see the *Upgrade Guide* at https://documentation.suse.com/sles/15-SP7/html/SLES-all/cha-upgrade-online.html#sec-upgrade-online-opensuse-to-sle.

Extended package search

Use the new Zypper command `zypper search-packages` to search across all SUSE repositories available for your product, even if they are not yet enabled. For more information see *Section 5.14.4, "Searching packages across all SLE modules"*.

Software Development Kit

In SLE 15, packages formerly shipped as part of the Software Development Kit are now integrated into the products. Development packages are packaged alongside other packages. In addition, the *Development Tools* module contains tools for development.

RMT replaces SMT

SMT (Subscription Management Tool) has been removed. Instead, RMT (Repository Mirroring Tool) now allows mirroring SUSE repositories and custom repositories. You can then register systems directly with RMT. In environments with tightened security, RMT can also proxy other RMT servers. If you are planning to migrate SLE 12 clients to version 15, RMT is the supported product to handle such migrations. If you still need to use SMT for these migrations, beware that the migrated clients will have *all* installation modules enabled. For more information see *Section 4.2.7, "SMT has been replaced by RMT"*.

Media changes

The *Unified Installer* and *Packages* media known from SUSE Linux Enterprise Server 15 SP1 have been replaced by the following media:

- **Online Installation Medium:** Allows installing all SUSE Linux Enterprise 15 products. Packages are fetched from online repositories. This type of installation requires a registration key. Available SLE modules are listed in *Section 3.1, "Modules in the SLE 15 SP7 product line"*.
- **Full Installation Medium:** Allows installing all SUSE Linux Enterprise Server 15 products without a network connection. This medium contains all packages from all SLE modules. SLE modules need to be enabled manually during installation. RMT (Repository Mirroring Tool) and SUSE Multi-Linux Manager provide additional options for disconnected or managed installations.

SLE HPC product removal

Instead of a separate product, HPC is now available as a module in SUSE Linux Enterprise Server. For more information see *Section 2.2.4, "SLE HPC HPC no longer a separate product"*.

MAJOR UPDATES TO THE SOFTWARE SELECTION:

Salt

SLE 15 SP7 can be managed via Salt, making it integrate better with modern management solutions such as SUSE Multi-Linux Manager.

Python 3

As the first enterprise distribution, SLE 15 offers full support for Python 3 development in addition to Python 2.

Directory Server

389 Directory Server replaces OpenLDAP as the LDAP directory service.

2.2.2 Changes in 15 SP7

SUSE Linux Enterprise Server 15 SP7 introduces changes compared to SUSE Linux Enterprise Server 15 SP6. The most important changes are listed below:

2.2.3 Package and module changes in 15 SP7

The full list of changed packages compared to 15 SP6 can be seen at this URL:

- https://documentation.suse.com/package-lists/sle/15-SP7/package-changes_SLE-15-SP6-GA_SLE-15-SP7-GA.txt

The full list of changed modules compared to 15 SP6 can be seen at this URL:

- https://documentation.suse.com/package-lists/sle/15-SP7/module-changes_SLE-15-SP6-GA_SLE-15-SP7-GA.txt

2.2.4 SLE HPC HPC no longer a separate product

As of 15 SP7, SUSE Linux Enterprise High Performance Computing is no longer a separate product. As a result:

- the HPC Module can now be enabled in SUSE Linux Enterprise Server
- when migrating from SUSE Linux Enterprise High Performance Computing 15 SP3, SP4, and SP5, only SUSE Linux Enterprise Server 15 SP6 will be available as migration target. The result of such a migration will be an installation of SUSE Linux Enterprise Server with all the previously enabled modules.

The SLE HPC release notes are maintained separately as a supplement to the SLES release notes. For detailed information about packages and changes in the HPC Module, see the separate SUSE Linux Enterprise High Performance Computing Release Notes at https://documentation.suse.com/releasenotes/sle-hpc/15-SP7/index.html.

Modules

For an HPC installation the user should enable the following modules:

- `Development Tools Module`
- `HPC Module`

On SUSE Linux Enterprise Server system, make sure the following modules are all enabled:

- `Server Application Module`
- `Web and Scripting Module`

- `HPC Module`
- `Desktop Applications Module`
- `Development Tools Module`

Roles

The HPC system roles are no longer available:

- HPC Management Server (Head Node)
- HPC Compute Node
- HPC Login and Development Node

It is recommended to start with a `Text Mode` or `Minimal System` istallation. The admin should make sure that the system is partitioned to the respective requirements and the firewall is configured appropriately. Also, the admin should select the software components required. This may include `slurm` for the management server, `slurm-node` for the compute nodes. For login and compute nodes the pattern HPC Modularized Libraries (`patterns-hpc-libraries`) is available.

2.3 Important sections of this document

If you are upgrading from a previous SUSE Linux Enterprise Server release, you should review at least the following sections:

- *Section 2.7, "Support statement for SUSE Linux Enterprise Server"*
- *Section 4.2, "Upgrade-related notes"*
- *Section 5, "Changes affecting all architectures"*

2.4 Security, standards, and certification

SUSE Linux Enterprise Server 15 SP7 will be submitted for Common Criteria certification but will not be submitted for NIST FIPS 140-3 certification.

For more information about certification, see https://www.suse.com/support/security/certifications/.

2.5 Documentation and other information

2.5.1 Available on the product media

- Read the READMEs on the media.
- Get the detailed change log information about a particular package from the RPM (where `FILENAME.rpm` is the name of the RPM):

  ```
  rpm --changelog -qp FILENAME.rpm
  ```

- Check the `ChangeLog` file in the top level of the installation medium for a chronological log of all changes made to the updated packages.
- Find more information in the `docu` directory of the installation medium of SUSE Linux Enterprise Server 15 SP7. This directory includes PDF versions of the SUSE Linux Enterprise Server 15 SP7 Installation Quick Start Guide.

2.5.2 Online documentation

- For the most up-to-date version of the documentation for SUSE Linux Enterprise Server 15 SP7, see https://documentation.suse.com/sles/15-SP7.
- Find change logs for public cloud images at the Public Cloud Information Tracker (PINT) at https://pint.suse.com/.

2.6 Support and life cycle

SUSE Linux Enterprise Server is backed by award-winning support from SUSE, an established technology leader with a proven history of delivering enterprise-quality support services.

The current version (SP7) will be fully maintained and supported until 31 Jul 2034.

If you need additional time to design, validate and test your upgrade plans, Long Term Service Pack Support can extend the support duration. You can buy an additional 12 to 36 months in twelve month increments. This means that you can receive support up to Dec 2037.

For more information, see the pages Support Policy (https://www.suse.com/support/policy.html) and Long Term Service Pack Support (https://www.suse.com/support/programs/long-term-service-pack-support.html).

2.6.1 Quarterly updates

SUSE provides quarterly updates for SUSE Linux Enterprise Server 15 SP7 until the end of General Support on 31 Jul 2031. SUSE refreshes the installation media, virtual machine (VM) images, and public cloud images at least quarterly.

2.6.2 Specific component lifecycles

Some packages and components shipped with SUSE Linux Enterprise Server have lifecycles that are not strictly aligned with the lifecycle of the product or its service packs. Some components (such as Java or Python) have specific, independent lifecycles. Others (such as Go, Rust, Node.js, and GCC) are updated in the released service packs to keep up with security and upstream developments.

For overall lifecycle information for SUSE products, refer to the SUSE Product Lifecycle page at https://www.suse.com/lifecycle/. For details on module-specific package lifecycles, see the SUSE Linux Enterprise Server 15 Modules Lifecycle page at https://scc.suse.com/docs/lifecycle/sle/15/modules.

2.6.2.1 Java lifecycle support

Java is not supported in Reactive LTSS and Extreme LTSS offerings. IBM Java 8 is available again in the *Legacy Module* of SUSE Linux Enterprise Server 15 SP7. SUSE does not support IBM Java. To get support, you must have a support contract with IBM.

The following table lists the support lifecycles for Java versions available on SUSE Linux Enterprise Server 15:

TABLE 1: JAVA LIFECYCLE SUPPORT ON SUSE LINUX ENTERPRISE SERVER 15

Name (Package Name)	Version	SLES SPs	Support Level	Support End	Note
IBM Java (`java-1_8_0-ibm`)	1.8.0	SP0–SP7 (Legacy Module)	External	December 2030	SUSE gives no support. IBM makes free public updates available until 2030.

Name (Package Name)	Version	SLES SPs	Support Level	Support End	Note
OpenJDK (`java-1_8_0-openjdk`)	1.8.0	SP0–SP7 (Legacy Module)	SUSE, L3	December 2026	Aligned with SLES 15 SP4 LTSS end.
OpenJDK (`java-11-openjdk`)	11	SP1–SP5 (Basesystem), SP6–SP7 (Legacy Module)	SUSE, L3	December 2027	Aligned with SLES 15 SP5 LTSS end.
OpenJDK (`java-17-openjdk`)	17	SP4–SP5 (Basesystem), SP6–SP7 (Legacy Module)	SUSE, L3	December 2027	Aligned with SLES 15 SP5 LTSS end.
OpenJDK (`java-21-openjdk`)	21	SP6–SP7	SUSE, L3	July 2034	Aligned with SLES 15 SP7 LTSS end.
OpenJDK (`java-25-openjdk`)	25	SP7	SUSE, L3	October 2033	Aligned with the OpenJDK 25 support end in SLES 16.

2.6.2.2 Python lifecycle support

Python 2.7 was deprecated in SLES 15 SP0 and removed entirely in SP4. The initial end of support for Python 2.7 was December 31, 2023 in SLES 15 SP3.

Python 3.6 remains the default system interpreter across all Service Packs. It is supported for the full lifetime of the SLES 15 product family until July 2034.

Recent Python versions (such as Python 3.9 in SP3, 3.10 in SP4, 3.11 in SP5, 3.12 in SP6, and 3.13 in SP7) are provided via the dedicated **Python 3 Module**. Only the system interpreter and the latest shipped interpreter are supported simultaneously per Service Pack. These recent Python versions are exempt from Reactive LTSS and XLSS.

2.6.2.3 Node.js lifecycle support

Before LTSS, up to three upstream major versions of `nodejs` are supported concurrently per Service Pack. During the LTSS phase, only the latest version of `nodejs` is supported.

The following table lists the support lifecycles for Node.js versions available on SUSE Linux Enterprise Server 15:

TABLE 2: NODE.JS LIFECYCLE SUPPORT ON SUSE LINUX ENTERPRISE SERVER 15

Version	Release Date	Upstream EOL	Inclusion in SLES 15	SUSE EOL
22.x	October 2024	April 2026	SP7 GA	End of 2027
24.x	October 2025	April 2027	End of 2025	End of 2028
26.x	October 2026	April 2028	End of 2026	End of 2029
28.x	October 2027	April 2029	End of 2027	End of 2030
30.x	October 2028	April 2030	End of 2028	July 2031 (General Support end)
32.x	October 2029	April 2031	End of 2029	July 2031 (General Support end)
34.x	October 2030	April 2032	End of 2030	July 2034 (LTSS end)

2.6.2.4 Database lifecycle support

MariaDB, PostgreSQL, and Valkey have specific support schedules on SUSE Linux Enterprise Server 15:

MariaDB

MariaDB is upgraded to the latest stable LTS release with each Service Pack (e.g., 10.6 in SP4/SP5, 10.11 in SP6, 11.8 LTS in SP7). Security fixes are handled via backports for older Service Packs. MariaDB 11.8 LTS is supported until SLES 15 SP7 LTSS end in December 2034.

On SLES 12 SP5, MariaDB 10.2 (`mariadb`) was supported under a special contract until December 31, 2023, and is now unsupported. MariaDB 10.4 is available via the `mariadb104` package (upstream EOL was June 2024).

PostgreSQL

Each Service Pack gets the latest PostgreSQL major version as default in the **Basesystem Module** (PostgreSQL 14 in SP4, 15 in SP5, 16 in SP6, and 17 in SP7). The default version from the previous Service Pack moves to the **Legacy Module** in the next Service Pack. Legacy versions receive minor updates until they reach upstream EOL.

Valkey and Redis

Redis was shipped up to SLES 15 SP6 (Redis 6.2 in SP4/SP5, 7.2 in SP6). Redis has been dropped in SLES 15 SP7 and replaced with Valkey 8.0.x (which is downward-compatible). Valkey minor version updates can be released into SLES 15 SP7.

2.6.2.5 Web and scripting lifecycle support

PHP and Apache Tomcat have specific support schedules on SUSE Linux Enterprise Server 15:

PHP

Each Service Pack gets a new PHP major version as default (PHP 7.2 in SP0/SP1, 7.4 in SP2/SP3, 8.0 in SP4/SP5, 8.2 in SP6, and 8.4 in SP7). Older PHP versions move to the **Legacy Module**. PHP patch updates (e.g. 8.4.x to 8.4.y) are released reactively for security CVEs and bugs.

Apache Tomcat

Tomcat 11 is introduced starting in SLES 15 SP6. It includes a 1-year initial commitment with a goal of a 6-month support overlap with the next major version.

2.6.2.6 Toolchain lifecycle support

The compiler suite, runtime libraries, and utility tools have independent lifecycles:

System Compiler (GCC 7.5.0)

GCC 7.5.0 remains static and is supported across all SLES 15 Service Packs until July 2034.

Application Compiler (GCC 13, 14, 15)

The Application Compiler in the **Development Tools Module** is updated roughly every year to the next major version. When a new major GCC version is introduced, the previous version remains supported for an overlap of 6 months.

Glibc, Binutils, and Gdb

Binutils and Gdb are upgraded to the latest upstream releases in active Service Packs to address security CVEs. Glibc is updated only occasionally when reasons accumulate (such as glibc 2.31 in SP3, and 2.38 in SP6).

2.6.2.7 Base Container Images (BCI) support

The base OS container images (such as `bci-base`, `bci-minimal`, `bci-micro`, `bci-init`, and `bci-busybox`) are updated throughout the entire lifetime of the Service Pack. This support extends through both the General Support phase and the LTSS phase.

2.7 Support statement for SUSE Linux Enterprise Server

To receive support, you need an appropriate subscription with SUSE. For more information, see https://www.suse.com/support/?id=SUSE_Linux_Enterprise_Server.

The following definitions apply:

L1

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

L2

Problem isolation, which means technical support designed to analyze data, reproduce customer problems, isolate the 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, see *Section 2.8, "Technology previews"*
- Sound, graphics, fonts and artwork
- Packages that require an additional customer contract, see *Section 2.7.2, "Software requiring specific contracts"*
- 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.

2.7.1 General support

To learn about supported features and limitations, refer to the following sections in this document:

- *Section 5.7, "Kernel"*
- *Section 5.12, "Storage and file systems"*
- *Section 5.15, "Virtualization"*
- *Section 10, "Removed and deprecated features and packages"*

2.7.2 Software requiring specific contracts

Certain software delivered as part of SUSE Linux Enterprise Server may require an external contract. Check the support status of individual packages using the RPM metadata that can be viewed with `rpm`, `zypper`, or YaST.

Major packages and groups of packages affected by this are:

2.7.3 Software under GNU AGPL

SUSE Linux Enterprise Server 15 SP7 (and the SUSE Linux Enterprise modules) includes the following software that is shipped *only* under a GNU AGPL software license:

- Ghostscript (including subpackages)

SUSE Linux Enterprise Server 15 SP7 (and the SUSE Linux Enterprise modules) includes the following software that is shipped under multiple licenses that include a GNU AGPL software license:

- MySpell dictionaries and LightProof
- ArgyllCMS

2.8 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, contact your SUSE representative and let them know about your experience and use cases. Your input is helpful for future development.

Technology previews come with the following limitations:

- Technology previews are still in development. Therefore, they may be functionally incomplete, unstable, or in other ways 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.
- Technology previews can be removed from a product at any time. This may be the case, for example, if SUSE discovers that a preview does not meet the customer or market needs, or does not comply with enterprise standards.

2.8.1 Technology previews for Arm 64-Bit (AArch64)

2.8.1.1 KVM virtualization with 64K page size kernel flavor

As a technology preview, SUSE Linux Enterprise Server for Arm 15 SP3 added a kernel flavor `64kb`. SUSE Linux Enterprise Server for Arm 15 SP6 introduced support for this `64kb` kernel flavor (*Section 9.5, "64K page size kernel flavor is supported"*).

KVM virtualization with this `64kb` kernel flavor remains a technology preview. Use the `default` kernel flavor for virtualization support.

2.8.1.2 Driver enablement for NVIDIA BlueField-2 DPU as host platform

SUSE Linux Enterprise Server for Arm 15 SP1 and later kernels include drivers for installing on NVIDIA* BlueField* Data Processing Unit (DPU) based server platforms and SmartNIC (Network Interface Controller) cards.

As a technology preview, the SUSE Linux Enterprise Server for Arm 15 SP6 and SP7 kernels include drivers for running on NVIDIA BlueField-2 DPU.

Should you wish to use SUSE Linux Enterprise Server for Arm on NVIDIA BlueField-2 or BlueField-2X (or BlueField-3) in production, contact your SUSE representative.



Note: Host drivers and tools for NVIDIA BlueField-2 SmartNICs

This Technology Preview status applies only to installing SUSE Linux Enterprise Server for Arm 15 SP7 **on** NVIDIA BlueField-2 DPUs.

For an NVIDIA BlueField-2 DPU PCIe card inserted as **SmartNIC** into a SUSE Linux Enterprise Server 15 SP7 or SUSE Linux Enterprise Server for Arm 15 SP7 based server, check *Section 2.8, "Technology previews"* and *Section 5.7, "Kernel"* for support status or known limitations of NVIDIA ConnectX* network drivers for BlueField-2 DPUs (`mlx5_core` and others).

The `rshim` tool is available from SUSE Package Hub (*Section 5.13, "SUSE Package Hub"*).

2.8.1.3 etnaviv drivers for Vivante GPUs are available

The NXP* Layerscape* LS1028A/LS1018A System-on-Chip (SoC) contains a Vivante GC7000UL Graphics Processor Unit (GPU), and the NXP i.MX 8M SoC contains a Vivante GC7000L GPU.

As a technology preview, the SUSE Linux Enterprise Server for Arm 15 SP7 kernel includes `etnaviv`, a Display Rendering Infrastructure (DRI) driver for Vivante GPUs, and the `Mesa-dri` package contains a matching `etnaviv_dri` graphics driver library. Together they can avoid the need for third-party drivers and libraries.



Note

To use them, the Device Tree passed by the bootloader to the kernel needs to include a description of the Vivante GPU for the kernel driver to get loaded. You may need to contact your hardware vendor for a bootloader firmware upgrade.

2.8.1.4 lima driver for Arm Mali Utgard GPUs available

The Xilinx* Zynq* UltraScale* + MPSoC contains an Arm* Mali*-400 Graphics Processor Unit (GPU).

Prior to SUSE Linux Enterprise Server for Arm 15 SP2, this GPU needed third-party drivers and libraries from your hardware vendor.

As a technology preview, the SUSE Linux Enterprise Server for Arm 15 SP2 kernel added `lima`, a Display Rendering Infrastructure (DRI) driver for Mali *Utgard* microarchitecture GPUs, such as Mali-400, and the `Mesa-dri` package contains a matching `lima_dri` graphics driver library.



Note

To use them, the Device Tree passed by the bootloader to the kernel needs to include a description of the Mali GPU for the kernel driver to get loaded. You may need to contact your hardware vendor for a bootloader firmware upgrade.



Note

The `panfrost` driver for Mali *Midgard* microarchitecture GPUs is supported since SUSE Linux Enterprise Server for Arm 15 SP2.

2.8.1.5 mali-dp driver for Arm Mali Display Processors available

The NXP* Layerscape* LS1028A/LS1018 System-on-Chip contains an Arm* Mali*-DP500 Display Processor.

As a technology preview, the SUSE Linux Enterprise Server for Arm 15 SP2 kernel added `mali-dp`, a Display Rendering Manager (DRM) driver for Mali Display Processors. It has undergone only limited testing because it requires an accompanying physical-layer driver for DisplayPort* output (see *Section 9.6.3, "No DisplayPort graphics output on NXP LS1028A and LS1018A"*).

2.8.1.6 Btrfs file system is enabled in U-Boot bootloader

For Raspberry Pi* devices, SUSE Linux Enterprise Server for Arm 12 SP3 and later include *Das U-Boot* as bootloader, in order to align the boot process with other platforms. By default, it loads GRUB as UEFI application from a FAT-formatted partition, and GRUB then loads Linux kernel and ramdisk from a file system such as Btrfs.

As a technology preview, SUSE Linux Enterprise Server for Arm 15 SP2 added a Btrfs driver to U-Boot for the Raspberry Pi (package `u-boot-rpiarm64`). This allows its commands `ls` and `load` to access files on Btrfs-formatted partitions on supported boot media, such as microSD and USB.

The U-Boot command `btrsubvol` lists Btrfs subvolumes.

2.8.2 Technology previews for Intel 64/AMD64 (x86-64)

2.8.2.1 Support for AMD Wheat Nas GPU

SLES 15 SP7 includes the kernel driver support for AMD Wheat Nas GPU (Navi32 dGPU). However because the corresponding firmware is still not publicly released yet, this feature is considered a technology preview.

2.8.2.2 Add IAA Crypto Driver

SLES 15 SP7 includes the Intel Analytics Accelerators (IAA) crypto compression kernel driver. Since this is a new upstream feature, is is considered a technology preview.

3 Modules, extensions, and related products

This section comprises information about modules and extensions for SUSE Linux Enterprise Server 15 SP7. Modules and extensions add functionality to the system.



Note: Package and module changes in 15 SP7

For more information about all package and module changes since the last version, see *Section 2.2.3, "Package and module changes in 15 SP7"*.

3.1 Modules in the SLE 15 SP7 product line

The SLE 15 SP7 product line is made up of modules that contain software packages. Each module has a clearly defined scope. Modules differ in their life cycles and update timelines.

The modules available within the product line based on SUSE Linux Enterprise 15 SP7 at the release of SUSE Linux Enterprise Server 15 SP7 are listed in the *Modules and Extensions Quick Start* at https://documentation.suse.com/sles/15-SP7/html/SLES-all/article-modules.html.

Not all SLE modules are available with a subscription for SUSE Linux Enterprise Server 15 SP7 itself (see the column *Available for*).

For information about the availability of individual packages within modules, see https://sc-c.suse.com/packages.

3.2 SLE extensions

SLE Extensions add extra functionality to the system and require their own registration key, usually at additional cost. Most extensions have their own release notes documents that are available from https://www.suse.com/releasenotes.

The following extensions are available for SUSE Linux Enterprise Server 15 SP7:

- SUSE Linux Enterprise Live Patching: https://www.suse.com/products/live-patching
- SUSE Linux Enterprise High Availability: https://www.suse.com/products/highavailability
- SUSE Linux Enterprise Workstation Extension: https://www.suse.com/products/workstation-extension

The following extension is not covered by SUSE support agreements, available at no additional cost and without an extra registration key:

- SUSE Package Hub: https://packagehub.suse.com/ (see *Section 5.13, "SUSE Package Hub"*)

3.3 Derived and related products

This sections lists derived and related products. Usually, these products have their own release notes documents that are available from https://www.suse.com/releasenotes.

- SUSE Linux Enterprise JeOS: https://www.suse.com/products/server/jeos (see *Section 4.3, "Minimal VM and Minimal Image"*)
- SUSE Linux Enterprise Desktop: https://www.suse.com/products/desktop
- SUSE Linux Enterprise Server for SAP Applications: https://www.suse.com/products/sles-for-sap
- SUSE Linux Enterprise High Performance Computing: https://www.suse.com/products/server/hpc
- SUSE Linux Enterprise Real Time: https://www.suse.com/products/realtime
- SUSE Multi-Linux Manager: https://www.suse.com/products/multi-linux-manager/

4 Installation and upgrade

SUSE Linux Enterprise Server can be deployed in several ways:

- Physical machine
- Virtual host
- Virtual machine
- System containers
- Application containers

4.1 Installation

This section includes information related to the initial installation of SUSE Linux Enterprise Server 15 SP7.

Important: Installation documentation

The following release notes contain additional notes regarding the installation of SUSE Linux Enterprise Server. However, they do not document the installation procedure itself.

For installation documentation, see the *Deployment Guide* at https://documentation.suse.com/sles/15-SP7/html/SLES-all/book-deployment.html.

4.1.1 New media layout

The set of media has changed with 15 SP2. There still are two different installation media, but the way they can be used has changed:

- You can install with registration using either the online-installation medium (as with SUSE Linux Enterprise Server 15 SP1) or the full medium.
- You can install without registration using the full medium. The installer has been added to the full medium and the full medium can now be used universally for all types of installations.
- You can install without registration using the online-installation medium. Point the installer at the required SLE repositories, combining the `install=` and `instsys=` boot parameters:
  - With the `install=` parameter, select a path that contains either just the product repository or the full content of the media.
  - With the `inst-sys=` parameter, point at the installer itself, that is, `/boot/ARCHITECTURE/root` on the medium.

  For more information about the parameters, see https://en.opensuse.org/SDB:Linuxrc#p_install.

4.2 Upgrade-related notes

This section includes upgrade-related information for SUSE Linux Enterprise Server 15 SP7.



Important: Upgrade documentation

The following release notes contain additional notes regarding the upgrade of SUSE Linux Enterprise Server. However, they do not document the upgrade procedure itself.

For upgrade documentation, see the *Upgrade Guide* at https://documentation.suse.com/sles/15-SP7/html/SLES-all/cha-upgrade-online.html.

4.2.1 Upgrade & Migration Quick Checklist

The following checklist summarizes key action items and potential gotchas documented across these release notes, organized by migration phase.

4.2.1.1 Phase 1: Before Upgrading (Preparation)

- ❑ **Patch Level:** Make sure the current system is completely up-to-date and fully patched.
  See *Section 4.2.4, "Make sure the current system is up-to-date before upgrading"*.
- ❑ **Service Pack Skipping:** Check if intermediate service packs are being skipped, which requires an LTSS contract.
  See *Section 4.2.5, "Skipping service packs requires LTSS"*.
- ❑ **Subscription Management:** Be aware that SMT has been replaced by RMT.
  See *Section 4.2.7, "SMT has been replaced by RMT"*.

4.2.1.2 Phase 2: During Upgrade (Migration)

- ❑ **Storage and Driver Changes:** Be aware that SLES 15 SP4 dropped `scsi_mod.use_blk_mq`.
  See *Section 4.2.2, "Removal of obsolete `scsi_mod.use_blk_mq` kernel parameter"*.

4.2.1.3 Phase 3: After Upgrading (Post-Migration & First Boot)

- ❑ **User Login:** Verify that regular user accounts can log in.

PAM `pam_unix2` is deprecated.

See *Section 4.2.3, "User Login Fails After Upgrade"*.

4.2.2 Removal of obsolete `scsi_mod.use_blk_mq` kernel parameter

The obsolete `scsi_mod.use_blk_mq` kernel parameter has been completely removed from the kernel. Multi-queue block I/O is now the only available block I/O framework. If configurations (such as the kernel command line or files under `/etc/modprobe.d/`) still reference `scsi_mod.use_blk_mq`, a warning is shown at boot: `scsi_mod: unknown parameter 'use_blk_mq' ignored`. This parameter can be safely removed from configurations as multi-queue block I/O is always active.

4.2.3 User Login Fails After Upgrade

After upgrading from SLES 12 SP4 or earlier, regular user accounts cannot log in to the system. This is caused by the deprecation of `pam_unix2` because of its issues with `systemd`. For information how to fix the issue, see https://www.suse.com/support/kb/doc/?id=000019703.

4.2.4 Make sure the current system is up-to-date before upgrading

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*. An upgrade on a system that is not fully patched may fail.

4.2.5 Skipping service packs requires LTSS

Skipping service packs during an upgrade is only supported if you have a Long Term Service Pack Support contract. Otherwise, you need to first upgrade to SLE 15 SP6 before upgrading to SLE 15 SP7.

4.2.6 Direct upgrade from SLES 12 SP5 LTSS to SLES 15 15 SP7 is supported

You can upgrade directly from SUSE Linux Enterprise Server 12 SP5 LTSS to SUSE Linux Enterprise Server 15 15 SP7. You cannot upgrade from SUSE Linux Enterprise Server 12 SP5 LTSS to SUSE Linux Enterprise Server 15 SP5 or older. Older service packs contain older package ver-

sions than SUSE Linux Enterprise Server 12 SP5 LTSS. Upgrading to those service packs causes package downgrades, which can break the system. To upgrade from SUSE Linux Enterprise Server 12 SP5 LTSS, you must upgrade directly to SUSE Linux Enterprise Server 15 SP6 or newer.

4.2.7 SMT has been replaced by RMT



Note

RMT supports SUSE Linux Enterprise Server 16.0 clients.

SLE 12 is the last codestream that SMT (Subscription Management Tool) is available for.

When upgrading your OS installation to SLE 15, we recommend also upgrading from SMT to its replacement RMT (Repository Mirroring Tool). RMT provides the following functionality:

- Mirroring of SUSE-originated repositories for the SLE 12-based and SLE 15-based products your organization has valid subscriptions for.
- Synchronization of subscriptions from SUSE Customer Center using your organization's mirroring credentials. (These credentials can be found in SCC under *Select Organization*, *Organization*, *Organization Credentials*)
- Selecting repositories to be mirrored locally via `rmt-cli` tool.
- Registering systems directly to RMT to get required updates.
- Adding custom repositories from external sources and distributing them via RMT to target systems.
- Improved security with proxying: If you have strict security requirements, an RMT instance with direct Internet access can proxy to another RMT instance without direct Internet access.
- Nginx as Web server: The default Web server of RMT is Nginx which has a smaller memory footprint and comparable performance than that used for SMT.

Note that unlike SMT, RMT does not support installations of SLE 11 and earlier.

For more feature comparison between RMT and SMT, see https://github.com/SUSE/rmt/blob/master/docs/smt_and_rmt.md.

For more information about RMT, see the RMT Guide at https://documentation.suse.com/sles/15-SP7/html/SLES-all/book-rmt.html.

4.3 Minimal VM and Minimal Image

SUSE Linux Enterprise Server Minimal VM and Minimal Image is a slimmed-down form factor of SUSE Linux Enterprise Server that is ready to run in virtualization environments and the cloud. With SUSE Linux Enterprise Server Minimal VM and Minimal Image, you can choose the right-sized SUSE Linux Enterprise Server option to fit your needs.

SUSE provides virtual disk images for Minimal VM and Minimal Image in the file formats `.qcow2`, `.vhdx`, and `.vmdk`, compatible with KVM, Xen, OpenStack, Hyper-V, and VMware environments. All Minimal VM and Minimal Image images set up the same disk size (24 GB) for the system. Due to the properties of different file formats, the size of Minimal VM and Minimal Image image downloads differs between formats.

4.4 JeOS renamed Minimal VM and Minimal Image

We have received feedback from users confused by the name JeOS, as a matter of fact the acronym JeOS, which meant Just enough Operating System, was not well understood and could be confused with other images provided by SUSE or openSUSE.

We have decided to go with simplicity and rename JeOS by "Minimal VM" for all our Virtual Machine Images and "Minimal Image" for the Raspberry Pi Image. We have also removed a few other characters, in the full images name to make it more simple and clear:

- `SLES15-SP4-Minimal-VM.x86_64-kvm-and-xen-GM.qcow2`
- `SLES15-SP4-Minimal-VM.x86_64-OpenStack-Cloud-GM.qcow2`
- `SLES15-SP4-Minimal-VM.x86_64-MS-HyperV-GM.vhdx.xz`
- `SLES15-SP4-Minimal-VM.x86_64-VMware-GM.vmdk.xz`
- `SLES15-SP4-Minimal-VM.aarch64-kvm-GM.qcow2`
- `SLES15-SP4-Minimal-Image.aarch64-RaspberryPi-GM.raw.xz`

4.5 Added iptables and nftables to SLES Minimal images

The `iptables` and `nftables` packages have been added to SLES Minimal Cloud and VMware VM images. This addition enables the successful provisioning of Rancher-deployed RKE2 and K3s clusters on SLES Minimal images without requiring manual package installation or Subscription Management (RMT) registration.

4.6 For more information

For more information, see *Section 5, "Changes affecting all architectures"* and the sections relating to your respective hardware architecture.

5 Changes affecting all architectures

Information in this section applies to all architectures supported by SUSE Linux Enterprise Server 15 SP7.

5.1 Authentication

5.1.1 krb5: Deprecated Encryption Types Disabled by Default

Kerberos 5 (krb5) now disables deprecated encryption types by default. These encryption types do not meet current security standards.

SUSE removed the following encryption types from the default krb5 configuration:

- `des3-cbc-sha1`
- `arcfour-hmac-md5`

To use these encryption types, add the following lines to the `[libdefaults]` section of the `/etc/krb5.conf` file:

```
[libdefaults]
allow_des3 = true
allow_rc4 = true
```

5.2 Containers

5.2.1 STIG-compliant container

A STIG-compliant SUSE Linux Enterprise Base Container Image (SLE BCI) is now available via the DoD's Iron Bank repository, supporting secure software supply chains for US Government agencies.

For more information see https://www.suse.com/c/sle-bci-base-container-available-for-us-government-agencies-on-iron-bank/.

5.2.2 Default container registries

The container registry entries for Docker Hub and openSUSE Registry, which were previously included by default, have now been removed. If you want to pull container images from either of them, add them to the `/etc/containers/registries.conf` file.

5.2.3 `suse/sle15` container uses NDB as the database back-end for RPM

Starting with SUSE Linux Enterprise 15 SP3, the `rpm` package in the `suse/sle15` container image no longer supports the BDB back-end (based on Berkeley DB) and switches to the NDB back-end. Tools for scanning, diffing, and building container image using the `rpm` binary of the host for introspection can fail or return incorrect results if the host's version of `rpm` does not recognize the NDB format.

To use such tools, make sure that the host supports reading NDB databases, such as hosts with SUSE Linux Enterprise 15 SP2 and later.

5.3 Databases

- PostgreSQL has been updated to version 14.
- MariaDB has been updated to the LTS version 11.8. See https://mariadb.org/11-8-lts-released/ for more information.

5.3.1 Full support for PostgreSQL

The PostgreSQL database is now fully supported by SUSE. You no longer need an external support contract.

5.3.2 pgAdmin has been updated

The `pgadmin4` package has been updated to version 8.5. It is now part of the *Python 3 Module*.

5.4 Desktop

5.4.1 `gtk4-lang` Package Included for GTK 4 Localization

The `gtk4-lang` package is now included. This provides the translation files necessary for GTK 4 applications to display localized user interfaces.

5.5 Development

- `python3-ovs` has been renamed to `python3-openvswitch`

5.5.1 `python311-apache-libcloud` package added

SUSE Linux Enterprise Server now includes the `python311-apache-libcloud` package. This package provides the Apache Libcloud library for Python 3.11. You can use this package to run `salt-cloud` in Python 3.11 environments.

5.5.2 Support for Ansible interpreter

The Ansible packages (`ansible-core`) are included in SUSE Linux Enterprise Server 15 SP6 and newer. Support is limited to any Ansible playbooks or roles that are provided by SUSE as part of SUSE Linux Enterprise Server or SUSE Multi-Linux Manager products, whether supplied directly (for example, via packages, ISO images, ready-to-run images) or dynamically generated by integrated tools within these products.

5.5.3 Ruby 3 has been added

In SLES 15 SP7, Ruby version 3.4 has been added. This is in addition to the existing Ruby 2.5.

5.5.4 Python 3 packages staying in Basesystem

The `python311-base` and `libpython3_11-1_0` packages have been moved to the *Basesystem Module* for technical reasons. These two packages still follow the lifecycle of the *Python 3 Module* (that is, until December 2029) and that is reflected in the metadata as well.

A new Python interpreter version 3.13 has been added. This interpreter has a shorter support period of 1.5 years and is there to support installing additional packages via `pip`.

5.5.5 `glibc` 2.38

The `glibc` package has been updated to version 2.38.

- A couple of internal `glibc` interfaces has changed; if an application uses these internal interfaces, the application needs fixing (note that internal interfaces should never be used)
- Split deprecated library `libnsl1` into separate package

5.5.6 Supported `nodejs` versions

Before LTSS we provide concurrent support for up to 3 upstream versions of `nodejs` in SLES 15 SP7. In LTSS we only support the latest `nodejs` version.

Note that the upstream version naming might change but this will not change what is supported.

Version	Date	Upstream EOL	Inclusion in SP7	SUSE EOL
22.x	Oct 2024	Apr 2026	GA	end of 2027
24.x	Oct 2025	Apr 2027	end of 2025	end of 2028
26.x	Oct 2026	Apr 2028	end of 2026	end of 2029
28.x	Oct 2027	Apr 2029	end of 2027	end of 2030
30.x	Oct 2028	Apr 2030	end of 2028	end of GS July 2031
32.x	Oct 2029	Apr 2031	end of 2029	end of GS July 2031
34.x	Oct 2030	Apr 2032	end of 2030	end of LTSS July 2034

Version	Date	Upstream EOL	Inclusion in SP7	SUSE EOL
36.x	Oct 2031	Apr 2033	not planned for SP7	

5.5.7 Node.js 24 added as default version

The `nodejs24` package has been added to the *Web and Scripting Module*. This is now the default Node.js version in SLES 15 SP7. The `nodejs-common` package has been updated so that the `nodejs` default command points to Node.js 24.

5.5.8 Supported Java versions

The following Java implementations are available in SUSE Linux Enterprise Server 15 SP7:

Name (Package Name)	Version	Module	Support
IBM Java (`java-1_8_0-ibm`)	1.8.0	Legacy	External, until 2030-12-31
OpenJDK (`java-1_8_0-openjdk`)	1.8.0	Legacy	SUSE, L3, until 2026-12-31
OpenJDK (`java-11-openjdk`)	11	Legacy	SUSE, L3, until 2026-12-31
OpenJDK (`java-17-openjdk`)	17	Legacy	SUSE, L3, until 2027-12-31
OpenJDK (`java-21-openjdk`)	21	Base System	SUSE, L3, until 2034-07-31
OpenJDK (`java-25-openjdk`)	25	Base System	SUSE, L3, until 2033-10-31

5.6 Hardware

5.6.1 Lack of PMU support for Intel hybrid CPUs

Performance Monitoring Unit (PMU) features do not function correctly on systems with Intel hybrid CPUs in this release. The Linux kernel requires additional changes to fully support the PMU on these processors, which were only introduced in Linux kernel version 6.9.

Because SLES 15 SP7 is based on kernel 6.4, these improvements are not included.

5.7 Kernel

- Allow enabling `CONFIG_RT_GROUP_SCHED` at boot time using the `rt_group_sched` kernel cmdline parameter

5.7.1 `smc` driver has been updated

The `smc` (Shared Memory Communication) kernel driver has been updated to the latest upstream version.

Note that currently using the `smc` driver can cause the system to freeze. This will be fixed in a future release.

5.7.2 cgroupv2 CPU load-balancing

The cgroups-v2 CPU load-balancing feature has been backported to the 15 SP7 kernel.

5.7.3 Externally supported flag change

The externally supported flag is no longer stored as a taint flag now. This means that the kernel is no longer tainted after an externally-supported module is inserted.

5.7.4 Userspace live patching

Currently, `libpulp` supports user space live patching of `glibc` and `openssl` binaries on the following architectures:

- x86-64
- ppc64le

For more information see https://documentation.suse.com/sles/15-SP7/html/SLES-all/cha-ulp.html

5.7.5 `CONFIG_HZ` value changes

The SUSE Linux Enterprise Server 15 SP6 kernels diverged from latest `CONFIG_HZ` default settings for multiple architectures.

The SUSE Linux Enterprise Server for Arm 15 SP7 kernel changed the `CONFIG_HZ` value (*Section 9.3, "Changed kernel `CONFIG_HZ` value"*): x86-64 and Arm* architectures now use the same value of 250 Hz.

PowerPC and IBM Z architectures continue to share a value of 100 Hz.

These configuration values cannot be overridden from the kernel command line. If your applications run into issues, contact your SUSE representative.

5.7.6 Kernel limits

This table summarizes the various limits which exist in our recent kernels and utilities (if related) for SUSE Linux Enterprise Server 15 SP7.

SLES 15 SP7 (Linux 6.4)	**AMD64/Intel 64 (x86_64)**	**IBM Z (s390x)**	**POWER (ppc64le)**	**Armv8 (AArch64)**
CPU bits	64	64	64	64
Maximum number of logical CPUs	8192	512	8192	768
Maximum amount of RAM (theoretical/certified)	>1 PiB/ 64 TiB	10 TiB/ 256 GiB	1 PiB/64 TiB	256 TiB/n.a.

SLES 15 SP7 (Linux 6.4)	AMD64/Intel 64 (x86_64)	IBM Z (s390x)	POWER (ppc64le)	Armv8 (AArch64)
Maximum amount of user space/kernel space	128 TiB/ 128 TiB	n.a.	4 PiB[1]/2 EiB	256 TiB/ 256 TiB
Maximum amount of swap space	Up to 29 * 64 GB	Up to 30 * 64 GB		
Maximum number of processes	1,048,576			
Maximum number of threads per process	Upper limit depends on memory and other parameters (tested with more than 120,000)[2].			
Maximum size per block device	Up to 8 EiB on all 64-bit architectures			
FD_SETSIZE	1024			

[1] By default, the user space memory limit on the POWER architecture is 128 TiB. However, you can explicitly request mmaps up to 4 PiB.

[2] The total number of all processes and all threads on a system may not be higher than the "maximum number of processes".

5.7.7 Restoring default Btrfs file compression

Previously in kernel 5.14, it was possible to disable compression by passing an empty string instead of explicitly mentioning `none` or `no`.

In SLES 15 SP7, this behavior is changed to the more expected one. From kernel 5.14 onwards, empty string will reset the default setting instead of disabling compression.

5.7.8 Clocksource watchdog disabled on HPE UV5 platforms

On HPE UV5 platforms (for example, Google Compute Engine (GCE) X4 bare-metal instances), the kernel clocksource watchdog monitored the Time Stamp Counter (TSC) clocksource. This monitoring could cause system instability. To prevent this instability, users had to disable the clocksource watchdog manually. This manual configuration required adding the `tsc=nowatchdog` parameter to the kernel command line and restarting the system.

Now, the kernel automatically disables the clocksource watchdog for the TSC on all HPE UV5 platforms. Users do not need to configure the kernel command line or restart their systems.

5.8 Miscellaneous

- Warnings are now printed using `dmesg` when deprecated cgroup v1 features are used

5.8.1 Apache's Portable Runtime Library devel package renaming

These two packages have been renamed:

- `libapr1-devel` to `apr-devel`
- `libapr-util1-devel` to `apr-util-devel`

5.8.2 `hwloc` has been updated

The `hwloc` package has been updated to version 2.11.2:

- Add missing CPU info attrs for aarch64 on Linux.
- Use ACPI CPPC on Linux to get better information about cpukinds, at least on AMD CPUs.
- `hwloc-calc --cpuset-output-format` systemd-dbus-api now allows. to generate `AllowedCPUs` information for systemd slices. See the `hwloc-calc` manpage for examples.
- API
  - Add `HWLOC_MEMBIND_WEIGHTED_INTERLEAVE` memory binding policy on Linux 6.9+.

        - `weighted_interleave_membind` is added to membind support bits.
        - The “weighted” policy is added to the `hwloc-bind` tool.
    - Add `hwloc_obj_set_subtype()`.
- GPU support
    - Don’t hide the GPU NUMA node on NVIDIA Grace Hopper.
    - Get Intel GPU OpenCL device locality.
    - Add bandwidths between subdevices in the `LevelZero` `XeLinkBandwidth` matrix.
- Tools
    - Option `--best-memattr` may now return multiple nodes. Additional configuration flags may be given to tweak its behavior.
    - `hwloc-info` has a new `--get-attr` option to get a single attribute.
    - `hwloc-info` now supports “levels”, “support” and “topology” special keywords for backward compatibility for hwloc 3.0.
    - The `--taskset` command-line option is superseded by the new `--cpuset-output-format` which also allows to export as list.
    - `hwloc-calc` may now import bitmasks described as a list of bits with the new `--cpuset-input-format list`.
- Misc
    - The `MemoryTiersNr` info attribute in the root object now says how many memory tiers were built.
    - Fix the management of infinite cpusets in the bitmap printf/sscanf API as well as in command-line tools.
    - Add section “Compiling software on top of hwloc’s C API” in the documentation with examples for GNU Make and CMake. Bug Fixes:
- Fix crash when manipulating cpukinds after topology duplication.
- Fix missing input target checks in memattr functions

- Fix a memory leak when ignoring NUMA distances on FreeBSD.
- Fix build failure on old Linux distributions without accessat().
- Fix non-Windows importing of XML topologies and CPUID dumps exported on Windows.
- Some fixes in manpage EXAMPLES and split them into subsections.
- Fix bash completions
    - Fix PCI Gen4+ link speed of NVIDIA GPU obtained from NVML.

5.8.3 systemd default configurations moved to `/usr`

Main configuration files have been moved from `/etc` to `/usr`. This ensures that main configuration files have lower precedence, allowing them to be overriden by package-supplied drop-in snippets.

Local configuration should be created by either modifying the default file in `/usr` (or a copy of it placed in `/etc` if the original file is shipped in `/usr`), or by creating drop-in snippets in the appropriate directory in (for example, `/etc/systemd/coredump.conf.d/`) - this is recommended.

Remove configurations in `/etc` to restore defaults.

5.8.4 FADump and kdump speed improvement

The default for `KDUMP_CPUS` changed from `1` to `32`, allowing `kdump` to use up to 32 threads to generate a kernel dump.

5.8.5 New systems-management module

A new module called *Systems Management Module* has been added. This module will include systems-management packages, such as Ansible.

5.8.6 Ansible is now available

In SLES 15 SP7, Ansible has been added to the *Systems Management Module*.

5.8.7 "IDXD: user: probe of wq1.0 failed with error -95" errors

Certain configurations can cause errors viewable using the `dmesg` command, with the following content:

```
IDXD: user: probe of wq1.0 failed with error -95
```

These can be safely ignored for now. They will be fixed in a future release.

5.8.8 Support of BPF-related tools

- The main userspace library and tooling, `libbpf` and `bpftool`, is only supported when running on a kernel of the same product. Pairing `libbpf` and `bpftool` from different products is not supported.
- `bcc`/`libbcc` is only supported when running on a kernel of the same product, and additionally uses kernel headers from the `kernel-*-devel` package of the same product to access in-kernel data types.
- `bpftrace` is only supported when running on a kernel of the same product, and additionally uses one of these:
  - kernel headers from the `kernel-*-devel` package of the same product
  - builtin BTF of kernel, when accessing in-kernel data types

5.8.9 Apache HTTP Server upgraded to version 2.4.66

The Apache HTTP Server (`apache2`) has been upgraded to version 2.4.66. This update addresses several stability issues, including a segmentation fault (`SIGSEGV`) when serving HTTP/2 requests under certain race conditions. Previously, connections could abort during complex subrequest error handling, causing `mod_include` to access freed memory. Upgrading to Apache 2.4.66 resolves this issue and ensures ongoing security and stability.

5.9 Networking

5.9.1 `firewalld` version 1.3.4 added

The `firewalld` package with the version 1.3.4 has been added to our repositories. We now provide this legacy version additionally to the existing package.

Due to high firewall reload times, some users are facing performance problems with the 2.x.x version series. Affected users can now downgrade to the legacy version but staying on the 2.x.x series is strongly recommended.

Execute the following commands to downgrade and to prevent the package from upgrading to the 2.x.x series:

```
zypper refresh
zypper install --oldpackage --allow-downgrade 'firewalld < 2'
zypper addlock 'firewalld >= 2'
```

During the downgrade, the firewall will stay active and the firewall configuration will be preserved. Check the firewall configuration and restart the relevant service to use the newly installed version. Execute the following command to restart the firewall:

```
systemctl restart firewalld.service
```

You are able to update your system as usual and the firewalld legacy package will receive updates but won't be upgraded to version 2.x.x. Once the performance problems are resolved, revert back to using the latest version available in our repositories.

Execute the following commands to revert back to the lastest version in our repositories. The firewall stays active during this process.

```
zypper removelock 'firewalld >= 2'
zypper refresh
zypper update
```

After the update succeeded, check your firewall configuration and restart the relevant service to use the newly installed version. Execute the following command to restart the firewall:

```
systemctl restart firewalld.service
```

5.9.2 Kea DHCP has been added

Kea DHCP (as package `kea`) is a DHCP server that is replacing the end-of-life `dhcpd` package (also known as ISC DHCP). For more information see https://www.isc.org/kea/

5.9.3 `bind` version 9.18

The `bind` package has been updated from version 9.16 to version 9.18. This is a major update that removes several options but also adds, among others, the following features:

- DoT and DoH (DNS over TLS and DNS over HTTPS) support
- OpenSSL version 3.0.0

See the full changelog (https://kb.isc.org/docs/changes-to-be-aware-of-when-moving-from-bind-916-to-918) for more information.

5.9.4 `systemd-resolved` packaged separately

The `systemd-resolved` package has been split from the main `systemd-network` package into an independent, standalone sub-package. `systemd-resolved` provides network name resolution via a local stub resolver, enabling features such as DNS-over-TLS (DoT).

5.9.5 Samba

The version of Samba shipped with SUSE Linux Enterprise Server 15 SP7 delivers integration with Windows Active Directory domains. In addition, we provide the clustered version of Samba as part of SUSE Linux Enterprise High Availability 15 SP7.

5.9.6 NFS

5.9.6.1 NFSv4

NFSv4 with IPv6 is only supported for the client side. An NFSv4 server with IPv6 is not supported.

5.10 Security

5.10.1 ClamAV has been updated to version 1.0

The `clamav` package has been updated to version 1.0. This major version update introduces several new features, security enhancements, and bug fixes:

- Expanded decryption support, including decrypted Microsoft Excel (XLS) files.
- Support for scanning images embedded in HTML emails.
- Performance optimizations and improved parsing of various file formats.
- Internal modernizations, including further integration of the Rust-based components for memory-safe execution.

5.10.2 Post-quantum cryptography (PQC) key exchange enabled by default

By default, system-wide cryptographic policies now enable the `sntrup761x25519-sha512@openssh.com` post-quantum cryptography (PQC) key exchange algorithm for SSH connections. This prevents connection warnings (such as `WARNING: connection is not using a post-quantum key exchange algorithm`) from modern external SSH clients that require post-quantum security by default. The algorithm is now enabled in the `DEFAULT`, `FUTURE`, and `LEGACY` system-wide cryptographic policies.

5.10.3 Support for mlkem768x25519-sha256 post-quantum key exchange in OpenSSH

OpenSSH now supports the `mlkem768x25519-sha256` post-quantum cryptography (PQC) hybrid key exchange algorithm. This algorithm combines ML-KEM-768 with X25519 to provide secure connections against future quantum computers. The system-wide cryptographic policies in the `crypto-policies` package enable this algorithm in the `DEFAULT` and `FUTURE` policies.

5.10.4 SSSD: support for running as unprivileged user

SSSD has been updated to version 2.10, which adds support for running as an unprivileged user instead of root. This allows containerized deployments to comply with security requirements that limit root privileges within containers.

By default, SSSD runs as root with the `sssd` supplementary group, which provides access to SSSD-owned files. To switch to unprivileged mode, create a systemd service override:

```
sudo systemctl edit sssd.service
```

Add the following:

```
[Service]
User=sssd
Group=sssd
SupplementaryGroups=
```

Then reload and restart the service:

```
sudo systemctl daemon-reload
sudo systemctl restart sssd
```

Note that running as an unprivileged user requires filesystem support for POSIX capabilities. On filesystems that do not support capabilities (such as NFS), SSSD must continue to run as root.

5.10.5 Microsoft Entra ID authentication

Microsoft Entra ID authentication capabilities have been added to SUSE Linux Enterprise Server.

We officially support authentication via Device Authorization Grant. Authentication via the project's experimental MFA flow is not supported.

5.10.6 New 4096-bit signing key

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. For more information see https://documentation.suse.com/sles/15-SP6/html/SLES-all/cha-update-preparation.html#sec-update-preparation-update

5.10.7 OpenSSH and crypto policies update

The `openssh` package has been updated to version 9.6p1, aligning with system crypto policies from the `crypto-policies` package. This update excludes insecure cryptographic algorithms, notably disallowing RSA keys under 2048 bits. This change may affect users with RSA host keys under 2048 bits for server connections.

To check for affected keys:

```
grep ssh-rsa ~/.ssh/known_hosts | ssh-keygen -lf -
```

The output lists key sizes and associated hostnames/IPs. After upgrade, connections to hosts with 1024 bit keys will fail if no alternative valid key exists.



Note: Troubleshooting

Before upgrade

a. Either update openssh to version 8.4p1, which enables `UpdateHostkeys` by default, allowing ssh to update `known_hosts` with all server's host keys. Users must connect to the host with a 1024-bit RSA key after updating to this version and before upgrading to SP6.

b. Or, manually add host keys:

```
ssh-keyscan hostname >> ~/.ssh/known_hosts
```

Note that this method adds keys without verification; use only if manual host verification is possible.

After upgrade

a. Either temporarily use insecure algorithms by setting the crypto policy to LEGACY:

```
sudo update-crypto-policies --set LEGACY
```

Then, revert to the default secure policy after connecting:

```
sudo update-crypto-policies --set DEFAULT
```

b. Or, remove the invalid host key from `known_hosts` and reconnect, manually verifying the new host key.

5.10.8 Automatic CPU mitigations and how to change them

By default, the CPU mitigations setting to prevent CPU side-channel attacks is set to `Auto`. However, the kernel boot parameters included in the `Auto` option may change from one Service Pack to the next due to the necessity of applying new security patches. This may result in performance loss in some scenarios. You might want to change these to achieve a different tradeoff between performance and security.

For more information on how to configure these settings, see https://documentation.suse.com/sles/15-SP7/single-html/SLES-administration/#vle-grub2-yast2-cpu-mitigations.

5.10.9 Support for MS SQL Server 2025 legacy hashing algorithms in OpenSSL 3

Microsoft SQL Server 2025 requires legacy hashing algorithms (such as MD2, MD4, and MD5) for functions like `HASHBYTE`. To support this, OpenSSL 3 in SLES is now compiled with the `enable-md2` option. Because these algorithms are disabled by default, the OpenSSL legacy provider must be explicitly enabled.

To enable the legacy provider, make the following modifications to `/etc/ssl/openssl.cnf`:

1. In the `[provider_sect]` section, ensure that the `legacy` provider is defined:

```
[provider_sect]
default = default_sect
legacy = legacy_sect
```

2. Ensure that both default and legacy sections are activated:

```
[default_sect]
activate = 1

[legacy_sect]
activate = 1
```

To verify the providers are active, run the `openssl list -providers` command. The output must display both `default` and `legacy` as active.

5.10.10 OpenSSL 3.2.3 is now default

In SLES 15 SP7, OpenSSL has been updated to version 3.2.3, replacing OpenSSL 1.1.1.

Because the development packages of different versions are mutually exclusive and automatic conflict resolution is not performed during updates, `libopenssl1_1-devel` should be manually selected for de-installation.

5.10.11 TLS 1.1 and 1.0 are no longer recommended for use

The TLS 1.0 and 1.1 standards have been superseded by TLS 1.2 and TLS 1.3. TLS 1.2 has been available for considerable time now.

SUSE Linux Enterprise Server packages using OpenSSL, GnuTLS, or Mozilla NSS already support TLS 1.3. We recommend no longer using TLS 1.0 and TLS 1.1, as SUSE plans to disable these protocols in a future service pack. However, not all packages, for example, Python, are TLS 1.3-enabled yet as this is an ongoing process.

5.11 Non-unified OVMF images for SEV

Non-unified OVMF images for SEV (ovmf-x86_64-sev-{code,vars}.bin) has been removed because it presents a security risk due to the non-measured variable store. For enhanced security with SEV, we recommended to use the unified image (ovmf-x86_64-sev.bin).

5.11.1 haveged switch-root service removed

The `haveged-switch-root.service` has been removed from SUSE Linux Enterprise Server 15 SP4, SP5, and SP6. Implementing a robust switch-root service for `haveged` is difficult and was prone to security and synchronization issues. Since Linux kernel 5.4, a HAVEGED-inspired entropy gathering algorithm has been included directly in the kernel, making `haveged-switch-root.service` unnecessary.

To resolve any remaining early-boot entropy requirements safely, `haveged-once.service` has been introduced instead, which runs with the `--once` flag during early boot and exits cleanly before switching root.

5.11.2 squid: ESI processing disabled

The `squid` caching proxy has disabled and removed Edge Side Includes (ESI) processing. This change improves security. It addresses vulnerabilities in ESI processing, such as CVE-2024-45802. ESI processing is rare in modern setups because it requires content manipulation in transit.

5.12 Storage and file systems

5.12.1 Deprecation of legacy XFS v4 filesystem format

SUSE Linux Enterprise maintains backward compatibility for legacy XFS v4 filesystems via the kernel configuration `CONFIG_XFS_SUPPORT_V4=y`. This support ensures uninterrupted access for existing environments. However, XFS v4 is deprecated, and creating new v4 filesystems is strongly discouraged.

September 2030 is the EOL target for upstream Linux kernel support for XFS v4. Any release post-September 2030 based on updated upstream kernels will omit XFS v4 support entirely. Legacy v4 filesystems will no longer be mountable on those versions.

Upgrading underlying filesystems from v4 to v5 is transparent to applications and requires no changes to userspace software.

To check the format version of an existing XFS filesystem, run:

```
xfs_info /path/to/mountpoint
```

An output including `crc=1` indicates the modern v5 format, while `crc=0` indicates the legacy v4 format.

There is no in-place or online upgrade path from XFS v4 to v5. Migration requires backing up data, reformatting the block device to XFS v5, and restoring the content. Migrating the root filesystem and any other critical data partitions requires planned downtime.

The operating system generates warnings when v4 format interaction occurs:

- `mkfs.xfs` displays a warning if forced to format as v4 (`crc=0`):

  ```
  V4 filesystems are deprecated and will not be supported by future versions
  ```

- The kernel logs a notification upon mounting a v4 filesystem (printed once per boot cycle, upon first mount of a v4 filesystem):

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

5.12.2 NFS over TLS support

NFS over TLS is now supported for storage traffic.

5.12.3 Reusing LVM no longer default

The installer no longer tries to re-use existing LVM configurations. See the *Deployment Guide* at https://documentation.suse.com/sles/15-SP7/single-html/SLES-deployment/#yast-installer-reuse-lvm for more information.

5.12.4 LUKS2 support in the installer

LUKS2 is no longer technical preview but is now fully supported in YaST Partitioner.

For more information see the Partioning section of the *AutoYaST Guide* at https://documentation.suse.com/sles/15-SP7/single-html/SLES-autoyast/#CreateProfile-Partitioning

5.12.5 Comparison of supported file systems

SUSE Linux Enterprise was the first enterprise Linux distribution to support journaling file systems and logical volume managers in 2000. Later, we introduced XFS to Linux, which allows for reliable large-scale file systems, systems with heavy load, and multiple parallel reading and writing operations. With SUSE Linux Enterprise 12, we started using the copy-on-write file system Btrfs as the default for the operating system, to support system snapshots and rollback.

The following table lists the file systems supported by SUSE Linux Enterprise.

Support status: + supported / – unsupported

Feature	Btrfs	XFS	Ext4	OCFS 2[1]	GFS2
Supported in product	SLE	SLE	SLE	SLE HA	SLE
Data/metadata journaling	N/A[2]	– / +	+ / +	– / +	– / +
Journal internal/external	N/A[2]	+ / +	+ / +	+ / –	+ / –
Journal checksumming	N/A[2]	+	+	+	+
Subvolumes	+	–	–	–	–
Offline extend/shrink	+ / +	– / –	+ / +	+ / –[3]	+ / –[5]
Inode allocation map	B-tree	B+-tree	Table	B-tree	B-tree
Sparse files	+	+	+	+	+
Tail packing	–	–	–	–	–
Small files stored inline	+ (in metadata)	–	+ (in inode)	+ (in inode)	+ (in inode)
Defragmentation	+	+	+	+	–
Extended file attributes/ACLs	+ / +	+ / +	+ / +	+ / +	+ / +
User/group quotas	– / –	+ / +	+ / +	+ / +	+ / +
Project quotas	–	+	+	–	–
Subvolume quotas	+	N/A	N/A	N/A	N/A
Data dump/restore	–	+	–	–	–
Block size default	4 KiB[4]				

Feature	Btrfs	XFS	Ext4	OCFS 2[1]	GFS2
Maximum file system size	16 EiB	8 EiB	1 EiB	4 PiB	8 EiB
Maximum file size	16 EiB	8 EiB	1 EiB	4 PiB	8 EiB

[1] OCFS 2 is fully supported as part of the SUSE Linux Enterprise High Availability.

[2] Btrfs is a copy-on-write file system. Instead of journaling changes before writing them in-place, it writes them to a new location and then links the new location in. Until the last write, the changes are not "committed". Because of the nature of the file system, quotas are implemented based on subvolumes (`qgroups`).

[3] To extend an OCFS 2 file system, the cluster must be online but the file system itself must be unmounted.

[4] The block size default varies with different host architectures. 64 KiB is used on POWER, 4 KiB on other systems. The actual size used can be checked with the command `getconf PAGE_SIZE`.

[5] See `gfs2_grow(8)`. It must be a mounted filesystem.

Additional notes

Maximum file size above can be larger than the file system's actual size because of the use of sparse blocks. All standard file systems on SUSE Linux Enterprise Server have LFS, which gives a maximum file size of 2^{63} bytes in theory.

The numbers in the table above assume that the file systems are using a 4 KiB block size which is the most common standard. When using different block sizes, the results are different.

In this document:

- 1024 Bytes = 1 KiB
- 1024 KiB = 1 MiB;
- 1024 MiB = 1 GiB
- 1024 GiB = 1 TiB
- 1024 TiB = 1 PiB
- 1024 PiB = 1 EiB.

See also http://physics.nist.gov/cuu/Units/binary.html.

Some file system features are available in SUSE Linux Enterprise Server 15 SP7 but are not supported by SUSE. By default, the file system drivers in SUSE Linux Enterprise Server 15 SP7 will refuse mounting file systems that use unsupported features (in particular, in read-write mode). To enable unsupported features, set the module parameter `allow_unsupported=1` in `/etc/modprobe.d` or write the value `1` to `/sys/module/MODULE_NAME/parameters/allow_unsupported`. However, note that setting this option will render your kernel and thus your system unsupported.

5.12.6 Supported Btrfs features

The following table lists supported and unsupported Btrfs features across multiple SLES versions.

Support status: + supported / – unsupported

Feature	SLES 11 SP4	SLES 12 SP5	SLES 15 GA	SLES 15 SP1	SLES 15 SP2	SLES 15 SP3
Copy on write	+	+	+	+	+	+
Free space tree (Free Space Cache v2)	–	–	–	+	+	+
Snapshots/subvolumes	+	+	+	+	+	+
Swap files	–	–	–	+	+	+
Metadata integrity	+	+	+	+	+	+
Data integrity	+	+	+	+	+	+
Online metadata scrubbing	+	+	+	+	+	+
Automatic defragmentation	–	–	–	–	–	–
Manual defragmentation	+	+	+	+	+	+

Feature	SLES 11 SP4	SLES 12 SP5	SLES 15 GA	SLES 15 SP1	SLES 15 SP2	SLES 15 SP3
In-band deduplication	–	–	–	–	–	–
Out-of-band deduplication	+	+	+	+	+	+
Quota groups	+	+	+	+	+	+
Metadata duplication	+	+	+	+	+	+
Changing metadata UUID	–	–	–	+	+	+
Multiple devices	–	+	+	+	+	+
RAID 0	–	+	+	+	+	+
RAID 1	–	+	+	+	+	+
RAID 5	–	–	–	–	–	–
RAID 6	–	–	–	–	–	–
RAID 10	–	+	+	+	+	+
Hot add/remove	–	+	+	+	+	+
Device replace	–	–	–	–	–	–
Seeding devices	–	–	–	–	–	–
Compression	–	+	+	+	+	+
Big metadata blocks	–	+	+	+	+	+
Skinny metadata	–	+	+	+	+	+

Feature	SLES 11 SP4	SLES 12 SP5	SLES 15 GA	SLES 15 SP1	SLES 15 SP2	SLES 15 SP3
Send without file data	–	+	+	+	+	+
Send/receive	–	+	+	+	+	+
Inode cache	–	–	–	–	–	–
Fallocate with hole punch	–	+	+	+	+	+

5.13 SUSE Package Hub

SUSE Package Hub brings open-source software packages from openSUSE to SUSE Linux Enterprise Server and SUSE Linux Enterprise Desktop.

Usage of software from SUSE Package Hub is not covered by SUSE support agreements. At the same time, usage of software from SUSE Package Hub does not affect the support status of your SUSE Linux Enterprise systems. SUSE Package Hub is available at no additional cost and without an extra registration key.

5.13.1 KDE migration issue

Installing the full KDE Plasma Desktop (using the `kde` pattern) requires an extra subscription for the Workstation Extension. Upgrading to 15 SP7 might fail if you have the `kde` pattern installed but do not have the required subscription.

A new `kde_minimal` pattern provides the KDE Plasma Desktop with fewer packages and does not require the Workstation Extension subscription. If your upgrade fails because of the missing subscription, finish the upgrade, then run these commands:

```
zypper rm -t pattern kde
zypper in -t pattern kde_minimal
```

5.14 System management

5.14.1 Support for regular user accounts in container UID ranges

Previously, systemd expected regular user accounts to be allocated within the UID range of 1000 to 60000. If user accounts were created with UIDs in the container range (524288 to 1879048191), journald would route their log messages to the system journal. As a result, these users could not access their own log messages via `journalctl` without administrator privileges. To address this, SUSE's systemd has been updated to treat UIDs in the container range as regular users. User-specific journals are now correctly created for these accounts, allowing them to view their log messages using `journalctl` without special group memberships.

5.14.2 Effective user limits in systemd setup

Before, the lookup of the effective session limit in a systemd setup was not trivial. Now these new properties have been added:

- `EffectiveMemoryMax`
- `EffectiveMemoryHigh`
- `EffectiveTasksMax`

5.14.3 Repository Mirroring Tool (RMT) updated to version 3

A maintenance update changes the `rmt-server` package from version 2 to version 3.1. RMT 3 uses Ruby 3.4 and Rails 7.1. RMT 2 uses Ruby 2.5, which is no longer maintained.

5.14.4 Searching packages across all SLE modules

In SLE 15 SP7 you can search for packages both within and outside of currently enabled SLE modules using the following command:

```
zypper search-packages SEARCH_TERM
```

This command contacts the SCC and searches all modules for matching packages. This functionality makes it easier for administrators and system architects to find the software packages needed. This feature is now also available when a system is registered against RMT.

5.14.5 Support for global service variables in /etc/sysconfig/service deprecated or removed

The configuration file `/etc/sysconfig/service` previously let system administrators control service updates globally. It contained the variables `DISABLE_RESTART_ON_UPDATE` and `DISABLE_STOP_ON_REMOVAL`. However, global service management can lead to inconsistent system states. It also prevents packages from applying security updates correctly. Therefore, the `DISABLE_STOP_ON_REMOVAL` variable has been removed. The `DISABLE_RESTART_ON_UPDATE` variable has also been deprecated. If a specific service must not restart or stop automatically, configure this behavior at the package level instead. Do not use global options in `/etc/sysconfig/service`.

5.14.6 HPC module package updates

The High Performance Computing (HPC) module has been updated with new package versions for `openmpi`, `lmod` (provided by the `lua-lmod` package), `genders`, and `munge`.

5.14.6.1 OpenMPI

OpenMPI now supports the Gridware Cluster Scheduler (Grid Engine) out-of-the-box. This update configures OpenMPI packages with the `--with-sge` parameter. Previously, OpenMPI only supported the Slurm workload manager out-of-the-box.

5.14.6.2 `lmod`

The `lmod` package has been updated to version 8.7.55. This update introduces the following changes:

- Added a warning when running `module use --help`.
- Configured `LMOD_IGNORE_CACHE` to use the yes/no environment variable setting system.
- Made `module --terse show <module>` print the location of the module, matching the behavior of `module --loc show <module>`.
- Added support for `module --terse spider phdf5/1.12.2` to print only the module in the hierarchy.

- Configured the build time to be reported in UTC when `$SOURCE_DATE_EPOCH` is set.
- Added support for downstream conflicts.
- Added support for dynamic `LMOD_MODULERC` configurations.
- Added the new function `depends_on_any()`.
  If `$MODULES_AUTO_HANDLING` is set, `prereq()` behaves like `depends_on()`, and `prereq_any()` behaves like `depends_on_any()`.
- Modified `ModuleTable` to store changes to `$MODULEPATH` in an entry.
- Added support for `terse avail` extensions.
- Added support for `LMOD_FILE_IGNORE_PATTERNS` to ignore files such as `.version.1.3` or `.modulerc-1.3.lua`.
- Renamed `--hidden_load` to `--hidden-loaded` (for TCL) and `hidden_load` to `hidden_loaded` (for Lua).
- Configured `dofile()` usage to be reported as an error.
- Updated `FPATH` support so that bash and ksh add the path (`init/ksh_funcs`) to `FPATH`.
- Updated zsh initialization to set `__zsh_fpath` using a sub-shell if `autoload` and `compinit` fail.
- Improved `addto` to prevent duplicate entries in path-like variables such as `PATH` and `FPATH`.
- Added support for `--dumpname` in `lmod` and `ml`, and updated the tab completion files.
- Prevented resetting of `BASH_ENV` in csh and bash initialization scripts if it is already set.
- Added support for `hide{}` and `forbid{}` functions.
- Configured reverse maps for `mod2versionT` and `full2aliasesT` to be built dynamically.
- Added support for the `LMOD_SHOW_HIDDEN` environment variable.
- Configured TCL files to run in `spider` mode matching when Lmod is in spider mode.
- Improved the test for spaces in front of `#`.
- Fixed a prepend and append path bug when attempting to add an empty string.

- Fixed a `serializeTbl` bug to handle empty or single blank strings as keys.
- Fixed the setting of `$FPATH` when running bash or ksh shell and executing `zsh -l`.
- Fixed shell syntax in the bash initialization script.

5.14.6.3 `genders`

The `genders` package has been updated to version 1.29.1. This update introduces the following changes:

- Increased the internal buffer size in `nodeattr` to support large cluster hostranges.

5.14.6.4 `munge`

The `munge` package has been updated to version 0.5.16. This update introduces the following changes:

- Fixed a connect failure retry issue when the socket listen queue is full.
- Added the `--listen-backlog` command-line option to `munged` to specify the socket's listen backlog limit. Check `man 8 munged` for details.
- The release is backwards-compatible to version 0.5. Credentials encoded with the current default of `MUNGE*MAC*SHA256` can be decoded by all releases of `munge` on all supported SUSE Linux Enterprise versions.

5.14.6.5 Bootable container image for compute nodes

To improve the user experience when deploying cluster nodes with `warewulf4`, a bootable container image is now available through `registry.suse.com`. The image contains the components missing from standard container images that are necessary for a system to boot, most notably a kernel and `systemd`. Subscribed customers can consume this image directly, removing the need to manually add a kernel to the container image and create a system overlay.

5.14.6.6 Warewulf 4.6.x

- Update to Warewulf version 4.6.x with the following changes:

  - Default values in `nodes.conf`:
    Warewulf 4.6.x removes implicit default values for the following configuration options:

    - Kernel command line
    - Initialization parameters
    - Root
      These values are now defined in the `default` profile. Include this profile in all other profiles. The installation process automatically upgrades `nodes.conf` to update the database.

  - Split overlays:
    The overlays `wwinit` and `runtime` are now split into separate, function-specific overlays. The upgrade process automatically updates the node database. This process replaces `wwinit` and `runtime` with a list of overlays that perform the same functions.

  - Site-specific and distribution overlays:
    Do not modify overlays in `/var/lib/warewulf/overlays`. Store site-specific overlays in `/etc/warewulf/overlays` instead. During an upgrade, modified overlays are saved with the `.rpmsave` suffix and moved to `/etc/warewulf/overlays/`*`OVERLAY_NAME`*.

  - Package split:
    The `warewulf` suite is now split into the following packages:

    `warewulf4`
    : The base package. It contains the main binary and configuration files.

    `warewulf4-overlays`
    : Contains the overlay files to configure the Warewulf host and nodes. These files are required.

    `warewulf4-man`
    : Contains the manual pages.

`warewulf4-dracut`

Required on the node image only when using `dracut` during deployment. Default installations do not require this package.

`warewulf4-reference-doc`

Contains the documentation as a PDF document.

`warewulf4-overlays-slurm`

Contains an overlay to simplify the installation of the Slurm workload manager.

5.15 Virtualization

For more information about acronyms used below, see https://documentation.suse.com/sles/15-SP7/html/SLES-all/book-virtualization.html.

Important: Virtualization limits and supported hosts/guests

These release notes only document changes in virtualization support compared to the immediate previous service pack of SUSE Linux Enterprise Server. Full information regarding virtualization limits for KVM and Xen as well as supported guest and host systems is now available as part of the SUSE Linux Enterprise Server documentation.

See the *Virtualization Guide* at https://documentation.suse.com/sles/15-SP7/html/SLES-all/cha-virt-support.html.

5.15.1 Xen

Xen has been updated to version 4.20, for more information: https://wiki.xenproject.org/wiki/Xen_Project_4.20_Release_Notes

5.15.2 QEMU

QEMU has been updated to version 9.2.2, full list of changes are available at https://wiki.qemu.org/ChangeLog/9.2

Highlights include:

- Removed features: https://qemu-project.gitlab.io/qemu/about/removed-features.html
- Deprecated features: https://qemu-project.gitlab.io/qemu/about/deprecated.html

5.15.3 libvirt

`libvirt` has been updated to version 11.0.0, this include many incremental improvements and bug fixes, see https://libvirt.org/news.html#v11-0-0-2025-01-15

Since SP6 `libvirt` provides two daemon deployment options: monolithic or modular daemons. Modular daemons are now enabled by default, but a deployment can be switched to the traditional monolithic daemon by disabling the individual daemons and enabling `libvirtd`.

5.15.4 VMware

5.15.4.1 open-vm-tools

`open-vm-tools` has been updated to version 12.5.0 that addresses a few critical problems and bug fixes. See https://github.com/vmware/open-vm-tools/blob/stable-12.5.0/ReleaseNotes.md

5.15.5 Others

5.15.5.1 NVIDIA GRID

Support for NVIDIA Virtual GPU (vGPU) v16.10 has been added, including migration under some specific scenarios.

5.15.5.2 sanlock

`sanlock` has been removed.

5.15.5.3 libguestfs

`libguestfs` has been updated to version 1.55.6.

5.15.5.4 virt-v2v

Update to version 2.7.7. Some of the changes include:

- Implement --parallel = N for parallel disk copies
- Update Translations
- Various fixes

5.15.5.5 `sevctl`

The `sevctl` package has been updated to version 0.6.0.

5.15.5.6 `snpguest`

The `snpguest` package has been updated to version 7.1.

5.15.5.7 AMD SEV-SNP guest support

SUSE Linux Enterprise Server 15 SP7 now fully supports AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) guest support. Before SLES 15 SP7, this feature was available as a Technology Preview. AMD SEV-SNP provides strong memory encryption, memory integrity protection, and virtualization isolation for virtual machines running under KVM.

5.15.5.8 `virtiofsd`

The `virtiofsd` has been updated to 1.12.0.

5.15.5.9 Kubevirt support

We provide L3 support for KubeVirt in SLES 15 SP7. It is supported for the lifecycle of the product only if you are using the latest version update (N + 1) or version N available. KubeVirt is not supported in via LTSS / Extended.

If you'd like to report a bug with KubeVirt, use the following components in Bugzilla: `KVM stack: QEMU/KVM, libvirt, virt-manager, kubevirt`.

5.15.5.10 KubeVirt support for AMD SEV and SEV-ES

We now provide AMD Secure Encrypted Virtualization (SEV) and Secure Encrypted Virtualization-Encrypted State (SEV-ES) support for KubeVirt. This support allows you to secure guest virtual machines with memory encryption. You can now run encrypted container-native virtualization workloads.

5.15.6 limitations

5.15.6.1 virt-install option "--cdrom" can not work with the SEV environment

This issue only occurs when installing an .iso file via CD-ROM. It is because the external device is not trusted by default from the Guest's perspective under the SEV environment.

SUSE has reported to upstream via https://github.com/tianocore/edk2/issues/11035

Possible workarounds:

- Using '--location' option instead of '--cdrom'.
- Using a pre-existing disk image (like qcow2) or performing a network installation via PXE.
- Disable SEV for guest installation, then user can enable SEV after guest installed.

6 AMD64/Intel 64-specific changes (x86-64)

Information in this section applies to SUSE Linux Enterprise Server 15 SP7 for the AMD64/Intel 64 architectures.

6.1 System-specific and vendor-specific information

6.1.1 Intel Clearwater Forest processor support

SLES 15 SP7 adds support for the Intel Clearwater Forest (CWF) processor.

7 POWER-specific changes (ppc64le)

Information in this section applies to SUSE Linux Enterprise Server for POWER 15 SP7.

7.1 Storage

7.1.1 DLPAR remove operation fails with Emulex FC adapters

Broadcom Emulex Fibre Channel (FC) adapters might fail to be properly removed with DLPAR operations in SUSE Linux Enterprise Server 15 SP7. All POWER 9 and Power10 systems with any Emulex FC adapter are affected.

When you perform DLPAR remove operations on Emulex FC adapters, there is a possibility that the adapter is not properly removed from the system. This operation can cause future DLPAR operations to fail. A failing system can show the following error messages:

```
EEH: Recovering PHB#204-PE#800000
EEH: PE location: N/A, PHB location: N/A
EEH: Frozen PHB#204-PE#800000 detected
EEH: Call Trace:
EEH: [c00000000005674c] __eeh_send_failure_event+0x6c/0x120
EEH: [c00000000004f8a0] eeh_dev_check_failure+0x270/0x6b0
EEH: [c00000000004fd78] eeh_check_failure+0x98/0x110
EEH: [c008000023ba6e00] lpfc_sli4_wait_bmbx_ready+0x118/0x1c0 [lpfc]
EEH: [c008000023ba702c] lpfc_sli4_post_sync_mbox+0x184/0x5a0 [lpfc]
EEH: [c008000023ba99ac] lpfc_sli_issue_mbox_s4+0x7a4/0xce0 [lpfc]
EEH: [c008000023bb4574] lpfc_sli_issue_mbox+0x2c/0x50 [lpfc]
EEH: [c008000023c0220c] __lpfc_reg_congestion_buf+0xd4/0x1d0 [lpfc]
EEH: [c008000023c0ef58] lpfc_pci_remove_one+0xc0/0xe50 [lpfc]
EEH: [c000000000983dc4] pci_device_remove+0x64/0x110
EEH: [c000000000b0a7e4] device_remove+0x74/0xd0
EEH: [c000000000b0c350] device_release_driver_internal+0x120/0x210
EEH: [c000000000974b98] pci_stop_bus_device+0x98/0xf0
EEH: [c000000000974db8] pci_stop_and_remove_bus_device+0x28/0x40
EEH: [c000000000077df0] pci_hp_remove_devices+0x90/0x130
EEH: [c008000026510568] disable_slot+0x40/0x90 [rpaphp]
EEH: [c0000000009abaf8] power_write_file+0xa8/0x170
EEH: [c0000000009a1504] pci_slot_attr_store+0x44/0x60
EEH: [c0000000006a2ed4] sysfs_kf_write+0x64/0x90
EEH: [c0000000006a19e4] kernfs_fop_write_iter+0x204/0x2b0
EEH: [c0000000005a378c] vfs_write+0x36c/0x440
EEH: [c0000000005a3a8c] ksys_write+0xdc/0x130
```

```
EEH: [c000000000034b18] system_call_exception+0x158/0x320
EEH: [c00000000000d05c] system_call_vectored_common+0x15c/0x2ec
Kernel attempted to read user page (18) - exploit attempt? (uid: 0)
BUG: Kernel NULL pointer dereference on read at 0x00000018
Faulting instruction address: 0xc008000023baf314
Oops: Kernel access of bad area, sig: 11 [#1]
```

There is currently no workaround nor fix available for this issue. Instead of using the DLPAR operation, you can shutdown the logical partition before you remove or add Emulex FC adapters to the configuration.

7.2 Miscellaneous

7.2.1 Out of memory during installation

There is a limit on the memory available to the GRUB bootloader. The installer ramdisk is particularly large because it includes kernel drivers for all possible installation scenarios as well as tools for loading the installer from different types of media. Enabling secure boot and vTPM on the LPAR further increases memory requirements.

When loading the OS from the installation medium the following message might appear:

```
Loading kernel ...
Loading initial ramdisk ...
error: ../../grub-core/kern/mm.c:548:out of memory.

Press any key to continue...
```

The recommended workaround is to disable vTPM support during installation.

7.2.2 Increased minimum RAM requirement for installation

Due to the use of uncompressed kernel modules in the initial ramdisk (initrd), the memory required during the installation process has increased. If the system has less than 2 GB of RAM, the installation might fail with errors such as `Initramfs unpacking failed: write error` or a kernel panic. To ensure a successful installation, the minimum RAM requirement for SUSE Linux Enterprise Server for POWER has been raised from 1 GB to 2 GB. This change applies to both SLES 15 SP6 and SLES 15 SP7.

8 IBM Z-specific changes (s390x)

Information in this section applies to SUSE Linux Enterprise Server for IBM Z and LinuxONE 15 SP7. For more information, see https://www.ibm.com/docs/en/linux-on-systems?topic=distributions-suse-linux-enterprise-server

8.1 Hardware

8.1.1 Valgrind: Support for IBM z17 Hardware

Valgrind has been updated to support IBM z17 processor instructions. This allows profiling and debugging of applications built for the new IBM Z hardware.

8.2 Security

8.2.1 `paes-xts-plain64` cipher now supported for disk encryption during installation

SLES 15 SP7 now allows selecting the `paes-xts-plain64` cipher for disk encryption in the YaST partitioner. This feature requires a Crypto Express adapter. The adapter can operate in CCA or EP11 mode. EP11 mode specifically needs a CEX7S adapter or newer.

When using LUKS2, you can choose between an AES data key or an AES cipher key. The crypto adapter must be correctly configured before installation. For configuration details, see https://www.ibm.com/docs/en/linux-on-systems?topic=utilities-master-key-administration.

8.2.2 Secure boot IPL requirements

Secure boot IPL has the following minimum system requirements, depending on the boot device to be IPLed:

- NVMe disk: IBM LinuxONE III or newer.
- FC-attached SCSI disk: IBM LinuxONE III, IBM z15 or newer.
- ECKD DASD with CDL layout: IBM z16, LinuxONE 4 or newer.

If these requirements are not met, the system can be IPLed in non-secure mode only.

8.3 Miscellaneous

8.3.1 Plymouth dropped from s390x image

Plymouth has been dropped from the s390x image. When running a bare metal installation on IBM Z (s390x) with a fully encrypted disk, the password prompt to decrypt the disk is now correctly shown in the HMC terminal (Operating Messages). The previous workaround of adding `plymouth.enable=0` to the boot command line is no longer required.

9 Arm 64-bit-specific changes (AArch64)

Information in this section applies to SUSE Linux Enterprise Server for Arm 15 SP7.

9.1 System-on-Chip driver enablement

SUSE Linux Enterprise Server for Arm 15 SP7 includes driver enablement for the following System-on-Chip (SoC) chipsets:

- AMD* Opteron* A1100
- Ampere* X-Gene*, eMAG*, Altra*, *Altra Max*, AmpereOne*
- AWS* Graviton, Graviton2, Graviton3
- Broadcom* BCM2837/BCM2710, BCM2711
- Fujitsu* A64FX
- Huawei* Kunpeng* 916, Kunpeng 920
- Marvell* ThunderX*, ThunderX2*; OCTEON TX*; Armada* 7040, Armada 8040
- NVIDIA* Grace; Tegra* X1, Tegra X2, Xavier*, Orin; BlueField*, *BlueField-2*
- NXP* i.MX 8M, 8M Mini; Layerscape* LS1012A, LS1027A/LS1017A, LS1028A/LS1018A, LS1043A, LS1046A, LS1088A, LS2080A/LS2040A, LS2088A, LX2160A

- Qualcomm* Centriq* 2400
- Rockchip RK3399
- Socionext* SynQuacer* SC2A11
- Xilinx* Zynq* UltraScale* + MPSoC



Note

Driver enablement is done as far as available and requested. Refer to the following sections for any known limitations.

Some systems might need additional drivers for external chips, such as a Power Management Integrated Chip (PMIC), which may differ between systems with the same SoC chipset.

For booting, systems need to fulfill either the Server Base Boot Requirements (SBBR) or the Embedded Base Boot Requirements (EBBR), that is, the Unified Extensible Firmware Interface (UEFI) either implementing the Advanced Configuration and Power Interface (ACPI) or providing a Flat Device Tree (FDT) table. If both are implemented, the kernel will default to the Device Tree; the kernel command line argument `acpi=force` can override this default behavior.

Check for SUSE *YES!* certified systems, which have undergone compatibility testing.

9.2 New features

9.2.1 Memory Tagging in GNU C Library

SUSE Linux Enterprise Server for Arm 15 SP4 and SP5 prepared their kernels for the Armv8.5 Memory Tagging Extension (`FEAT_MTE`). Their `glibc` packages were based on version 2.31 and did not yet support Memory Tagging.

SUSE Linux Enterprise Server for Arm 15 SP7 updates `glibc` base version to 2.38 and enables Memory Tagging in the GNU C Library as well.

9.3 Changed kernel `CONFIG_HZ` value

SUSE Linux Enterprise Server for Arm 15 SP6 and earlier kernels have used a `CONFIG_HZ` value of 100 Hz.

The SUSE Linux Enterprise Server for Arm 15 SP7 kernel instead uses a value of 250 Hz. This matches the latest default and the value for x86-64 architecture (*Section 5.7.5, "`CONFIG_HZ` value changes"*).

9.4 Changed kernel I/O MMU default

SUSE Linux Enterprise Server for Arm 15 SP6 and earlier kernels have defaulted the I/O MMU (Input/Output Memory Management Unit) to **passthrough** mode. This was the most performant setting, but did not work on all machines. It then required the user to override the default via `iommu.passthrough=0` kernel command line option.

SUSE Linux Enterprise Server for Arm 15 SP7 kernel instead defaults to **translated** mode. This achieves a greater hardware compatibility.

To force the previous behavior, use the kernel command line option `iommu.passthrough=1`.

9.5 64K page size kernel flavor is supported

SUSE Linux Enterprise Server for Arm 12 SP2 and later kernels have used a page size of 4K. This offers the widest compatibility also for small systems with little RAM, allowing to use Transparent Huge Pages (THP) where large pages make sense.

As a technology preview, SUSE Linux Enterprise Server for Arm 15 SP3 added a kernel flavor `64kb`, offering a page size of 64 KiB and physical/virtual address size of 52 bits. Same as the `default` kernel flavor, it does not use preemption.

SUSE Linux Enterprise Server for Arm 15 SP6 largely removed this technology preview status, offering support for `kernel-64kb` on select platforms, such as NVIDIA Grace*. KVM virtualization remains a technology preview on this `64kb` kernel flavor (*Section 2.8.1.1, "KVM virtualization with 64K page size kernel flavor"*).



Note: Default file system no longer needs to be changed

SUSE Linux Enterprise Server for Arm 15 SP7 SP4 and later allow the use of Btrfs based file systems with 4 KiB block size also with 64 KiB page size kernels.

Important: Swap needs to be re-initialized

After booting the 64K kernel, any swap partitions need to re-initialized to be usable. To do this, run the `swapon` command with the `--fixpgsz` parameter on the swap partition. Note that this process deletes data present in the swap partition (for example, suspend data). In this example, the swap partition is on `/dev/sdc1`:

```
swapon --fixpgsz /dev/sdc1
```

Warning: RAID 5 uses page size as stripe size

It is currently possible to configure stripe size by setting the following kernel parameter:

```
echo 16384 > /sys/block/md1/md/stripe_size
```

Keep in mind that `stripe_size` must be in multiples of 4KB and not bigger than `PAGE_SIZE`. Also, it is only supported on systems where `PAGE_SIZE` is not 4096, such as arm64.

Avoid RAID 5 volumes when benchmarking 64K vs. 4K page size kernels.

See the *Storage Guide* for more information on software RAID.

Note: Cross-architecture compatibility considerations

The SUSE Linux Enterprise Server 15 SP7 kernels on x86-64 use 4K page size.

The SUSE Linux Enterprise Server for POWER 15 SP7 kernel uses 64K page size.

9.6 Known limitations

9.6.1 No graphics drivers on NVIDIA Grace Hopper

The NVIDIA Grace Hopper* System-on-Chip contains an integrated, *Hopper* microarchitecture-based Graphics Processor Unit (GPU).

SUSE Linux Enterprise Server for Arm 15 SP7 maintenance updates currently provide packages `nvidia-open-driver-G06-signed-kmp-default` and `kernel-firmware-nvidia-gspx-G06` in version `535.104.05`, which does not yet enable NVIDIA Grace Hopper GH200.

Check for maintenance updates of those packages with version `545.29.02` or later, or contact the system vendor or chip vendor NVIDIA for whether third-party graphics drivers are available for SUSE Linux Enterprise Server for Arm 15 SP7.



Note: PCIe GPUs not affected

Discrete GPU cards with *Hopper* microarchitecture, such as NVIDIA H100, are already enabled in shipping package versions.

9.6.2 No graphics drivers on NVIDIA Jetson

The NVIDIA* Tegra* System-on-Chip chipsets include an integrated Graphics Processor Unit (GPU).

SUSE Linux Enterprise Server for Arm 15 SP7 does not include graphics drivers for any of the NVIDIA Jetson*, NVIDIA IGX or NVIDIA DRIVE* platforms.

Contact the chip vendor NVIDIA for whether third-party graphics drivers are available for SUSE Linux Enterprise Server for Arm 15 SP7.

9.6.3 No DisplayPort graphics output on NXP LS1028A and LS1018A

The NXP* Layerscape* LS1028A/LS1018A System-on-Chip contains an Arm* Mali*-DP500 Display Processor, whose output is connected to a DisplayPort* TX Controller (HDP-TX) based on Cadence* High Definition (HD) Display Intellectual Property (IP).

A Display Rendering Manager (DRM) driver for the Arm Mali-DP500 Display Processor is available as technology preview (*Section 2.8.1.5, “mali-dp driver for Arm Mali Display Processors available”*).

However, there was no HDP-TX physical-layer (PHY) controller driver ready yet. Therefore no graphics output will be available, for example, on the DisplayPort* connector of the NXP LS1028A Reference Design Board (RDB).

Contact the chip vendor NXP for whether third-party graphics drivers are available for SUSE Linux Enterprise Server for Arm 15 SP7.

Alternatively, contact your hardware vendor for whether a bootloader update is available that implements graphics output, allowing to instead use `efifb` framebuffer graphics in SUSE Linux Enterprise Server for Arm 15 SP7.



Note

The Vivante GC7000UL GPU driver (`etnaviv`) is available as a technology preview (*Section 2.8.1.3, "etnaviv drivers for Vivante GPUs are available"*).

10 Removed and deprecated features and packages

This section lists features and packages that were removed from SUSE Linux Enterprise Server or will be removed in upcoming versions.



Note: Package and module changes in 15 SP7

For more information about all package and module changes since the last version, see *Section 2.2.3, "Package and module changes in 15 SP7"*.

10.1 Removed features and packages

The following features and packages have been removed in this release.

- The `haveged-switch-root.service` has been removed. For more information, see *Section 5.11.1, "haveged switch-root service removed"*.
- removed the `KBD_DISABLE_CAPS_LOCK` feature from `/etc/sysconfig/keyboard`
- `intel-opencl` and `intel-graphics-compiler` packages have been moved to SUSE Package Hub after being deprecated in 15 SP6.
- `redis` has been removed in SLES 15 SP7 and will not be supported in SLES 15 after June 2031. Use `valkey` instead.
- `ntp` has been moved to the *Legacy Module* and will be removed in SLES 16.0. Use `chrony` instead.
- PHP 7.4 has been removed.
- `numad` has been removed.

10.1.1 Removal of Intel True Scale support (PSM1)

Support for Intel's True Scale fabric hardware (PSM1) has been removed. The `libpsm_infinipath1`, `libinfinipath4`, and `infinipath-psm-devel` packages have been removed from the distribution. Related software packages like `libfabric`, `openmpi`, and `mvapich` have been rebuilt to remove True Scale support. For modern Omni-Path (OPA) fabrics, use `libpsm2` instead.

10.2 ceph client packages moved to Legacy Module

The following `ceph` client packages have been moved to Legacy Module:

- `ceph-common`
- `libcephfs-devel`
- `python3-ceph-common`
- `python3-rbd`
- `python3-rgw`

10.2.1 OpenLDAP server

The release notes for SUSE Linux Enterprise Server 15 SP4-SP6 stated that the OpenLDAP server package was deprecated and would be removed in favor of the 389 Directory Server (`389-ds`). Based on customer feedback, OpenLDAP server was reintroduced in SLES to provide an extended migration period to the 389 Directory Server. While the OpenLDAP server is available in SLES 15 SP7, we continue to strongly recommend that customers migrate to the `389-ds` package. The inclusion of OpenLDAP server is designed to facilitate a smoother transition and neither should it be considered for new deployments, nor it is planned to be included in SLES 16.0.

10.2.2 `intel-opencl` and `intel-graphics-compiler` packages removal

Since SLE15 SP5, Intel stopped requesting updates for `intel-opencl` and `intel-graphics-compiler` packages, and thus the packages have been deprecated in 15 SP6. They have now been removed from 15 SP7, and moved to Package Hub.

10.3 Deprecated features and packages

The following features and packages are deprecated and will be removed in a future version of SUSE Linux Enterprise Server.

- Legacy XFS v4 filesystems are deprecated. For details, see *Section 5.12.1, "Deprecation of legacy XFS v4 filesystem format"*.
- NIS is deprecated and will be removed with the next major version of SUSE Linux Enterprise Server. This includes packages implementing NIS, like `ypserv`. NIS code will be removed from SUSE tools and all NIS client code will be dropped with the next major version of SUSE Linux Enterprise Server.
- The standalone `wire` package is deprecated and will not receive further updates. Grafana now vendors the `wire` package internally.
- `netiucv` and `lcs` drivers have been deprecated and will be removed in SLES 16.
- The 2MB OVMF image will be deprecated and removed in SLES 16.1.

11 Obtaining source code

This SUSE product includes materials licensed to SUSE under the GNU General Public License (GPL). The GPL requires SUSE to provide the source code that corresponds to the GPL-licensed material. The source code is available for download at https://www.suse.com/products/server/download/ on Medium 2. For up to three years after distribution of the SUSE product, upon request, SUSE will mail a copy of the source code. Send requests by e-mail to sle_source_request@suse.com (mailto:sle_source_request@suse.com). SUSE may charge a reasonable fee to recover distribution costs.

12 Legal notices

SUSE makes no representations or warranties with regard to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, SUSE reserves the right to revise this publication and to make changes to its content, at any time, without the obligation to notify any person or entity of such revisions or changes.

Further, SUSE makes no representations or warranties with regard to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, SUSE reserves the right to make changes to any and all parts of SUSE software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classifications to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical/biological weaponry end uses. Refer to https://www.suse.com/company/legal/ for more information on exporting SUSE software. SUSE assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2010-2026 SUSE LLC.

This release notes document is licensed under a Creative Commons Attribution-NoDerivatives 4.0 International License (CC-BY-ND-4.0). You should have received a copy of the license along with this document. If not, see https://creativecommons.org/licenses/by-nd/4.0/.

SUSE has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at https://www.suse.com/company/legal/ and one or more additional patents or pending patent applications in the U.S. and other countries.

For SUSE trademarks, see the SUSE Trademark and Service Mark list (https://www.suse.com/company/legal/). All third-party trademarks are the property of their respective owners.

13 Changelog for 15 SP7

13.1 2026-10-01

13.1.1 Updated

- Converted appendices to regular sections to improve navigation in single-page HTML.
- Replaced screenshot with console error text in *Section 7.1.1, "DLPAR remove operation fails with Emulex FC adapters"* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1222895)).
- Fixed link to RMT Guide in *Section 4, "Installation and upgrade"*.

13.1.2 New

- Added note about krb5 deprecated encryption types disabled by default (*Section 5.1.1, "krb5: Deprecated Encryption Types Disabled by Default"*, Jira (https://jira.suse.com/browse/PED-13712)).
- Added OpenJDK 25 to *Section 5.5.8, "Supported Java versions"* and *Section 2.6.2.1, "Java lifecycle support"* (Jira (https://jira.suse.com/browse/PED-14233)).
- Corrected the OpenJDK 21 support end to 2034-07-31 in *Section 5.5.8, "Supported Java versions"* (Jira (https://jira.suse.com/browse/PED-1590)).
- Corrected the IBM Java availability in *Section 2.6.2.1, "Java lifecycle support"* and *Section 10, "Removed and deprecated features and packages"* (Jira (https://jira.suse.com/browse/PED-13389)).
- Added note about squid ESI processing disabling (*Section 5.11.2, "squid: ESI processing disabled"*, Jira (https://jira.suse.com/browse/PED-15619), Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1232485)).
- Added note about disabling the clocksource watchdog on HPE UV5 platforms (*Section 5.7.8, "Clocksource watchdog disabled on HPE UV5 platforms"*, Jira (https://jira.suse.com/browse/PED-16395)).

- Added note about Valgrind support for IBM z17 hardware instructions (*Section 8.1.1, "Valgrind: Support for IBM z17 Hardware"*, Jira (https://jira.suse.com/browse/PED-16489)).
- Added note about deprecation and removal of global service options in `/etc/sysconfig/service` (*Section 5.14.5, "Support for global service variables in /etc/sysconfig/service deprecated or removed"*, Jira (https://jira.suse.com/browse/PED-6231)).
- Added note about OpenMPI support for Gridware Cluster Scheduler (Grid Engine) (*Section 5.14.6.1, "OpenMPI"*, Jira (https://jira.suse.com/browse/PED-13377)).
- Added note about the RMT update to version 3 (*Section 5.14.3, "Repository Mirroring Tool (RMT) updated to version 3"*, Jira (https://jira.suse.com/browse/PED-16425)).
- Added note about the addition of the `python311-apache-libcloud` package (*Section 5.5.1, "`python311-apache-libcloud` package added"*, Jira (https://jira.suse.com/browse/PED-14451), Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1257268)).
- Added note about `systemd-resolved` package split to *Section 5.9.4, "`systemd-resolved` packaged separately"* (Jira (https://jira.suse.com/browse/PED-12690)).
- Added note about Warewulf 4.6.x updates to *Section 5.14.6.6, "Warewulf 4.6.x"* (Jira (https://jira.suse.com/browse/PED-12409)).
- Added note about direct upgrade support from SLES 12 SP5 LTSS to SLES 15 15 SP7 (*Section 4.2.6, "Direct upgrade from SLES 12 SP5 LTSS to SLES 15 15 SP7 is supported"*, Jira (https://jira.suse.com/browse/PED-7994)).
- Added note about quarterly updates for SUSE Linux Enterprise Server 15 SP7 to *Section 2.6.1, "Quarterly updates"* (Jira (https://jira.suse.com/browse/PED-14584)).
- Added note about AMD SEV and SEV-ES support for KubeVirt to *Section 5.15.5.10, "KubeVirt support for AMD SEV and SEV-ES"* (Jira (https://jira.suse.com/browse/SLE-23244)).
- Added link to the Public Cloud Information Tracker (PINT) to *Section 2.5, "Documentation and other information"* (Jira (https://jira.suse.com/browse/DOCTEAM-351)).
- Added note about `haveged-switch-root.service` removal and replacement to *Section 5.11.1, "`haveged` switch-root service removed"* (Jira (https://jira.suse.com/browse/PED-6185)).
- Added note about Intel True Scale support removal to *Section 10, "Removed and deprecated features and packages"* (Jira (https://jira.suse.com/browse/PED-5615), Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1212146)).

- Added legacy XFS v4 format deprecation notice to *Section 10, "Removed and deprecated features and packages"* and *Section 5.12.1, "Deprecation of legacy XFS v4 filesystem format"* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1275537), Jira (https://jira.suse.com/browse/DOCTEAM-2174)).
- *Section 5.14.6.5, "Bootable container image for compute nodes"* (Jira (https://jira.suse.com/browse/PED-8142))
- Added note about container UID ranges used for regular user accounts (*Section 5.14.1, "Support for regular user accounts in container UID ranges"*, Jira (https://jira.suse.com/browse/PED-15595)).
- Added note about HPC package updates for Lmod, Genders, and MUNGE (*Section 5.14.6, "HPC module package updates"*, Jira (https://jira.suse.com/browse/PED-12466), Jira (https://jira.suse.com/browse/PED-12468)).
- Added reference to supplementary SUSE Linux Enterprise High Performance Computing release notes under *Section 2.2.4, "SLE HPC HPC no longer a separate product"* (Jira (https://jira.suse.com/browse/PED-7876)).
- Added note about ClamAV 1.0 update to *Section 5.10.1, "ClamAV has been updated to version 1.0"* (Jira (https://jira.suse.com/browse/PED-4597)).
- Added note about Node.js 24 default version (*Section 5.5.7, "Node.js 24 added as default version"*, Jira (https://jira.suse.com/browse/PED-15471)).
- Added note about post-quantum cryptography (PQC) default enablement in SSH to *Section 5.10.2, "Post-quantum cryptography (PQC) key exchange enabled by default"* (Jira (https://jira.suse.com/browse/PED-15713), Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1259825)).
- Added note about OpenSSH mlkem768x25519-sha256 hybrid key exchange support to *Section 5.10.3, "Support for mlkem768x25519-sha256 post-quantum key exchange in OpenSSH"* (Jira (https://jira.suse.com/browse/PED-16657), Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1275660)).
- Added iptables and nftables to SLES Minimal images (*Section 4.5, "Added iptables and nftables to SLES Minimal images"*, Jira (https://jira.suse.com/browse/PED-16001)).
- Added comprehensive lifecycle documentation for various components (*Section 2.6.2, "Specific component lifecycles"*, Jira (https://jira.suse.com/browse/DOCTEAM-2098)).

- Added note about gtk4-lang inclusion to *Section 5.4, "Desktop"* (Jira (https://jira.suse.com/browse/PED-14448)).
- Added `wire` package deprecation notice to *Section 10, "Removed and deprecated features and packages"* (Jira (https://jira.suse.com/browse/PED-15902)).
- Added release note for the removal of Plymouth from the s390x image (*Section 8.3.1, "Plymouth dropped from s390x image"*, Jira (https://jira.suse.com/browse/PED-11267))
- Added note about AMD SEV-SNP guest support to *Section 5.15.5.7, "AMD SEV-SNP guest support"* (Jira (https://jira.suse.com/browse/SLE-21027)).
- Restored the deprecation notice for NIS (*Section 10, "Removed and deprecated features and packages"*, Jira (https://jira.suse.com/browse/PED-3865), Jira (https://jira.suse.com/browse/SLE-24335)).

13.2 2026-07-09

13.2.1 New

- Upgraded Apache HTTP Server to 2.4.66 to fix HTTP/2 segfaults (*Section 5.8.9, "Apache HTTP Server upgraded to version 2.4.66"*, Jira (https://jira.suse.com/browse/PED-15955)).
- Chronological upgrade action checklist added to *Section 4.2.1, "Upgrade & Migration Quick Checklist"* (Jira (https://jira.suse.com/browse/DOCTEAM-2049)).
- Support for MS SQL Server 2025 legacy hashing algorithms in OpenSSL 3 added to *Section 5.10.9, "Support for MS SQL Server 2025 legacy hashing algorithms in OpenSSL 3"* (Jira (https://jira.suse.com/browse/PED-15721)).

13.3 2026-02-27

13.3.1 New

- *Section 5.15.5.9, "Kubevirt support"* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1219730))
- *Section 5.5.6, "Supported* `nodejs` *versions"* (Jira (https://jira.suse.com/browse/PED-11943))

- *Section 5.9.1, "`firewalld` version 1.3.4 added"* (Jira (https://jira.suse.com/browse/PED-13827))
- Added note about `python3-ovs` renaming to *Section 5.5, "Development"* (Jira (https://jira.suse.com/browse/PED-13323))
- *Section 5.10.4, "SSSD: support for running as unprivileged user"* (Jira (https://jira.suse.com/browse/PED-11986))
- *Section 5.10.5, "Microsoft Entra ID authentication"* (Jira (https://jira.suse.com/browse/PED-11278))
- Added note about PostgreSQL 14 to *Section 5.3, "Databases"* (Jira (https://jira.suse.com/browse/PED-13777))
- Added note about SLE 16.0 clients to *Section 4.2.7, "SMT has been replaced by RMT"*
- *Section 6.1.1, "Intel Clearwater Forest processor support"* (Jira (https://jira.suse.com/browse/PED-9144))

13.3.2 Changed

- Updated the maximum number of logical CPUs in *Section 5.7.6, "Kernel limits"* in the following way:
  - IBM Z (s390x): from 256 to 512
  - POWER (ppc64le): from 2048 to 8192
- Updated wording in *Section 5.5.4, "Python 3 packages staying in Basesystem"* (Jira (https://jira.suse.com/browse/PED-12762))

13.4 2025-10-31

13.4.1 New

- Added a note about MariaDB 11.8 to *Section 5.3, "Databases"* (Jira (https://jira.suse.com/browse/PED-13318))
- Added a note about dmesg warnings when using deprecated cgroup v1 features in *Section 5.8, "Miscellaneous"* (Jira (https://jira.suse.com/browse/PED-12406))
- *Section 5.12.2, "NFS over TLS support"* (Jira (https://jira.suse.com/browse/PED-13449))
- Added note about `KBD_DISABLE_CAPS_LOCK` removal in *Section 10.1, "Removed features and packages"* (Jira (https://jira.suse.com/browse/PED-12575))
- *Section 5.8.1, "Apache's Portable Runtime Library devel package renaming"* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1247839))

13.4.2 Changed

- Extend IBM Java support lifecycle in *Section 5.5.8, "Supported Java versions"* (Jira (https://jira.suse.com/browse/PED-13389))

13.5 2025-08-21

13.5.1 New

- *Section 5.5.2, "Support for Ansible interpreter"* (Jira (https://jira.suse.com/browse/PED-13352))

13.6 2025-07-11

13.6.1 Changed

- changed `ntp` from being removed to moved to *Legacy Module* in *Section 10.1, "Removed features and packages"*
- changed OpenLDAP server from being removed to being deprecated in *Section 10.2.1, "OpenLDAP server"* (Jira (https://jira.suse.com/browse/PED-13239))

13.7 2025-06-25

13.7.1 New

- *Section 5.8.2, "`hwloc` has been updated"* (Jira (https://jira.suse.com/browse/PED-11875))
- *Section 8.2.1, "`paes-xts-plain64` cipher now supported for disk encryption during installation"* (Jira (https://jira.suse.com/browse/PED-12579))
- *Section 5.10.6, "New 4096-bit signing key"* (Jira (https://jira.suse.com/browse/PED-8000))

13.8 2025-05-28

13.8.1 New

- *Section 5.8.3, "systemd default configurations moved to `/usr`"* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1237496))

13.9 2025-04-07

13.9.1 New

- *Section 5.2.1, "STIG-compliant container"* (Jira (https://jira.suse.com/browse/PED-4943))
- *Section 5.5.3, "Ruby 3 has been added"* (Jira (https://jira.suse.com/browse/PED-12434))
- Added `redis` removal notice in *Section 10.1, "Removed features and packages"* (Jira (https://jira.suse.com/browse/PED-11967))
- *Section 5.8.4, "FADump and kdump speed improvement"* (Jira (https://jira.suse.com/browse/PED-12263))
- *Section 5.7.1, "`smc` driver has been updated"* (Jira (https://jira.suse.com/browse/PED-12711))

13.10 2025-03-10

13.10.1 New

- *Section 5.8.5, "New systems-management module"* (Jira (https://jira.suse.com/browse/PED-11907))
- *Section 5.8.6, "Ansible is now available"* (Jira (https://jira.suse.com/browse/PED-11816))
- *Section 5.7.2, "cgroupv2 CPU load-balancing"* (Jira (https://jira.suse.com/browse/PED-11935))
- *Section 5.9.2, "Kea DHCP has been added"* (Jira (https://jira.suse.com/browse/PED-11692))

- *Section 5.7.3, "Externally supported flag change"* (Jira (https://jira.suse.com/browse/PED-8462))
- *Section 5.7.4, "Userspace live patching"* (Jira (https://jira.suse.com/browse/PED-12170))
- Added `netiucv` and `lcs` to *Section 10.3, "Deprecated features and packages"*
- Added `chrony` to the list of removed packages in *Section 10, "Removed and deprecated features and packages"*
- *Section 5.8.7, ""IDXD: user: probe of wq1.0 failed with error -95" errors"* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1234633))

13.11 2025-01-14

13.11.1 New

- *Section 5.8.8, "Support of BPF-related tools"* (Jira (https://jira.suse.com/browse/PED-8569))

13.12 2024-09-12

13.12.1 New

- Initial SP7 release

14 Kernel parameter changes



Warning

This list of changes may not be exhaustive.

14.1 Changes from SP6 to SP7

These Linux kernel parameters have been changed since SLES 15 SP6.