Release Notes

openSUSE Leap is a free and Linux-based operating system for your PC, Laptop or Server. You can surf the Web, manage your e-mails and photos, do office work, play videos or music and have a lot of fun!

Publication Date: 2019-03-14, Version: 15.1.20190314.51e9af5

Contents

1 Installation 2

2 System Upgrade 5

3 Packaging Changes 5

4 Security 6

5 More Information and Feedback 6

This is the initial version of the release notes for the forthcoming openSUSE Leap 15.1.

If you upgrade from an older version to this openSUSE Leap release, see previous release notes listed here: https://en.opensuse.org/openSUSE:Release_Notes.

This public beta test is part of the openSUSE project. Information about the project is available at https://www.opensuse.org.

Report all bugs you encounter using this prerelease of openSUSE Leap 15.1 in the openSUSE Bugzilla. For more information, see https://en.opensuse.org/Submitting_Bug_Reports. If you would like to see anything added to the release notes, file a bug report against the component "Release Notes".

1 Installation

This section contains installation-related notes. For detailed upgrade instructions, see the documentation at https://doc.opensuse.org/documentation/leap/startup/html/book.opensuse.startup/part.basics.html.

1.1 Using Atomic Updates With the System Role *Transactional Server*

The installer supports the system role *Transactional Server*. This system role features an update system that applies updates atomically (as a single operation) and makes them easy to revert should that become necessary. These features are based on the package management tools that all other SUSE and openSUSE distributions also rely on. This means that the vast majority of RPM packages that work with other system roles of openSUSE Leap 15.1 also work with the system role *Transactional Server*.



Note: Incompatible Packages

Some packages modify the contents of `/var` or `/srv` in their RPM `%post` scripts. These packages are incompatible. If you happen upon such package, file a bug report.

To provide these features, this update system relies on:

- **Btrfs snapshots.** Before a system update is started, a new Btrfs snapshot of the root file system is created. Then, all the changes from the update are installed into that Btrfs snapshot. To complete the update, you can then restart the system into the new snapshot.
  To revert the update, simply boot from the previous snapshot instead.

- **A read-only root file system.** To avoid issues with and data loss because of updates, the root file system must not be written to otherwise. Therefore, the root file system is mounted read-only during normal operation.
  To make this setup work, two additional changes to the file system needed to be made: To allow writing user configuration in `/etc`, this directory is automatically configured to use OverlayFS. `/var` is now a separate subvolume which can be written to by processes.



Important: *Transactional Server* Needs At Least 12 GB of Disk Space

The system role *Transactional Server* needs a disk size of at least 12 GB to accommodate Btrfs snapshots.

To work with transactional updates, always use the command **`transactional-update`** instead of YaST and Zypper for all software management:

- Update the system: **`transactional-update up`**
- Install a package: **`transactional-update pkg in`** *PACKAGE_NAME*
- Remove a package: **`transactional-update pkg rm`** *PACKAGE_NAME*
- To revert the last snapshot, that is the last set of changes to the root file system, make sure your system is booted into the next to last snapshot and run: **`transactional-update rollback`**
  Optionally, add a snapshot ID to the end of the command to rollback to a specific ID.

When using this system role, by default, the system will perform a daily update and reboot between 03:30 am and 05:00 am. Both of these actions are systemd-based and if necessary can be disabled using **`systemctl`**:

```
systemctl disable --now transactional-update.timer rebootmgr.service
```

For more information about transactional updates, see the openSUSE Kubic blog posts https://kubic.opensuse.org/blog/2018-04-04-transactionalupdates/ and https://kubic.opensuse.org/blog/2018-04-20-transactionalupdates2/.

1.2 Minimal System Installation

The minimal system installation lacks certain functionality that is often taken for granted:

- It does not contain a software firewall front-end. You can install the package `firewalld` additionally.
- It does not contain a YaST. You can install the pattern `patterns-yast-yast2_basis` additionally.

1.3 Installing on Hard Disks With Less Than 12 GB of Capacity

The installer will only propose a partitioning scheme if the available hard disk size is larger than 12 GB. If you want to set up, for example, very small virtual machines images, use the guided partitioner to tune partitioning parameters manually.

1.4 UEFI—Unified Extensible Firmware Interface

Prior to installing openSUSE on a system that boots using UEFI (Unified Extensible Firmware Interface), you are urgently advised to check for any firmware updates the hardware vendor recommends and, if available, to install such an update. A pre-installation of Windows 8 or later is a strong indication that your system boots using UEFI.

Background: Some UEFI firmware has bugs that cause it to break if too much data gets written to the UEFI storage area. However, there is no clear data of how much is “too much”.

openSUSE minimizes the risk by not writing more than the bare minimum required to boot the OS. The minimum means telling the UEFI firmware about the location of the openSUSE boot loader. Upstream Linux kernel features that use the UEFI storage area for storing boot and crash information (`pstore`) have been disabled by default. Nevertheless, it is recommended to install any firmware updates the hardware vendor recommends.

1.5 UEFI, GPT, and MS-DOS Partitions

Together with the EFI/UEFI specification, a new style of partitioning arrived: GPT (GUID Partition Table). This new schema uses globally unique identifiers (128-bit values displayed in 32 hexadecimal digits) to identify devices and partition types.

Additionally, the UEFI specification also allows legacy MBR (MS-DOS) partitions. The Linux boot loaders (ELILO or GRUB 2) try to automatically generate a GUID for those legacy partitions, and write them to the firmware. Such a GUID can change frequently, causing a rewrite in the firmware. A rewrite consists of two different operations: Removing the old entry and creating a new entry that replaces the first one.

Modern firmware has a garbage collector that collects deleted entries and frees the memory reserved for old entries. A problem arises when faulty firmware does not collect and free those entries. This can result in a non-bootable system.

To work around this problem, convert the legacy MBR partition to GPT.

2 System Upgrade

This section lists notes related to upgrading the system. For detailed upgrade instructions, see the documentation at https://doc.opensuse.org/documentation/leap/startup/html/book.opensuse.startup/cha.update.osuse.html.

Additionally, check *Section 3, "Packaging Changes"*.

3 Packaging Changes

3.1 Deprecated Packages

Deprecated packages are still shipped as part of the distribution but are scheduled to be removed the next version of openSUSE Leap. These packages exist to aid migration, but their use is discouraged and they may not receive updates.

To check whether installed packages are no longer maintained: Make sure that `lifecycle-data-openSUSE` is installed, then use the command:

```
zypper lifecycle
```

3.2 Removed Packages

Removed packages are not shipped as part of the distribution anymore.

- `git-annex`: Has been removed because the package is not maintained anymore.
- `iksemel`: Has been removed because the package is not maintained anymore.
- `mozaddon-bugmenot`: Has been removed because the add-on is no longer compatible with current versions of Firefox.
- `python-dns-lexicon`: Did not build anymore

4 Security

This section lists changes to security features in openSUSE Leap 15.1.

4.1 Users and Groups Associated with AMANDA Backup Utility

AMANDA (*Advanced Maryland Automatic Network Disk Archiver*) is a backup solution that allows setting up a master backup server to back up multiple hosts over network to tape drives/changers or disks or optical media. This tool is shipped in openSUSE within the package `amanda`.

The execution of the binaries in this package is restricted to the group `amanda`. However, some of those binaries use the attribute `setuid` to gain `root` rights. As the implementation of at least some of these binaries is problematic, the user `amanda` and members of the group `amanda` are effectively privileged users whose rights are equivalent to those of `root`.

Hence, carefully consider who you allow access to either the user account or the group.

5 More Information and Feedback

- Read the `README` documents on the medium.
- View a detailed changelog information about a particular package from its RPM:

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

  Replace *`FILENAME`* with the name of the RPM.

- Check the `ChangeLog` file in the top level of the medium for a chronological log of all changes made to the updated packages.
- Find more information in the `docu` directory on the medium.
- For additional or updated documentation, see https://doc.opensuse.org/.
- For the latest product news, from openSUSE, visit https://www.opensuse.org.

Copyright © 2019 SUSE LLC