

SUSE Linux Enterprise Server 15 SP5

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 SP5 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-SP5>.

Publication Date: 2023-05-15, Version: 15.5.20230515

Contents

- 1 About the release notes 3
- 2 SUSE Linux Enterprise Server 3
- 3 Modules, extensions, and related products 10
- 4 Installation and upgrade 12
- 5 Changes affecting all architectures 17
- 6 POWER-specific changes (ppc64le) 36
- 7 IBM Z-specific changes (s390x) 39
- 8 Removed and deprecated features and packages 46
- 9 Obtaining source code 47
- 10 Legal notices 48

- A Changelog for 15 SP5 49
- B Kernel parameter changes 55

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/releasesnotes> .

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 SP5 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 SP5, 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-SP5/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 5.9.3, "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 4.2.4, "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 SP5 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 Manager provide additional options for disconnected or managed installations.

MAJOR UPDATES TO THE SOFTWARE SELECTION:

Salt

SLE 15 SP5 can be managed via Salt, making it integrate better with modern management solutions such as SUSE 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 SP5

SUSE Linux Enterprise Server 15 SP5 introduces changes compared to SUSE Linux Enterprise Server 15 SP4. The most important changes are listed below:

2.2.3 Package and module changes in 15 SP5

The full list of changed packages compared to 15 SP4 can be seen at this URL:

- https://documentation.suse.com/package-lists/sle/15-SP5/package-changes_SLE-15-SP4-GA_SLE-15-SP5-GA.txt ↗

The full list of changed modules compared to 15 SP4 can be seen at this URL:

- https://documentation.suse.com/package-lists/sle/15-SP5/module-changes_SLE-15-SP4-GA_SLE-15-SP5-GA.txt ↗

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 SP5 has been submitted to the certification bodies for:

- Common Criteria Certification, see <https://www.commoncriteriaportal.org/> ↗
- FIPS 140-2 validation, see <https://doi.org/10.6028/NIST.FIPS.140-2> ↗

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 SP5. This directory includes PDF versions of the SUSE Linux Enterprise Server 15 SP5 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 SP5, see <https://documentation.suse.com/sles/15-SP5> .

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.

SUSE Linux Enterprise Server 15 has a 13-year life cycle, with 10 years of General Support and three years of Extended Support. The current version (SP5) will be fully maintained and supported until six months after the release of SUSE Linux Enterprise Server 15 SP6.

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 receive a total of three to five years of support per Service Pack.

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

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 5.4, “Kernel”*
- *Section 5.7, “Storage and file systems”*
- *Section 5.10, “Virtualization”*
- *Section 8, “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:

- PostgreSQL (all versions, including all subpackages)

2.7.3 Software under GNU AGPL

SUSE Linux Enterprise Server 15 SP5 (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 SP5 (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.

3 Modules, extensions, and related products

This section comprises information about modules and extensions for SUSE Linux Enterprise Server 15 SP5. Modules and extensions add functionality to the system.



Note: Package and module changes in 15 SP5

For more information about all package and module changes since the last version, see [Section 2.2.3, “Package and module changes in 15 SP5”](#).

3.1 Modules in the SLE 15 SP5 product line

The SLE 15 SP5 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 SP5 at the release of SUSE Linux Enterprise Server 15 SP5 are listed in the *Modules and Extensions Quick Start* at <https://documentation.suse.com/sles/15-SP5/html/SLES-all/article-modules.html>.

Not all SLE modules are available with a subscription for SUSE Linux Enterprise Server 15 SP5 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/releasesnotes>.

The following extensions are available for SUSE Linux Enterprise Server 15 SP5:

- SUSE Linux Enterprise Live Patching: <https://www.suse.com/products/live-patching>
- SUSE Linux Enterprise High Availability Extension: <https://www.suse.com/products/high-availability>
- 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 5.8, “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/releasesnotes>.

- 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 for High-Performance Computing: <https://www.suse.com/products/server/hpc> ↗
- SUSE Linux Enterprise Real Time: <https://www.suse.com/products/realtime> ↗
- SUSE Manager: <https://www.suse.com/products/suse-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 SP5.



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-SP5/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.

4.1.2 Storage requirements for Btrfs installation on PowerPC

There is a known issue with using guided partitioning to install SUSE Linux Enterprise Server on PowerPC architecture. The root filesystem needs more storage than the listed minimum. It is recommended to allocate at least 20 gigabytes.

4.1.3 Installation via SSH on s390x

Before starting the installation using `yast.ssh`, it is necessary to set the environmental variable `QT_XCB_GL_INTEGRATION` to `xcb_egl`:

```
export QT_XCB_GL_INTEGRATION=xcb_egl
```

4.2 Upgrade-related notes

This section includes upgrade-related information for SUSE Linux Enterprise Server 15 SP5.



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-SP5/html/SLES-all/cha-upgrade-online.html>.

4.2.1 Hibernation requires manual intervention

Previously, it was possible for data loss to occur due to the system not hibernating correctly.

In 15 SP5, a sanity check was introduced to prevent this. It works by removing the kernel `resume` parameter if it points to a non-existent device. However, that means a system would not use the hibernation data. To fix it, do the following:

1. Edit `/etc/default/grub` and correct the `resume` parameter to point to an existing device.
2. Regenerate `initrd`.
3. Reboot.

4.2.2 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.

4.2.3 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 SP4 before upgrading to SLE 15 SP5.

4.2.4 SMT has been replaced by RMT

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, also see the new RMT Guide at <https://documentation.suse.com/sles/15-SP3/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`, `.vhd`, 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`](#)

4.4.1 Alternative Python 3 development interpreter moved to a separate module

SLE 15 SP4 introduces a new *Python 3* Module, which includes the alternatively available development Python interpreter, formerly included in the *Basesystem* Module. This new module will allow for more flexibility for the lifecycle of the packages provided within it and a clean separation between the system and development interpreter.

As the `python39` package was part of the *Basesystem* Module on SLE 15 SP3, the introduction of this new module will require some changes when migrating to SLE 15 SP5. If you are using `python39` and migrate from SLE 15 SP3, you will have to add the *Python 3* module after migration via SUSEConnect to receive updates for this alternative interpreter. Otherwise the package will remain orphaned and without security updates.

Packages inside this module can have differing support level and support lifecycle. For more information, see documentation.

4.5 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 SP5.

5.1 Containers

5.1.1 Podman upgrade from 3.4.x to 4.3.1

Podman 4.x is a major release with 60 new features and more than 50 bug fixes compared to Podman 3. It also includes a complete rewrite of the network stack.

Podman 4.x brings a new container network stack based on [Netavark](https://github.com/containers/netavark) (<https://github.com/containers/netavark>), the new container network stack and [Aardvark DNS server](https://github.com/containers/aardvark-dns) (<https://github.com/containers/aardvark-dns>) in addition to the existing container network interface (CNI) stack used by Podman 3.x. The new stack brings 3 important improvements:

- Better support for containers in multiple networks
- Better IPv6 support
- Better performance

To ensure that nothing breaks with this major change, the old CNI stack will remain the default on existing installations, while new installs will use Netavark.

New installations can opt to use CNI by explicitly specifying it via the `containers.conf` configuration file, using the `network_backend` field.

If you have run Podman 3.x before upgrading to Podman 4, Podman will continue to use CNI plugins as it had before. There is a marker in Podman's local storage that indicates this. In order to begin using Podman 4, you need to destroy that marker with `podman system reset`. This will destroy the marker, all of the images, all of the networks, and all of the containers.



Warning

Before testing Podman 4 and the new network stack, you will have to destroy all your current containers, images, and networks. You must export/save any import containers or images on a private registry, or make sure that your Dockerfiles are available for rebuilding and scripts/playbooks/states to reapply any settings, regenerate secrets, etc.

Last but not least CNI will be deprecated from upstream at a future date: <https://github.com/containers/podman/tree/main/cni>

For a complete overview of the changes, please check out the upstream 4.0.0 (<https://github.com/containers/podman/releases/tag/v4.0.0>) but also 4.1.1 (<https://github.com/containers/podman/releases/tag/v4.1.1>), 4.2.0 (<https://github.com/containers/podman/releases/tag/v4.2.0>) and 4.3.0 (<https://github.com/containers/podman/releases/tag/v4.3.0>) to be informed about all the new features and changes.

5.1.2 [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.

5.2 Desktop

5.2.1 nouveau disabled for Nvidia Turing and Ampere GPUs / openGPU recommendation

The `nouveau` driver is still considered experimental for Nvidia Turing and Ampere GPUs. Therefore it has been disabled by default on systems with these GPUs.

Instead of using the `nouveau` driver we recommend using Nvidia's new openGPU driver. Install this driver by installing these following packages:

- `nvidia-open-driver-G06-signed-kmp-default`
- `kernel-firmware-nvidia-gsp-G06`

Then uncomment the `options nvidia` line in the `/etc/modprobe.d/50-nvidia-default.conf` file so that it looks like the following afterwards:

```
### Enable support on *all* Turing/Ampere GPUs: Alpha Quality!  
options nvidia NVreg_OpenRmEnableUnsupportedGpus=1
```

If you prefer using `nouveau` driver anyway, add `nouveau.force_probe=1` to your kernel boot parameters, and do not install the above openGPU package.

5.3 Development

5.3.1 Python 3.10 modules, Reduced Python Stack

- Add Python 3.10 interpreter and modules
 - We have added an additional long-term supported Python 3.10 interpreter and modules needed to be able to get python modules from PyPI (`python-setuptools`, `python-pip`, `python-virtenv`) via the *Python 3* Module. It will be regularly updated to the latest patch version.
- Add Python Reduced Stack

- A reduced subset of what we provide today in SLES 15 SP5 has been added as modules.
- Keep Python 3.6
 - The current Python 3.6 interpreter and packages stay intact.
 - Renaming of Python packages would be done only to avoid source name conflicts.
- Life-cycle & support
 - Python Reduced Stack will be supported until 2026, which is the upstream end-of-life date for Python 3.10. The interpreter will be updated regularly to the latest patch version but modules will stay stable as much as possible.
 - We will continue delivering new interpreters (along with the respective `setup-tools` / `wheel` / `pip`) with each new service pack. These are short-term supported for each Service Pack.

5.3.2 Alternative Python 3 development interpreter moved to a separate module

SLE 15 SP4 introduces a new *Python 3* Module, which includes the alternatively available development Python interpreter, formerly included in the *Basesystem* Module. This new module will allow for more flexibility for the lifecycle of the packages provided within it and a clean separation between the system and development interpreter.

As the `python39` package was part of the *Basesystem* Module on SLE 15 SP3, the introduction of this new module will require some changes when migrating to SLE 15 SP5. If you are using `python39` and migrate from SLE 15 SP3, you will have to add the *Python 3* module after migration via SUSEConnect to receive updates for this alternative interpreter. Otherwise the package will remain orphaned and without security updates.

Packages inside this module can have differing support level and support lifecycle. For more information, see documentation.

5.3.3 Supported Java versions

The following Java implementations are available in SUSE Linux Enterprise Server 15 SP5:

Name (Package Name)	Version	Module	Support
OpenJDK (java-11-openjdk)	11	Base System	SUSE, L3, until 2026-12-31
OpenJDK (java-17-openjdk)	17	Base System	SUSE, L3, until 2028-06-30
OpenJDK (java-1_8_0-openjdk)	1.8.0	Legacy	SUSE, L3, until 2026-12-31
IBM Java (java-1_8_0-ibm)	1.8.0	Legacy	External, until 2025-04-30

5.4 Kernel

5.4.1 Kernel limits

This table summarizes the various limits which exist in our recent kernels and utilities (if related) for SUSE Linux Enterprise Server 15 SP5.

SLES 15 SP5 (Linux 5.14.21)	AMD64/Intel 64 (x86_64)	IBM Z (s390x)	POWER (ppc64le)	ARMv8 (AArch64)
CPU bits	64	64	64	64
Maximum number of logical CPUs	8192	256	2048	768
Maximum amount of RAM (theoretical/certified)	> 1 PiB/ 64 TiB	10 TiB/ 256 GiB	1 PiB/64 TiB	256 TiB/n.a.
Maximum amount of user space/kernel space	128 TiB/ 128 TiB	n.a.	512 TiB ¹ / 2 EiB	256 TiB/ 256 TiB

SLES 15 SP5 (Linux 5.14.21)	AMD64/Intel 64 (x86_64)	IBM Z (s390x)	POWER (ppc64le)	ARMv8 (AArch64)
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 mmmaps up to 512 TiB.

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

5.4.2 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 SP5, 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.

5.5 Miscellaneous

5.5.1 cpuid has been added

The `cpuid` package has been added. It provides detailed information about the CPU. For more information see <http://etallen.com/cpuid.html>.

5.6 Security

5.6.1 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.

5.6.2 Replacement of `gpg` as recommended tool for file encryption

A new `rage-encryption` package has been added. The package provides the `rage` executable. `rage` is an implementation of the `age` file encryption format using Rust.

This replaces `gpg` as the preferred tool over `gpg` for file encryption. The main reasons are that `gpg` has a history of security issues, and is well known for its complexity. In comparison, `rage` focuses on usability and security. It especially tries to make key handling as simple as handling SSH keys (essentially short lines of text), which it also supports.

For more information, see:

- <https://github.com/str4d/rage> ↗
- <https://age-encryption.org/v1> ↗

5.7 Storage and file systems

5.7.1 dracut default persistent policy change

The previously used `by-path` policy had the following shortcomings:

- doesn't work for multi-path
- very fragile for iSCSI
- can change with hardware changes

To avoid the above problems, the persistent policy of `dracut` is now set to `by-uuid`.

5.7.2 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
Supported in product	SLE	SLE	SLE	SLE HA
Data/metadata journaling	N/A ²	– / +	+ / +	– / +
Journal internal/external	N/A ²	+ / +	+ / +	+ / –
Journal checksumming	N/A ²	+	+	+
Subvolumes	+	–	–	–
Offline extend/shrink	+ / +	– / –	+ / +	+ / – ³
Inode allocation map	B-tree	B+ -tree	Table	B-tree
Sparse files	+	+	+	+
Tail packing	–	–	–	–
Small files stored inline	+ (in metadata)	–	+ (in inode)	+ (in inode)
Defragmentation	+	+	+	–
Extended file attributes/ACLs	+ / +	+ / +	+ / +	+ / +

Feature	Btrfs	XFS	Ext4	OCFS 2 ¹
User/group quotas	– / –	+ / +	+ / +	+ / +
Project quotas	–	+	+	–
Subvolume quotas	+	N/A	N/A	N/A
Data dump/restore	–	+	–	–
Block size default	4 KiB ⁴			
Maximum file system size	16 EiB	8 EiB	1 EiB	4 PiB
Maximum file size	16 EiB	8 EiB	1 EiB	4 PiB

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

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`.

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 SP5 but are not supported by SUSE. By default, the file system drivers in SUSE Linux Enterprise Server 15 SP5 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.

5.7.3 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/subvol- umes	+	+	+	+	+	+
Swap files	–	–	–	+	+	+
Metadata integrity	+	+	+	+	+	+
Data integrity	+	+	+	+	+	+
Online metadata scrubbing	+	+	+	+	+	+

Feature	SLES 11 SP4	SLES 12 SP5	SLES 15 GA	SLES 15 SP1	SLES 15 SP2	SLES 15 SP3
Automatic defragmentation	–	–	–	–	–	–
Manual defragmentation	+	+	+	+	+	+
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	–	–	–	–	–	–

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

5.8 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.

5.8.1 Important package additions to SUSE Package Hub

Among others, the following packages have been added to SUSE Package Hub:

5.9 System management

5.9.1 Silence KillMode=None messages

The log level of the deprecation warnings regarding `killmode=None` have been reduced. Instead of `warning`, they are now logged at the `debug` log level.

5.9.2 `yast2-iscsi-client` drops `open-iscsi` and `iscsiuio` as dependencies

The `yast2-iscsi-client` package no longer automatically installs `open-iscsi` and `iscsiuio`. The two packages need to be installed manually before using `yast2-iscsi-client`.

5.9.3 Searching packages across all SLE modules

In SLE 15 SP5 you can search for packages both within and outside of currently enabled SLE modules using the following command:

```
zypper search-packages -d 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.

5.10 Virtualization

For more information about acronyms used below, see <https://documentation.suse.com/sles/15-SP5/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-SP5/html/SLES-all/cha-virt-support.html>.

5.10.1 KVM

We increase the support from 288 up 768 VCPU per virtual Machine.

5.10.2 Xen

Xen has been updated to version 4.17:

- The x86 MCE command line option info is now updated.
- __ro_after_init support, for marking data as immutable after boot.
- The project has officially adopted 4 directives and 24 rules of MISRA-C, added MISRA-C checker build integration, and defined how to document deviations.
- IOMMU superpage support on x86, affecting PV guests as well as HVM/PVH ones when they don't share page tables with the CPU (HAP/EPT/NPT).
- Support for VIRT_SSBD and MSR_SPEC_CTRL for HVM guests on AMD.
- Improved TSC, CPU, and APIC clock frequency calibration on x86.
- Support for Xen using x86 Control Flow Enforcement technology for its own protection. Both Shadow Stacks (ROP protection) and Indirect Branch Tracking (COP/JOP protection).
- Add mwait-idle support for SPR and ADL on x86.
- Extend security support for hosts to 12 TiB of memory on x86.
- Add command line option to set cpuid parameters for dom0 at boot time on x86.
- It is possible to use PV drivers with dom0less guests, allowing statically booted dom0less guests with PV devices.
- Add Xue - console over USB 3 Debug Capability.
- dropped support for the (x86-only) vesa-mtrr and vesa-remap command line options
- launch_security: Use SEV-ES policy = 0x07 if host supports it

5.10.3 QEMU

QEMU has been updated to version 7.1:

- Raise the maximum number of vCPUs a VM can have to 1024 (only 768 is supported)
- Improve dependency handling (for example, what is recommended compared to what is required)
- Add the `qemu-headless` subpackage that brings in all the packages that are needed for creating VMs with tools like `virt-install` or `VirtManager`; it can be run either locally or from a remote host
- The old `qemu-binfmt` wrappers around the various `qemu-$ARCH` Linux user emulation binaries are not necessary any longer
- Enable `aio=io_uring`` on all KVM architectures

For more information see the following:

- <https://wiki.qemu.org/ChangeLog/7.1> ↗
- <https://wiki.qemu.org/ChangeLog/7.0> ↗
- <https://qemu-project.gitlab.io/qemu/about/removed-features.html> ↗
- <https://qemu-project.gitlab.io/qemu/about/deprecated.html> ↗



Note: Deprecation notice

In previous versions, if no explicit image format was provided, some QEMU tools tried to guess the format of the image, and then process it accordingly. Because this feature is a potential source of security issues, it has been deprecated and removed. It is now necessary to explicitly specify the image format. For more information, see <https://qemu-project.gitlab.io/qemu/about/removed-features.html#qemu-img-backing-file-without-format-removed-in-6-1> ↗.

5.10.4 libvirt

libvirt has been updated to version 9.0.0:

- New virt-qemu-sev-validate utility for validating the measurement reported for a domain launched with AMD SEV
- New subpackage libvirt-client-qemu providing client utilities to interact with QEMU-specific features of libvirt
- Migration to /usr/etc: saving user changed configuration files in /etc and restoring them while an RPM update

For more information see the following:

- <https://libvirt.org/news.html#v9-0-0-2023-01-16> ↗
- <https://libvirt.org/news.html#v8-10-0-2022-12-01> ↗
- <https://libvirt.org/news.html#v8-9-0-2022-11-01> ↗
- <https://libvirt.org/news.html#v8-8-0-2022-10-03> ↗
- <https://libvirt.org/news.html#v8-7-0-2022-09-01> ↗

5.10.5 VMware

5.10.5.1 open-vm-tools

open-vm-tools has been updated to version 12.1.5:

- Migration of PAM settings to /usr/lib/pam.d
- Remove `libgrpc++`, `libgrpc`, and `libprotobuf` from `containerinfo` Requires section. The dependencies will be added automatically.
- Add containerInfo plugin
- Add dependencies on `grpc`, `protobuf`, and `containerd` for container introspection
- A number of Coverity reported issues have been addressed.

- The `deployPkg` plugin may prematurely reboot the guest VM before cloud-init has completed user data setup. If both the Perl based Linux customization script and cloud-init run when the guest VM boots, the `deployPkg` plugin may reboot the guest before cloud-init has finished. The `deployPkg` plugin has been updated to wait for a running cloud-init process to finish before the guest VM reboot is initiated.
- A `SIGSEGV` may be encountered when a non-quiescing snapshot times out
- Unwanted `vmtoolsd` service error message if not on a VMware hypervisor When `open-vm-tools` comes preinstalled in a base Linux release, the `vmtoolsd` services are started automatically at system start and desktop login. If running on physical hardware or in a non-VMware hypervisor, the services will emit an error message to the systemd's logging service before stopping.

5.10.6 Others

5.10.6.1 NVIDIA GRID

Support for NVIDIA Virtual GPU (vGPU) v15.1 has been added. The support does NOT include NVIDIA vGPU live migration support.

5.10.6.2 virt-manager

`virt-manager` has been updated to version 4.1.0:

- Specifying `--boot` no longer implies `no_install=yes`
- add UI and cli support for `qemu-vdagent` channel
- cli: More `--iothreads` suboptions
- cli: Add support for URL query with disks

5.10.6.3 `sanlock`

`sanlock` has been updated to version 3.8.5:

- Add support for Python 3
- Add support for 4k sector size
- Support `SANLOCK_RUN_DIR` and `SANLOCK_PRIVILEGED` environment variables

5.10.6.4 `Perl-Sys-Virt`

Update to 0.9.0: * Add all new APIs and constants in libvirt 9.0.0

5.10.6.5 `numactl`

`numactl` has been updated to version 2.0.15.0.g01a39cb:

- Update to support multiple nodes
- numademo: Add a new test for multiple-preferred-nodes policy
- numactl: Simplify preferred selection

5.10.6.6 `libguestfs`

`libguestfs` has been updated to version 1.48.4:

- Drop reiserfs
- Multiple fixes to the OCaml bindings
- Inspection of guests which use LUKS encryption on top of LVM logical volumes should now work `guestfs_remove_drive` has been deprecated and now returns an error.
- `guestfs_add_drive` no longer supports hotplugging
- In `guestfs_xfs_admin` the `lazycounter` parameter is deprecated because it is no longer supported in recent versions of XFS.
- The User-mode Linux ("uml") backend has been removed.

- This release has moved many virt tools like virt-builder, virt-cat, virt-customize, virt-df, etc. to the guestfs-tools project. This makes libguestfs a bit easier to build and manage.
- We now use the `qemu/libvirt` feature `-cpu max` to select the best CPU to run the appliance.
- The `qemu -enable-fips` option is no longer used. It was not needed and has been deprecated by `qemu`.
- Using the equivalent SeaBIOS feature instead of `qemu's Serial Graphics Adapter option ROM
- Renamed packages:
 - `guestfs-winsupport` → `libguestfs-winsupport`
 - `guestfsd` → `libguestfsd`
- New packages:
 - `libguestfs`, `libguestfs-typelib-Guestfs`,
 - `libguestfs-gobject`, `libguestfs-gobject-devel`
 - `libguestfs-rescue`, `libguestfs-rsync`, `libguestfs-xfs`
- Dropped packages:
 - `libguestfs-test`

5.10.6.7 virt-v2v

Update to version 2.0.7:

- Virt-v2v has been modularised allowing external programs to examine the state of the conversion and inject their own copying step. Further enhancements will be made to this new architecture in forthcoming releases.
- The command line is almost identical apart from some debugging features that were removed (see below). The only significant difference is that the output format (-of) now has to be specified if it is different from the input format, whereas previous versions of virt-v2v would use the same output format as input format automatically.

- A lot of time was spent improving the performance of virt-v2v in common cases.
- Many bug fixes and performance enhancements were made to oVirt imageio output (Nir Soffer).
- There is a new virt-v2v-in-place(1) tool which replaces the existing virt-v2v --in-place option.
- Virt-v2v can now convert guests which use LUKS encrypted logical volumes.
- Option -oo rhv-direct has been replaced by -oo rhv-proxy, and direct mode (which is much faster) is now the default when writing to oVirt, with proxy mode available for restricted network configurations.
- The following command line options were removed: -print-estimate, --debug-overlays, --no-copy.
- Virt-v2v no longer installs the RHEV-APT tool in Windows guests. This tool was deprecated and then removed in oVirt 4.3.
- Deprecated tool virt-v2v-copy-to-local has been removed.

5.10.6.8 `sevctl`

The `sevctl` package version 0.3.2 has been added. It replaces the deprecated `sev-tool` package.

6 POWER-specific changes (ppc64le)

Information in this section applies to SUSE Linux Enterprise Server for POWER 15 SP5.

Also see the following notes elsewhere:

- [Section 4.1.2, "Storage requirements for Btrfs installation on PowerPC"](#)

6.1 Security

There were also the following changes:

- POWER10 performance enhancements for cryptography: NSS FreeBL

6.1.1 POWER10 performance enhancements for cryptography: nettle

There were the following improvements:

- Use defined structure constants of P1305 in [asm.m4](#)
- Implement Poly1305 single block update based on radix 2^{64}
- Workaround for qemu bug affecting the ppc instruction vmsumudm

6.1.2 POWER10 performance enhancements for cryptography: libgcrypt

There were the following improvements:

- Chacha20/poly1305 - Optimized chacha20/poly1305 for P10 operation
- AES-GCM: Bulk implementation of AES-GCM acceleration for ppc64le
- hwf-ppc: fix missing HWF_PPC_ARCH_3_10 in HW feature

6.1.3 POWER10 performance enhancements for cryptography: OpenSSL

There were the following improvements:

- AES-GCM
 - AES-GCM performance optimization with stitched method for p9+ ppc64le
- Chacha20

- chacha20 performance optimizations for ppc64le with 8x lanes, Performance increase around 50%

6.2 Storage

6.2.1 NVMe-oF on LVM with multiple NVMe disks

The installation of NVMe Over Fabrics (NVMe-oF) does not work with Logical Volume Management when the root Volume Group utilizes a storage pool consisting of multiple NVMe-oF disks, which necessitates discovery beyond the boot disk.

6.3 Virtualization

There were also the following changes:

- Added NVMf-FC kdump support

6.3.1 Support for the new H_WATCHDOG hypercall included with P10 firmware

Added a `pseries-wdt` driver that exposes these hypercall-based watchdog timers to userspace via the Linux watchdog API.

6.3.2 `ibmveth` driver performance improvement

Changed the `ibmveth` driver to implement a more efficient way of giving packets to the hypervisor for transmit. Instead of DMA mapping and unmapping every outgoing data buffer, the buffer is copied into a reusable DMA mapped buffer. Also implemented multiple transmit queues for parallel packet processing.

6.3.3 Adding changes in `ibmvnic` driver to assign IRQ affinity to all

CPU's after hotplug events (CPU or vnic device): `irqbalance` daemon provides `--banmod` option so that IRQ affinities will be preserved with driver settings. But the `irqbalance --banmod` option is not working with vnic IRQs and this feature fixes the bug in the `irqbalance` daemon code.

7 IBM Z-specific changes (s390x)

Information in this section applies to SUSE Linux Enterprise Server for IBM Z and LinuxONE 15 SP5. For more information, see <https://www.ibm.com/docs/en/linux-on-systems?topic=distributions-suse-linux-enterprise-server> ↗

7.1 Hardware

There were the following hardware-related changes:

- Support for IBM z16 and LinuxONE 4 in `qclib`
- Exploitation support of new IBM Z crypto hardware in `zcrypt` DD
- Support for a new set of crypto performance counters of the IBM z16 and LinuxONE 4
- Add new CPU-MF Counters for IBM z16 and LinuxONE 4 in kernel, `s390-tools` and `libpfm` part.
- Support for "Crypto Compliance" feature of the IBM z16 and LinuxONE 4 Processor-Activity-Instrumentation Facility in kernel and `s390-tools`

7.2 Networking

7.2.1 Enablement for MIO Instructions - kernel and `rdma-core` parts

Make use of the new PCI Load/Store instructions in the `rdma-core` package for increased performance.

7.3 Performance

7.3.1 zlib CRC32 optimization for s390x

This new feature utilizes SIMD instructions to accelerate the zlib CRC32 implementation, resulting in significant performance improvements for applications that rely heavily on zlib.

7.4 Security

7.4.1 Secure Execution

If you want to use IBM Secure Execution see <https://www.ibm.com/docs/en/linux-on-systems?topic=execution-prerequisites-restrictions> ↗

7.4.2 openCryptoki: p11sak support Dilithium and Kyber keys

The openCryptoki p11sak tool has been extended to manage Dilithium and Kyber keys.

7.4.3 In-kernel crypto: SIMD implementation of chacha20

Recent kernel releases provide support for the chacha20 cipher and the goal of this feature is to use z System SIMD instruction to accelerate the chacha20 implementation on IBM Z and LinuxONE.

7.4.4 openCryptoki ep11 token: master key consistency

Ensuring that all APQNs used by an openCryptoki ep11 token are configured with the same master key, if not print an error message and fail initialization.

7.4.5 zcrypt DD: Exploitation Support of new IBM Z Crypto Hardware for kernel and s390-tools

zcrypt DD: exploitation support of new IBM Z crypto hardware by recognizing and supporting the CEX8 adapters.

7.4.6 Display PAI (Processor Activity Instrumentation) CPACF counters (s390-tools)

Provides a tool to display CPACF usage counters from the IBM z16 and LinuxONE 4 Processor Activity Instrumentation Facility.

7.4.7 openCryptoki EP11 token: IBM z16 and LinuxONE 4 support

The openCryptoki EP11 token supports new vendor specific mechanisms for quantum safe ciphers (Dilithium and Kyber) supported by the CEX8S crypto adapter.

7.4.8 openCryptoki EP11 token: vendor-specific key derivation

Support of a new function from EP11 7.2 by the openCryptoki EP11 token. Comprises the support of vendor-specific mechanisms for a key derivation function used with cryptocurrencies and Schnorr signatures.

7.4.9 openCryptoki: support crypto profiles

Support for a new configuration option to restrict cryptographic functions/mechanisms.

7.4.10 openCryptoki key generation with expected MKVP only on CCA and EP11 tokens

For the EP11 and CCA tokens allow to configure expected master key verification pattern (MKVPs) configured in the crypto adapter(s) and upon generation of a new secure keys ensures that the MKVP of the generated key is equal to an expected MKVP.

7.4.11 libica: extend statistics to reflect security measures (crypto)

Adds new `-k` parameter to `icastats` to display detailed counters to reflect security measures (key size/curve/hash size).

7.4.12 libica: eliminate SW fallbacks - stage 2

Eliminates implementations of SW fallback functions for RSA in `libica`.

7.4.13 `zcryptctl` support for control domains - kernel and s390-tools parts

Improves access control to crypto resources via device nodes, for example, for Docker containers by allowing to assign control domains to a device node created by `zcryptctl`.

7.4.14 `openCryptoki`: PKCS #11 3.1 - support `CKA_DERIVE_TEMPLATE`

In `openCryptoki`, support the new attribute `CKA_DERIVE_TEMPLATE` introduced with PKCS #11 v3.1.

7.4.15 `p11-kit`: add IBM specific mechanisms and attributes

Adds support for IBM-specific attributes and mechanisms to the PKCS11 client-server implementation of `p11-kit`.

7.4.16 `libica`: FIPS 140-3 compliance

Update of `libica` to fulfill FIPS 140-3 requirements.

7.5 Storage

7.5.1 Transparent DASD PPRC (Peer-to-Peer Remote Copy) handling

Enables user of Linux on Z to use DASD volumes in a PPRC (Peer-to-Peer Remote Copy) relation like a normal DASD volume thereby enabling platform support along with improving user experience.

7.5.2 `zdev`: Site-aware device configuration

Enables a Linux on Z admin to prepare a Linux root/boot volume so that it can be started on a different system (site) or with different device IDs and parameters without manually changing the configuration.

7.5.3 `zipl` support for Secure Boot IPL and Dump from ECKD DASD

Enables `zipl` to use an ECKD DASD for Secure Boot IPL and Dump.

7.5.4 `zipl`: Site-aware environment block

Enables a Linux on Z admin to create a `zipl` configuration file that enables different kernel parameters depending on the IPL site.

7.5.5 Transparent PCI device recovery

Improves reliability and reduces downtime by using cooperative recovery strategies that allow the drivers to recover from error scenarios automatically (without intervention from userspace), and without going through a complete tear-down and subsequent re-init.

7.5.6 ROCE: Independent Usage of Secondary Physical Function

This feature enables zLinux running in an LPAR to use the Physical Function (PF) that corresponds to the second opрт of a ConnectX-5/6 card even if the PF that corresponds to the first port is assigned to a different LPAR.

7.6 Virtualization

The following new features are supported in SUSE Linux Enterprise Server 15 SP5 under KVM:

7.6.1 KVM: Enable GISA support for Secure Execution guests

GISA (Guest Interruption State Area) is now supported for Secure Execution Guests. This allows the direct injection of interrupts into running VMs, which results in reduced processing overhead.

7.6.2 Enhanced Interpretation for PCI Functions

For improving performance, the interpretive execution of the PCI store and PCI load instructions are enabled. Further improvement is achieved by enabling the Adapter-Event-Notification Interpretation which enables customers to run PCI I/O intensive workloads in KVM guests. This feature also allows KVM guests to use the Shared Memory Communications - Direct (SMC-D) protocol.

7.6.3 vfio-ap enhancements

This feature adds hotplug support, which allows to dynamically assign and remove crypto adapters to or from a running KVM guest. This additionally provides a tool to persistently define the configuration of crypto adapters and domains that are allowed for passthrough usage as well as the configuration of the matrix/vfio-ap devices to be passed through to avoid that customers have to reconfigure after every IPL.

7.6.4 Secure Execution guest dump encryption with customer keys, tool to process encrypted Secure Execution guest dumps

These features implements dumps created in a way that can only be decrypted by the owner of the guest image and be used for problem determination hence mitigating the outcomes of situations where kdump hypervisor-initiated dumps are not helpful.

7.6.5 KVM: Attestation support for Secure Execution (crypto), KVM: Secure Execution Attestation Userspace Tool

Provides attestation support, for example, for external frameworks, specific deployment models or potentially regulatory requirements.

7.6.6 KVM: Provide virtual CPU topology to guests

This feature allows to specify a virtual CPU topology which can help to configure the guest for better performance.

7.6.7 KVM: Allow long kernel command lines for Secure Execution guests and QEMU

This feature allows Secure Execution guests to use larger command lines.

7.6.8 Allow to list persisted `driverctl` definitions

Updated `driverctl` to version newer than 0.111 because the previous version did not allow to list persisted override definitions.

7.6.9 KVM: Enablement of device busid for subchannels

Displaying the original CCW device numbers for `vfio-ap`` devices improves the usability of `vfio-ccw` device passthrough to KVM guests.

7.7 Kernel

7.7.1 NVMe stand-alone dump support

Supports the HW roadmap, full exploitation of NVMe on the IBM Z platform.

7.7.2 Support IBM z16 and LinuxONE 4 Processor-Activity-Instrumentation Facility

Support for the Crypto Compliance feature of the IBM z16 and LinuxONE 4 Processor-Activity-Instrumentation Facility.

7.7.3 New CPU-MF Counters for IBM z16 and LinuxONE 4

Added new CPU-MF Counters for IBM z16 and LinuxONE 4.

7.7.4 Support Processor Activity Instrumentation Extension 1

Support for a new set of crypto performance counters of the IBM z16 and LinuxONE 4.

7.7.5 Add additional information to SCLP CPI

Includes distribution, release number, and detailed kernel version in CPI data to be displayed on the HMC.

7.8 Miscellaneous

7.8.1 Auto scale crashkernel size with hardware changes

`kdump` now has a configuration option called `KDUMP_AUTO_RESIZE`. This option makes the boot-time init script call `kdumptool-calibrate --shrink`. This performs the same reservation size estimate that `kdumptool calibrate` normally does and shrinks the memory reservation to the calculated value by writing to `/sys/kernel/kexec_crash_size`.

YaST now has an option to turn this run-time auto-detection on. The result will be a very large `crashkernel=` value (around half the RAM) passed to the kernel and the reservation is reduced during boot using the `KDUMP_AUTO_RESIZE` option.

7.8.2 Enabled installer to configure PCI-attached networking devices

The installer now supports PCI-attached networking devices.

7.8.3 Removed ESCON from installer

Removed the ESCON entry from the menu because it is no longer supported by the YaST module for network configuration.

8 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 SP5

For more information about all package and module changes since the last version, see [Section 2.2.3, “Package and module changes in 15 SP5”](#).

8.1 Removed features and packages

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

- The `samba-ad-dc-libs` package has been removed. It was previously available as technical preview.
- Setting up Kerberos with LDAP backend via YaST has been removed.
- The `thunderbolt-user-space` package has been removed.
- `zypper-docker` has been removed.
- `xpram` device driver has been removed.

8.2 Deprecated features and packages

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

- `sev-tool` has been deprecated. Use `sevctl` instead.
- `gnote` has been deprecated. Use `bijiben` instead.
- We have switched from `openmpi2` to `openmpi4` as the default `openmpi` implementation. This is because `openmpi2` and `openmpi3` have been EOL for some time now. They will be removed in SLES 15 SP6.

9 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.


10 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 © 2010-2023 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.

A Changelog for 15 SP5








A.1 2023-05-15



A.1.1 New

- *Section 7.4.1, "Secure Execution"* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1211316) )

A.2 2023-05-11









A.2.1 New

- Added note about xpram removal in *Section 8, "Removed and deprecated features and packages"* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1205381) )
- *Section 6.3.3, "Adding changes in ibmvnic driver to assign IRQ affinity to all"* (Jira (<https://jira.suse.com/browse/PED-2319>) )
- *Section 6.3.2, "ibmveth driver performance improvement"* (Jira (<https://jira.suse.com/browse/PED-2638>) )
- Added note about NVMf-FC kdump in *Section 6.3, "Virtualization"* (Jira (<https://jira.suse.com/browse/PED-1256>) )
- *Section 6.3.1, "Support for the new H_WATCHDOG hypercall included with P10 firmware"* (Jira (<https://jira.suse.com/browse/PED-530>) )
- *Section 6.1.3, "POWER10 performance enhancements for cryptography: OpenSSL"* (Jira (<https://jira.suse.com/browse/PED-512>) )
- Added a note about cryptography enhancements in NSS FreeBL in *Section 6.1, "Security"* (Jira (<https://jira.suse.com/browse/PED-495>) )

- *Section 6.1.2, “POWER10 performance enhancements for cryptography: libgcrypt”* (Jira (<https://jira.suse.com/browse/PED-520>) )
- *Section 6.1.1, “POWER10 performance enhancements for cryptography: nettle”* (Jira (<https://jira.suse.com/browse/PED-505>) )

A.3 2023-05-10

















A.3.1 New

- *Section 5.5.1, “cpuid has been added”* (Jira (<https://jira.suse.com/browse/PED-2653>) )
- *Section 5.7.1, “dracut default persistent policy change”* (Jira (<https://jira.suse.com/browse/PED-1884>) )
- *Section 7.4.2, “openCryptoki: p11sak support Dilithium and Kyber keys”* (Jira (<https://jira.suse.com/browse/PED-2867>) )
- *Section 7.6.1, “KVM: Enable GISA support for Secure Execution guests”* (Jira (<https://jira.suse.com/browse/PED-461>) )
- *Section 4.1.2, “Storage requirements for Btrfs installation on PowerPC”* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1209365) )
- *Section 6.2.1, “NVMe-oF on LVM with multiple NVMe disks”* (Jira (<https://jira.suse.com/browse/DOCTEAM-978>) )
- *Section 5.2.1, “nouveau disabled for Nvidia Turing and Ampere GPUs / openGPU recommendation”* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1210197) )
- *Section 5.1.1, “Podman upgrade from 3.4.x to 4.3.1”* (Jira (<https://jira.suse.com/browse/PED-1805>) )

A.4 2023-04-12

A.4.1 New

- *Section 7.7.5, "Add additional information to SCLP CPI"* (Jira (<https://jira.suse.com/browse/PED-472>) )
- *Section 7.7.4, "Support Processor Activity Instrumentation Extension 1"* (Jira (<https://jira.suse.com/browse/PED-472>) )
- *Section 7.7.3, "New CPU-MF Counters for IBM z16 and LinuxONE 4"* (Jira (<https://jira.suse.com/browse/PED-472>) )
- *Section 7.7.2, "Support IBM z16 and LinuxONE 4 Processor-Activity-Instrumentation Facility"* (Jira (<https://jira.suse.com/browse/PED-472>) )
- *Section 7.7.1, "NVMe stand-alone dump support"* (Jira (<https://jira.suse.com/browse/PED-472>) )
- *Section 7.8.3, "Removed ESCON from installer"* (Jira (<https://jira.suse.com/browse/PED-482>) )
- *Section 7.8.2, "Enabled installer to configure PCI-attached networking devices"* (Jira (<https://jira.suse.com/browse/PED-454>) )
- *Section 7.8.1, "Auto scale crashkernel size with hardware changes"* (Jira (<https://jira.suse.com/browse/PED-432>) )
- *Section 7.6.9, "KVM: Enablement of device busid for subchannels"* (Jira (<https://jira.suse.com/browse/PED-3182>) )
- *Section 7.6.8, "Allow to list persisted driverctl definitions"* (Jira (<https://jira.suse.com/browse/PED-2317>) )
- *Section 7.6.7, "KVM: Allow long kernel command lines for Secure Execution guests and QEMU"* (Jira (<https://jira.suse.com/browse/PED-472>) )
- *Section 7.6.6, "KVM: Provide virtual CPU topology to guests"* (Jira (<https://jira.suse.com/browse/PED-445>) )
- *Section 7.6.5, "KVM: Attestation support for Secure Execution (crypto), KVM: Secure Execution Attestation Userspace Tool"* (Jira (<https://jira.suse.com/browse/PED-466>) )
- *Section 7.6.4, "Secure Execution guest dump encryption with customer keys, tool to process encrypted Secure Execution guest dumps"* (Jira (<https://jira.suse.com/browse/PED-449>) )

- *Section 7.6.3, “vfio-ap enhancements”* (Jira (<https://jira.suse.com/browse/PED-456>) )
- *Section 7.6.2, “Enhanced Interpretation for PCI Functions”* (Jira (<https://jira.suse.com/browse/PED-473>) )
- *Section 7.5.6, “ROCE: Independent Usage of Secondary Physical Function”* (Jira (<https://jira.suse.com/browse/PED-470>) )
- *Section 7.5.4, “zipl: Site-aware environment block”* (Jira (<https://jira.suse.com/browse/PED-472>) )
- *Section 7.5.3, “zipl support for Secure Boot IPL and Dump from ECKD DASD”* (Jira (<https://jira.suse.com/browse/PED-472>) )
- *Section 7.5.5, “Transparent PCI device recovery”* (Jira (<https://jira.suse.com/browse/PED-457>) )
- *Section 7.5.2, “zdev: Site-aware device configuration”* (Jira (<https://jira.suse.com/browse/PED-472>) )
- *Section 7.5.1, “Transparent DASD PPRC (Peer-to-Peer Remote Copy) handling”* (Jira (<https://jira.suse.com/browse/PED-444>) )
- *Section 7.4.16, “libica: FIPS 140-3 compliance”* (Jira (<https://jira.suse.com/browse/PED-2871>) )
- *Section 7.4.15, “p11-kit: add IBM specific mechanisms and attributes”* (Jira (<https://jira.suse.com/browse/PED-440>) )
- *Section 7.4.14, “openCryptoki: PKCS #11 3.1 - support CKA_DERIVE_TEMPLATE”* (Jira (<https://jira.suse.com/browse/PED-442>) )
- *Section 7.4.13, “zcryptctl support for control domains - kernel and s390-tools parts”* (Jira (<https://jira.suse.com/browse/PED-480>) )
- *Section 7.4.6, “Display PAI (Processor Activity Instrumentation) CPACF counters (s390-tools)”* (Jira (<https://jira.suse.com/browse/PED-472>) )
- *Section 7.4.12, “libica: eliminate SW fall backs - stage 2”* (Jira (<https://jira.suse.com/browse/PED-468>) )
- *Section 7.4.11, “libica: extend statistics to reflect security measures (crypto)”* (Jira (<https://jira.suse.com/browse/PED-478>) )
- *Section 7.4.10, “openCryptoki key generation with expected MKVP only on CCA and EP11 tokens”* (Jira (<https://jira.suse.com/browse/PED-442>) )



- *Section 7.4.9, “openCryptoki: support crypto profiles”* (Jira (<https://jira.suse.com/browse/PED-442>) )
- *Section 7.4.8, “openCryptoki EP11 token: vendor-specific key derivation”* (Jira (<https://jira.suse.com/browse/PED-442>) )
- *Section 7.4.7, “openCryptoki EP11 token: IBM z16 and LinuxONE 4 support”* (Jira (<https://jira.suse.com/browse/PED-442>) )
- *Section 7.4.5, “zcrypt DD: Exploitation Support of new IBM Z Crypto Hardware for kernel and s390-tools”* (Jira (<https://jira.suse.com/browse/PED-472>) )
- *Section 7.4.4, “openCryptoki ep11 token: master key consistency”* (Jira (<https://jira.suse.com/browse/PED-442>) )
- *Section 7.4.3, “In-kernel crypto: SIMD implementation of chacha20”* (Jira (<https://jira.suse.com/browse/PED-439>) )
- *Section 7.3.1, “zlib CRC32 optimization for s390x”* (Jira (<https://jira.suse.com/browse/PED-1350>) )
- *Section 5.3.1, “Python 3.10 modules, Reduced Python Stack”* (Jira (<https://jira.suse.com/browse/PED-3799>) )
- *Section 7.2.1, “Enablement for MIO Instructions - kernel and rdma-core parts”* (Jira (<https://jira.suse.com/browse/PED-2175>) )

A.4.2 Updated






- Changed SLES release date year to the correct 2023

A.5 2023-03-01

A.5.1 New



- *Section 5.6.2, “Replacement of gpg as recommended tool for file encryption”* (Jira (<https://jira.suse.com/browse/PED-1891>) )
- *Section 5.10.5.1, “open-vm-tools”* (Jira (<https://jira.suse.com/browse/PED-1344>) )

A.5.2 Updated

- *Section 5.10.2, “Xen”* (Jira (<https://jira.suse.com/browse/PED-1858>) )
- *Section 5.10.3, “QEMU”* (Jira (<https://jira.suse.com/browse/PED-1716>) )
- *Section 5.10.1, “KVM”* (Jira (<https://jira.suse.com/browse/PED-1855>) )
- *Section 5.10.4, “libvirt”* (Jira (<https://jira.suse.com/browse/PED-447>) , Jira (<https://jira.suse.com/browse/PED-225>) )




A.6 2023-02-01

A.6.1 New

- *Section 4.1.3, “Installation via SSH on s390x”* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1206585) )
- *Section 5.9.1, “Silence KillMode=None messages”* (Jira (<https://jira.suse.com/browse/PED-407>) )

A.7 2022-11-30

A.7.1 New

- Deprecation of gnote in *Section 8.2, “Deprecated features and packages”* (Jira (<https://jira.suse.com/browse/PED-1839>) )
- Removal of samba-ad-dc-libs in *Section 8.1, “Removed features and packages”* (Jira (<https://jira.suse.com/browse/PED-143>) )
- *Section 5.9.2, “yast2-iscsi-client drops open-iscsi and iscsiui as dependencies”* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1204978) )



A.8 2022-11-02

A.8.1 New


- *Section 5.4.2, “Restoring default Btrfs file compression”* (Jira (<https://jira.suse.com/browse/PED-63>) )
- Added note about `openmpi2` and `openmpi3` in *Section 8.2, “Deprecated features and packages”* (Jira (<https://jira.suse.com/browse/PED-904>) )

A.9 2022-10-18

A.9.1 New

- Added note about removing Kerberos/LDAP from YaST in *Section 8, “Removed and deprecated features and packages”* (Bugzilla (https://bugzilla.suse.com/show_bug.cgi?id=1202257) )
- Added note about removing `thunderbolt-user-space` in *Section 8, “Removed and deprecated features and packages”* (Jira (<https://jira.suse.com/browse/PED-1358>) )

A.9.2 Updated

- Updated Java lifecycle in *Section 5.3.3, “Supported Java versions”* (Jira (<https://jira.suse.com/browse/PED-1590>) ):
 - OpenJDK 11 end of life is now end of 2026
 - OpenJDK 17 added
 - OpenJDK 18 end of life is now end of 2026

B Kernel parameter changes



Warning

This list of changes may not be exhaustive.

B.1 Changes from SP4 to SP5

These Linux kernel parameters have been changed since SLES 15 SP4.