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: 15.0.20190314.a215c14

Contents

1 Installation 2

2 System Upgrade 5

3 Packaging Changes 8

4 Drivers and Hardware 9

5 Desktop 10

6 Security 15

7 Technical 17

8 More Information and Feedback 18

The release notes are under constant development. To find out about the latest updates, see the online version at https://doc.opensuse.org/release-notes. The English release notes are updated whenever need arises. Translated language versions can temporarily be incomplete.

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

Information about the project is available at https://www.opensuse.org.

To report bugs against this release, use the openSUSE Bugzilla. For more information, see http://en.opensuse.org/Submitting_Bug_Reports.

Major new features of openSUSE Leap 15.0 are also listed at https://en.opensuse.org/Features_15.0.

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.

Make sure to also review *Section 4, "Drivers and Hardware"*.

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

The installer now supports a new system role *Transactional Server* that is an outcome of the openSUSE Kubic effort. This system role features a new 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 15.0 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`**:

```
tux@linux > sudo 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.

1.6 Scaling the Installer UI on Computers with High-DPI Displays

The YaST installer does not scale its UI for High-DPI displays by default. If you have a computer with a high-DPI display, you can set YaST to scale its UI automatically for the display. To do so, add the parameter `QT_AUTO_SCREEN_SCALE_FACTOR=1` to the bootloader command line.

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.

Make sure to also review *Section 4, “Drivers and Hardware”*.

Additionally, check *Section 3, “Packaging Changes”*.

2.1 Upgrading from openSUSE Leap 42.3

2.1.1 Package Downgrades During System Upgrade

The RPM package information of packages shipped in openSUSE Leap 15.0 contain an added openSUSE Leap version string. For this reason, packages that contain the same upstream version of software as shipped in openSUSE Leap 42.3 will be displayed as downgrades, even though they actually contain the same software but compiled for a newer operating system.

2.1.2 `cryptconfig` Has Been Removed

Previous versions of openSUSE Leap supported encrypting home directories individually via `cryptconfig`. This feature and the `cryptconfig` package are not available anymore in openSUSE Leap 15.0.

To encrypt user data on openSUSE Leap 15.0, encrypt the whole partition or volume which contains the home directories.



Tip: Decrypt Before Upgrading

We encourage you to decrypt encrypted home directories before performing an upgrade from openSUSE Leap 42.3. While under openSUSE Leap 15.0, existing encrypted home directories can still be used (the underlying technology, `pam_mount`, is still available), there may not be an easy upgrade path in the future.

There is also no way to individually encrypt the home directories of users added after the upgrade to openSUSE Leap 15.0.

2.1.3 Postfix Admin Uses Backwards-Incompatible Directory Layout

Starting with the version 3.2, as shipped in openSUSE Leap 15.0, Postfix Admin (package `postfixadmin`) uses a new and backwards-incompatible directory layout:

- The configuration files moved to `/etc/postfixadmin`.
- The PHP code moved to `/usr/share/postfixadmin`.
- The Smarty cache moved to `/var/cache/postfixadmin`.

Postfix Admin no longer reads configuration files from their previous locations and the configuration is not migrated automatically. Therefore, you need to migrate the following items manually:

- Move `config.local.php` from `/srv/www/htdocs/postfixadmin` to `/etc/postfixadmin`.
- If you made customizations to `config.inc.php`, ideally merge these customizations into `/etc/postfixadmin/config.local.php`. We recommended keeping `config.inc.php` unmodified.
- In the Apache configuration, add or enable the alias `/postfixadmin`:
  - To make the alias available on all virtual hosts, run:

    ```
    tux@linux > sudo a2enflag POSTFIXADMIN && rcapache2 restart
    ```

  - To make the alias available only on a specific virtual host only, add the alias to the config of that virtual host.

2.1.4 Offline Upgrade Fails When Encrypted Disks Are Mapped by Name

Using the offline upgrade feature of the installation medium on a computer with an encrypted data partition, such as `/home`, can crash the YaST installer when selecting the previous installation.

This happens when the encrypted data partition is listed in `/etc/fstab` by device mapper name, such as `/dev/mapper/cr_home`. In the installation environment, YaST cannot associate that path with an automatically detected volume.

To be able to use the offline upgrade functionality, before starting the upgrade, change `/etc/fstab` to use device UUIDs instead of device names. To determine the correct device UUIDs, use the following command:

```
tux@linux > blkid | grep "DEVICE_MAPPER_NAME"
```

The output of this command will contain a quoted UUID after the string `UUID=`.

2.1.5 GPG Has New Key Database Format

openSUSE Leap 42.3 shipped with GPG 2.0, while openSUSE Leap 15.0 includes GPG 2.2. In between these GPG versions, a new key database format was introduced. GPG 2.2 will automatically upgrade your key ring to the new format. However, the upgraded key ring cannot be used by older versions of GPG anymore.

If you need to keep the older version of your key database available, back up the directory `~/.gnupg` before starting the upgrade to openSUSE Leap 15.0.

2.1.6 `ntpd` Has Been Replaced With Chrony

The time server synchronization daemon `ntpd` has been replaced with the more modern daemon Chrony.

This change means that AutoYaST files with an `ntp_client` section need to be updated to a new format for this section. For more information about the new AutoYaST `ntp_client` format, see https://doc.opensuse.org/projects/autoyast/#Configuration.Network.Ntp.

To synchronize time in intervals, YaST sets up a cron configuration file. From openSUSE Leap 15.0 on, the configuration file used for this is owned by the package `yast2-ntp-client` (previously no package owned it). The configuration file has been renamed from `novell.ntp-synchronization` to `suse-ntp_synchronization` to be consistent with other cron configuration files. The upgrade from previous versions of openSUSE Leap is performed automatically: If a file with the old name is found, it will be renamed and references to `ntpd` in it will be replaced by `chrony` references.

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:

```
tux@linux > zypper lifecycle
```

3.2 Removed Packages

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

- `cryptconfig`: Was not maintained anymore. Use partition encryption instead. For more information, see *Section 2.1.2, "`cryptconfig` Has Been Removed"*.
- `SuSEfirewall2`: Replaced by `firewalld`. For information about migrating to `firewalld`, see https://en.opensuse.org/Firewalld and https://doc.opensuse.org/documentation/leap/security/html/book.security/cha.security.firewall.html#sec.security.firewall.firewalld.
- `php7-imap`: The optional IMAP PHP extension is no longer shipped as the UW IMAP reference implementation is no longer maintained.

4 Drivers and Hardware

4.1 Hang on Machines with Nvidia GPUs and Hybrid Graphics

With the kernel shipped in openSUSE Leap 15.0 GM, the Nouveau driver for Nvidia graphics card may hang at reboot, shutdown, or during runtime power management actions. This bug occurs primarily on system with hybrid graphics, such as laptops that include integrated Intel graphics and a discrete Nvidia graphics card.

The bug will be fixed in a maintenance update for the kernel. However, as the installation image does not receive updates, this issue may occur during installation or first boot even after that update has shipped. In that case, as a temporary workaround, boot with the option `nouveau.modeset=0`. After the updated kernel including the fix is installed, you can remove this option again.

4.2 KDE on Wayland Is Not Supported with Proprietary Nvidia Driver

The KDE Plasma Wayland session is not supported with the proprietary Nvidia driver. If you are using KDE and the proprietary Nvidia driver, stay with the X session.

5 Desktop

This section lists desktop issues and changes in openSUSE Leap 15.0.

5.1 No Default Compose Key Combination

In previous versions of openSUSE, the compose key combination allowed typing characters that were not part of the regular keyboard layout. For example, to produce “å”, you could press and release `Shift`–`Right Ctrl` and then press `a` twice.

In openSUSE Leap 15.0, there is no longer a predefined compose key combination because `Shift`–`Right Ctrl` does not work as expected anymore.

- To define a system-wide custom compose key combination, use the file `/etc/X11/Xmodmap` and look for the following lines:

```
[...]
!! Third example: Change right Control key to Compose key.
!! To do Compose Character, press this key and afterwards two
!! characters (e.g. `a' and `^' to get 342).
!remove  Control  = Control_R
!keysym Control_R = Multi_key
!add     Control  = Control_R
[...]
```

  To uncomment the example code, remove the `!` characters at the beginning of lines. However, note that the setup from `Xmodmap` will be overwritten if you are using **`setxkbmap`**.

- To define a user-specific compose key combination, use your desktop's keyboard configuration tool or the command-line tool **`setxkbmap`**:

```
tux@linux > setxkbmap [...] -option compose:COMPOSE_KEY
```

For the variable *COMPOSE_KEY*, use your preferred character, for example `ralt`, `lwin`, `rwin`, `menu`, `rctl`, or `caps`.

- Alternatively, use an IBus input method that allows typing the characters you need without a Compose key.

5.2 Use **update-alternatives** to Set Login Manager and Desktop Session

In the past, you could use `/etc/sysconfig` or the YaST module */etc/sysconfig Editor* to define the login manager and desktop session. Starting with openSUSE Leap 15.0, the values are not defined using `/etc/sysconfig` anymore but with the alternatives system.

To change the defaults, use the following alternatives:

- Login manager: `default-displaymanager`
- Wayland session: `default-waylandsession.desktop`
- X desktop session: `default-xsession.desktop`

For example, to check the value of `default-displaymanager`, use:

```
tux@linux > sudo update-alternatives --display default-displaymanager
```

To switch the `default-displaymanager` to **`xdm`**, use:

```
tux@linux > sudo update-alternatives --set default-displaymanager \
  /usr/lib/X11/displaymanagers/xdm
```

To enable graphical management of alternatives, use the YaST module *Alternatives* that can be installed from the package `yast2-alternatives`.

5.3 No Screen Lock When Using GNOME Shell But Not GDM

When using GNOME Shell together with a login manager other than GDM, such as SDDM or LightDM, the screen will not blank or lock. Additionally, switching users without logging out is not possible.

To be able to lock the screen from GNOME Shell, enable GDM as your login manager:

1. Make sure that the package `gdm` is installed.

2. Set GDM as the display manager:

```
tux@linux > sudo update-alternatives --set default-displaymanager \
  /usr/lib/X11/displaymanagers/gdm
```

3. Reboot.

5.4 Scaling the SDDM UI on Computers with High-DPI Displays

The default login manager for KDE, SDDM, does not scale its UI for High-DPI displays by default. If you have a computer with a high-DPI display, you can set SDDM to scale its UI automatically for the display using the configuration file `/etc/sddm.conf`:

```
[X11]
EnableHiDPI=true
ServerArguments=-nolisten tcp -dpi DPI_VALUE
```

Replace *`DPI_VALUE`* with an appropriate DPI value, such as `192`. For best scaling results, use a DPI value that is a multiple of the default 96 DPI.

5.5 Scaling the YaST UI on Computers with High-DPI Displays

YaST does not scale its UI for High-DPI displays by default. If you have a computer with a high-DPI display, you can set YaST to scale its UI automatically for the display. To do so, set the environment variable `QT_AUTO_SCREEN_SCALE_FACTOR=1`.

5.6 Using Automatic Scaling in Qt Applications in Setups Which Mix High-DPI/Regular-DPI Monitors

Qt supports automatic per-monitor scaling on X. It uses the DPI value of the virtual X screen to calculate the font size for the primary monitor. By default, this value is 96 DPI. It uses the relative DPI of the primary monitor to derive font DPI for all other monitors.

Two widely used desktops will override this behavior of Qt, therefore this note does not apply to them:

- GNOME will set `Xft.dpi` to the configured multiple of 96 DPI.
- KDE Plasma disables the automatic scaling of Qt and uses a manual scaling configuration.

On other desktops, this behavior of Qt can lead to undesirable situations such as the following: If the primary display is High-DPI (>= 144 DPI), fonts in Qt applications that request scaling, such as VLC, are effectively scaled to half the desired size on all monitors. Applications which do not request scaling, such as YaST (with default settings), use the same DPI value on all monitors. Hence, they will look smaller on the High-DPI monitor.

You can use one of the following workarounds for this issue:

- Use a monitor with a regular DPI value as the primary monitor. Applications that request scaling are then scaled appropriately on the High-DPI monitor.
- Set an appropriate font DPI (`Xft.dpi`). You can do so either with the configuration utility of your desktop. Alternatively, after every login run the following command:

  ```
  tux@linux > echo Xft.dpi:DPI_VALUE | xrdb -nocpp -merge
  ```

  Replace *`DPI_VALUE`* with an appropriate DPI value for the primary monitor.

5.7 Screen Sharing Does Not Work in Firefox or Chromium on Wayland

Firefox and Chromium normally allow Web-based tools such as videoconferencing applications to share the entire screen or individual application windows. This functionality is currently not supported in either browser when using a Wayland session.

To be able to share your screen in Firefox or Chromium, use an X session instead.

5.8 Playing MP3 Media Files

The codecs to play MP3 media files are shipped as part of the standard repository.

To use this decoder in gstreamer-based applications and frameworks, such as Rhythmbox or Totem, install the package `gstreamer-plugins-ugly`.

5.9 No Support for Type-1 Fonts in LibreOffice

LibreOffice 5.3 and higher do not support legacy Type-1 fonts (file extensions `.afm` and `.pfb`) anymore. Most users should not be affected by this, as current fonts are available either in the format TrueType (`.ttf`) or OpenType (`.otf`) formats.

If you are affected by this, convert Type-1 fonts to a supported format, such as TrueType and then use the converted fonts. Conversion is possible with the application FontForge (package `fontforge`) which is included in openSUSE. For information on scripting such conversions, see https://fontforge.github.io/en-US/documentation/scripting/.

5.10 FreeType Font Rendering Changes

FreeType 2.6.4 has a new default glyph hinting interpreter (version 38) that more closely matches other operating systems but may look "more fuzzy" to some. To restore the previous FreeType behavior, set the following environment variable at any level (system-wide, user-specific, or program-specific) of your choice:

```
FREETYPE_PROPERTIES="truetype:interpreter-version=35"
```

5.11 Enabling KDE Plasma Browser Integration

Plasma browser integration for Firefox and Chromium/Chrome allows monitoring multimedia and downloads using KDE system tools and gives quick access to tabs via the *Run Command* bar of the KDE Plasma desktop.

The browser integration functionality consists of two parts that need to work together:

- The desktop part that can be installed using the system package `plasma-browser-integration`.
- The browser part that needs to be installed from the add-on store of your browser:
  - Firefox: https://addons.mozilla.org/firefox/addon/plasma-integration/
  - Chromium/Chrome: https://chrome.google.com/webstore/detail/plasma-integration/cimiefiiaegbelhefglklhhakcgmhkai

Note that this functionality is officially still in development and openSUSE Leap 15.0 ships with an early version of it.

5.12 Loading the Emacs `psgml` Module

Because of conflicts with Emacs modules from the default installation, openSUSE Leap 15.0 can no longer load the `psgml` module automatically. For more information, see the file `README` from the package `psgml`.

6 Security

This section lists changes to security features in openSUSE Leap 15.0.

6.1 GPG Does Not Support GPG V3 Keys Anymore, Resulting in Zypper/`rpm` Warnings

openSUSE Leap 42.3 shipped with GPG 2.0, while openSUSE Leap 15.0 includes GPG 2.2. In between these GPG versions, support for GPG V3 keys was removed. If your system's key database still contains GPG V3 keys, you may receive warnings about this when executing Zypper or `rpm` commands, as these commands are checking the integrity of the package database. These warnings take the form `warning: Unsupported version of key: V3`.

Usually, these warnings are benign, as these keys may have been used for repositories that are no longer enabled on the system or that have since had key updates. However, if these keys are still in active use by the upstream repository, they must be replaced as soon as possible:

- Package management tools in openSUSE Leap 15.0 can no longer use them to verify package integrity.
- The keys in themselves are insecure. Hence, even though older package management tools will use them to verify integrity of packages, the result of this check cannot be trusted anymore.

To delete such keys, perform the following:

1. Run an `rpm` command with high verbosity and check its output:

```
tux@linux > rpm -vv -qf /etc
ufdio: 1 reads, 18883 total bytes in 0.000006 secs
[...]
D: read h# 168 Header sanity check: OK
warning: Unsupported version of key: V3
```

```
[...]
```

In the example, header 168 is associated with an outdated key—the warning appears directly after the message that this specific header is being checked.

2. Find out the key number associated with the header:

```
tux@linux > rpm -q --querybynumber HEADER
```

Replace *HEADER* with the required header number. In the example, that would be `168`. This command returns a key identifier starting with `gpg-pubkey-`.

3. *(Optional)* Use the key identifier (*KEY_ID*) to learn more about the key:

```
tux@linux > rpm -qi KEY_ID
```

4. Remove the key from the system:

```
tux@linux > sudo rpm -e KEY_ID
```

5. If you continue to see warnings on subsequent uses of package management tools, repeat the procedure.

6.2 `systemctl stop apparmor` Does Not Work

In the past, there could be confusion over the difference between how the very similarly named **`systemctl`** subcommands `reload` and `restart` worked for AppArmor:

- **`systemctl reload apparmor`** properly reloaded all AppArmor profiles. (It was and continues to be the recommended way of reloading AppArmor profiles.)
- **`systemctl restart apparmor`** meant that AppArmor would stop, thereby unloading all AppArmor profiles and then restart which left all existing processes unconfined. Only newly started processes would then be confined again.

Unfortunately, `systemd` does not provide a solution within its unit file format for the issue posed by the `restart` scenario.

Starting with AppArmor 2.12, the command **`systemctl stop apparmor`** will not work. As a consequence, **`systemctl restart apparmor`** will now correctly reload AppArmor profiles.

To unload all AppArmor profiles, use the new command **`aa-teardown`** instead which matches the previous behavior of **`systemctl stop apparmor`**.

For more information, see https://bugzilla.opensuse.org/show_bug.cgi?id=996520 and https://bugzilla.opensuse.org/show_bug.cgi?id=853019.

7 Technical

7.1 Updated Btrfs Subvolume Layout

openSUSE Leap 15.0 introduces a new default Btrfs subvolume layout that aims for the following:

- Simplified snapshots and rollbacks
- Prevention of accidental data loss
- Better performance of databases and VM images stored in `/var`

Instead of using multiple Btrfs subvolumes for different subdirectories of `/var`, openSUSE Leap 15.0 ships with a single subvolume for all of `/var`. This new subvolume has copy-on-write functionality disabled.

There is no defined way of upgrading to this new Btrfs subvolume layout. Therefore, if you want to take advantage of it, make sure to freshly install openSUSE Leap 15.0 instead of upgrading.

For more information on the default Btrfs subvolume layout before and after this change, see https://en.opensuse.org/SDB:BTRFS.

7.2 Wicked: Using RFC 4361 DHCPv4 `client-id` on Ethernet

RFC 4361 updates the `client-id` defined in RFC 2132, section 9.14 to be compatible with DHCP 6 `client-id` (`duid`). The use of an RFC 4361 is mandatory on Infiniband (RFC 4390) and is also required to perform DNS record updates in the same zone for DHCP 4 and DHCP 6 addresses also on Ethernet.

In openSUSE Leap 15.0:

- ISC DHCP 4.3.x server supports the new RFC 4361 (required for DNS update)
- Wicked provides an option to send such a `client-id` and to automatically use a DHCPv6-based `client-id` in DHCPv4 (used on Infiniband).

To send the `client-id` during the installation, use `linuxrc` (also see https://en.opensuse.org/SDB:Linuxrc) with the following `ifcfg`:

```
ifcfg=eth0=dhcp,DHCLIENT_CLIENT_ID=01:03:52:54:00:02:c2:67,DHCLIENT6_CLIENT_ID=00:03:52:54:00:02:c2:67
```

For more information, see the documentation for the options `dhcp4 "create-cid"`, `dhcp6 "default-duid"` in `man 5 wicked-config`, `wicked duid --help`, and `wicked iaid --help`.

The traditionally used RFC 2132 DHCPv4 `client-id` on Ethernet is constructed from the hardware type (`01` for Ethernet) and followed by the hardware address (the MAC address), for example:

```
01:52:54:00:02:c2:67
```

The RFC 4361 `client-id` starts with `0xff` (instead of the hardware type), followed by the DHCPv6 IAID (the interface-address association ID that describes the interface on the machine), followed by the DHCPv6 DUID (`client-id` which identifies the machine).

Using the above hardware type-based and hardware address-based DUID (LLT type used by default), the new RFC 4361 DHCPv4 `client-id` would be:

- Using the last bytes of the MAC address as the IAID: `ff:00:02:c2:67:00:01:xx:xx:xx:xx:52:54:00:02:c2:67`
- When the IAID is a simple incremented number: `ff:00:00:00:01:00:01:xx:xx:xx:xx:52:54:00:02:c2:67`

The `xx:xx:xx:xx` in the DUID-LLT is a creation timestamp. A DUID-LL (`00:03:00:01:`*`MAC`*) does not have a timestamp.

8 More Information and Feedback

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

  ```
  tux@linux > 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