WORK IN PROGRESS

This page is not done yet - cocomeat4

openSUSE

A good security/usability/privacy/freedom compromise operating system that should fit most people's needs.

openSUSE comes in 4 different versions. In this guide, we will talk about how to choose the right one, the advantages and disadvantages of each version and how to set them up.

The choice

The 4 different openSUSE editions are:

- openSUSE Tumbleweed, a rolling release with fresh software (but that is quite reliable because it's well-tested by an automated system but also by humans and using a snapshots system). It is your only option if you are using a 32 bit computer.

- openSUSE Leap, a fixed release that gets a new version every 7 months based on the source code of SUSE Linux Enterprise. Very recent drivers won't be included in this edition before the release of its next version. Sadly, it doesn't support graphical system upgrades from version N to N+1

- openSUSE MicroOS, based on Tumbleweed, MicroOS uses Transactional (Atomic) updates upon a read-only btrfs root file system. Most of the filesystem being read-only, this edition is overally more secure than the two classic editions and is the best you can get out of openSUSE in terms of security.

- openSUSE Leap Micro, the same as MicroOS, but based on Leap, and server-oriented. This one doesn't provide any graphical user interface by default so we won't use it in this guide

Requirements

- 2 Ghz dual core processor or better

- 2GB physical RAM + additional memory for your workload

- Over 40GB of free hard drive space

- Either a DVD drive or USB port for the installation media (This guide will only explain how to make an USB stick, not a DVD)

- Internet access is helpful, and required for the Network Installer

Optionally, you can have:

- UEFI, required for Secure Boot - Secure Boot, it will improve your security.

Download openSUSE

To download openSUSE, every edition is available at https://get.opensuse.org. You should use the offline image because the network installers are very, very slow. Installing offline will also make sure you aren't installing malware if the repositories ever get hacked.

You should verify your download to make sure your OpenSUSE iso image is safe and sound.

To verify your download :

- Scoll down on the download page to the "Verify Your Download Before Use"

- There is a line that starts with "It should be [some suite of characters in blue]"

- Click that line of characters, it should download a .asc file that starts with gpg-pubkey

- Now sroll up to the download section on the download page

- Click the arrow next to the download button and download the "Checksum" file

- Click the arrow again, this time right click on "Checksum" and copy the link address

- Paste the link you just copied in your browser's url bar and add ".asc" at the end of it, it should download an extra file

- Now, open a terminal in your downloads folder. If you're on windows, you can use Cygwin: https://www.cygwin.com

- Type the following commands:

This will import the OpenSUSE GPG key :

```
gpg --import gpg-pubkey-*.asc
```

This will verify the checksum file. Do not include "<" and ">":

```
gpg --verify <insert the name of the checksum ASC file you downloaded here>
```

You should have a line `gpg: Good signature from` "openSUSE Project Signing Key opensuse@opensuse.org". This means that the checksum file is safe. If you don't have that line, you shouldn't trust what you have downloaded.

This will verify the checksum of the installer iso image. :

```
sha256sum openSUSE-*.sha256
```

You may get an error `sha256sum: openSUSE-something.iso: No such file or directory`. In that case, change the filename in the .sha256sum file to match the file you downloaded. Alternatively, run `sha256sum openSUSE-*.iso && cat openSUSE-*.sha256` and compare both outputs. If they are the same, your file is safe. You should have `openSUSE-something.iso: OK`. If you don't, it means your iso image has a problem and you shouldn't trust it.

If everything is fine, your iso image is safe and you can proceed to the creation of a bootable USB stick.

Prepare the USB stick

Now that we made sure that what we downloaded is safe, we should prepare a bootable USB stick. First, you will need a tool such as balenaEtcher: https://www.balena.io/etcher.

Once balenaEtcher is downloaded, open it and plug your USB stick into your computer.

Now, click the "Select Image" button and select the .iso file you downloaded

Next, click the "Select drive" button and select your USB stick

Now click "Flash" and wait till it finishes.

Your USB stick should now be ready to install openSUSE on your computer.

Installation

Boot your USB stick, you should be prompted by a small menu, select "Installation" with your keyboard arrows.

Be aware the following is for openSUSE MicroOS, the steps for other openSUSE editions are very similar but classic editions prompt for disk setup earlier than we do it in this guide, just scroll down to see what you should do, everything is explained here, just not in the right order for classic editions.
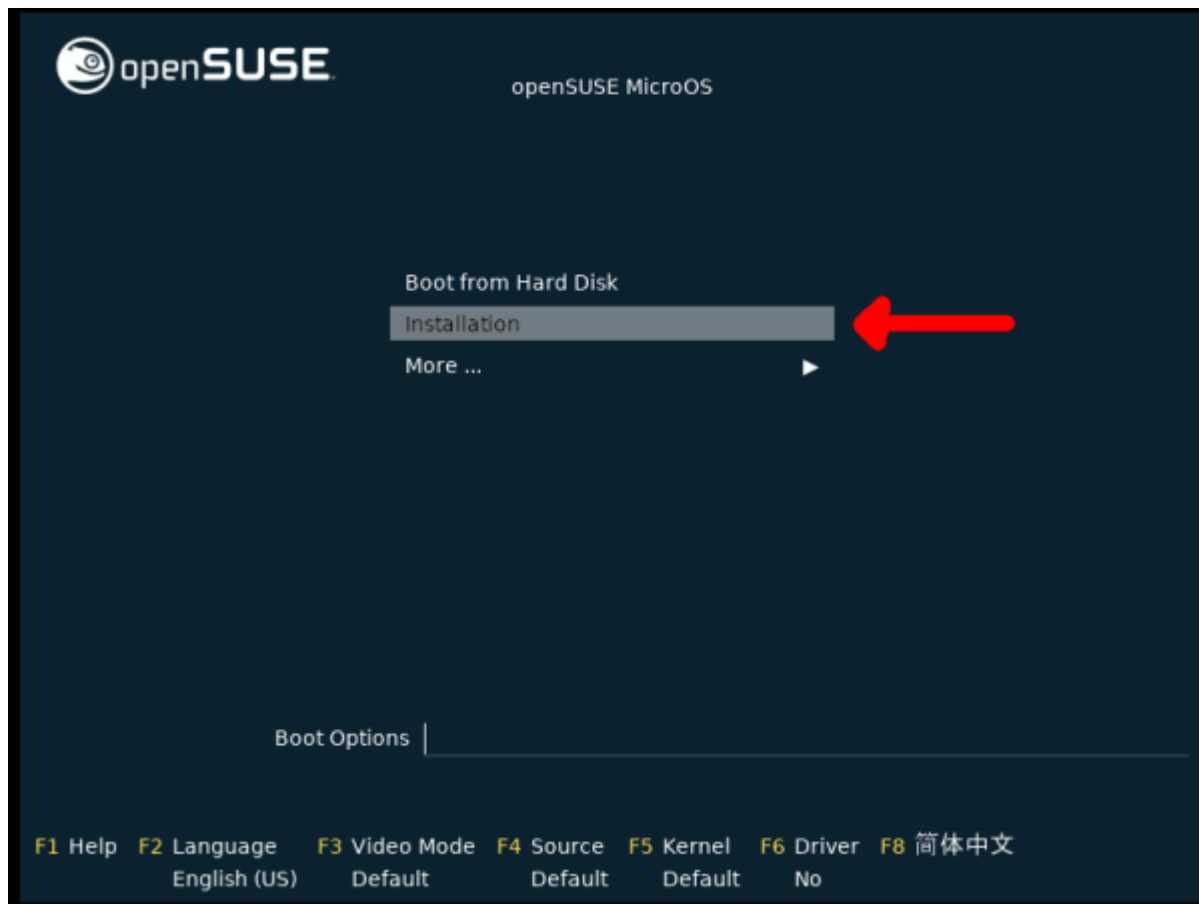
Now wait till the installer loads. It may take some time, especially if your USB stick is slow, so grab a coffee ☕.

Once the installer has started, you will be welcomed by a Language and Keyboard selection page. Set up your language and keyboard layout then click next.
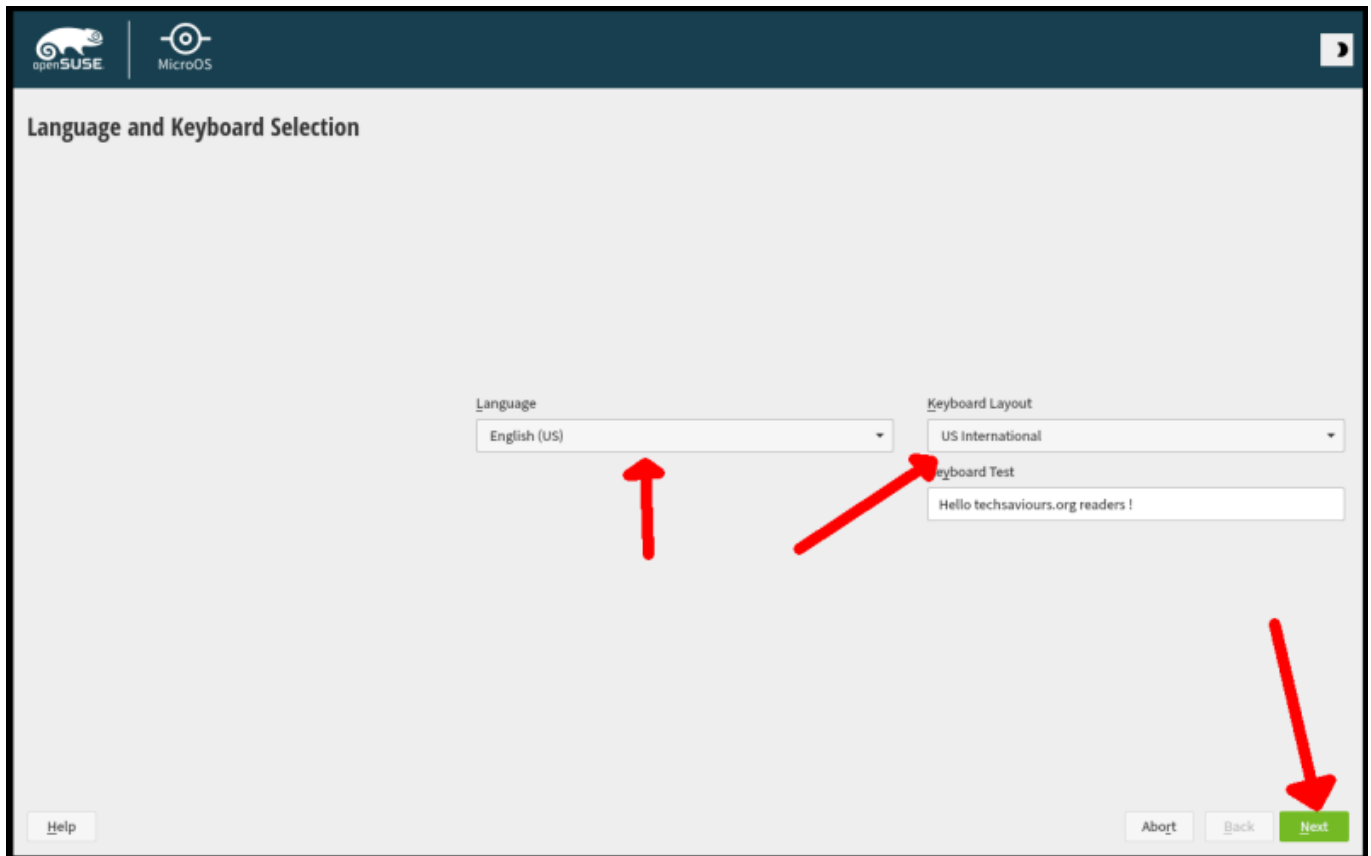
Next, you will be prompted to choose a System Role. This is basically what you want to do with your openSUSE installation. You should choose either GNOME or KDE Plasma when using MicroOS. If you use openSUSE Tumbleweed, you can choose Xfce here, which isn't available in other editions. It is much lighter. On the screenshot, I chose GNOME. As of time of writing, both are still experimental in MicroOS, but I had no issues so far with both.
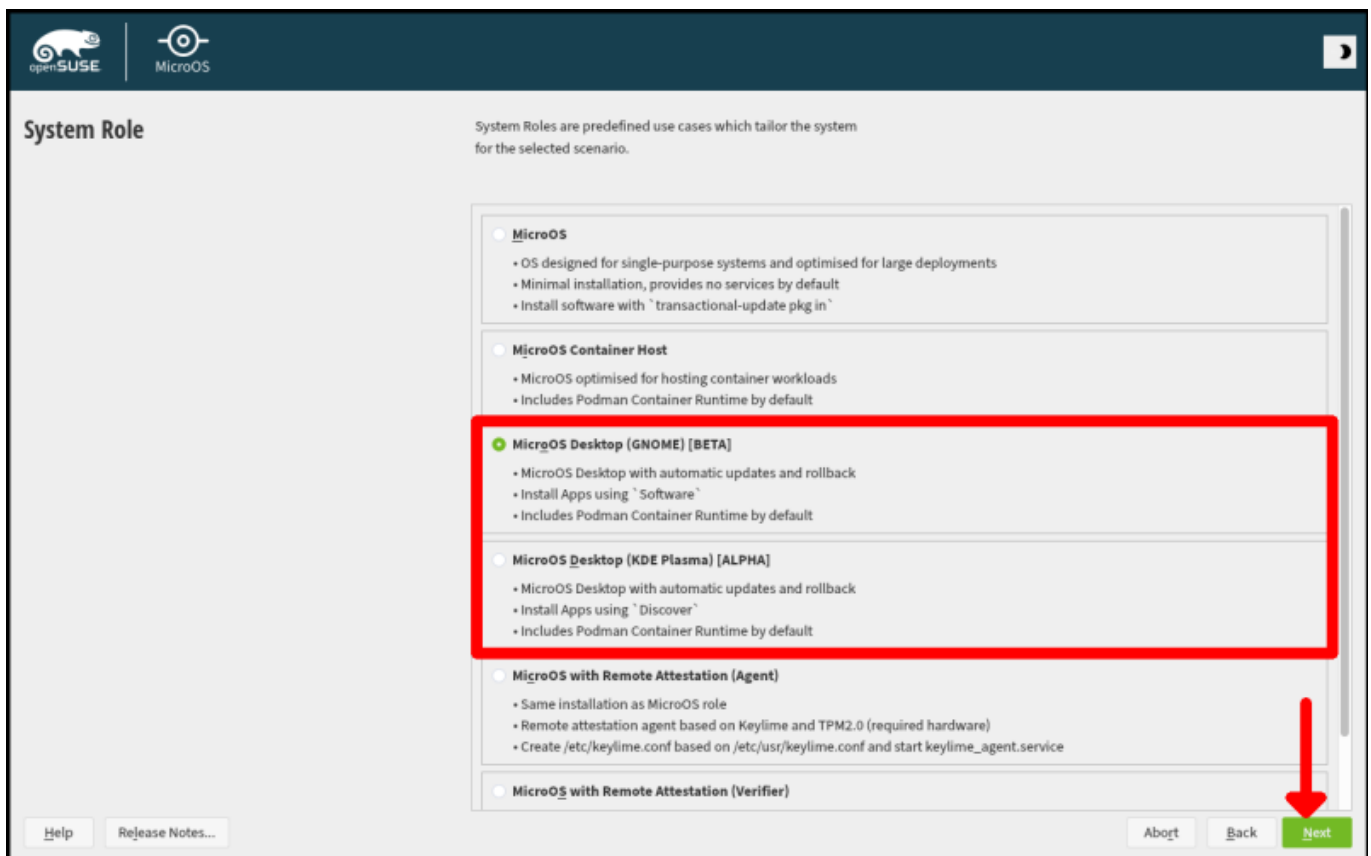
Next, the installer will prompt you to create a new user, choose whatever you want for your full name, but the username should be kept simple (no caps, no spaces, no special characters, i'd recommend you limit to a-z and 0-9).

Preferably, setup a strong password. You can enable automatic login as we will setup disk encryption later.
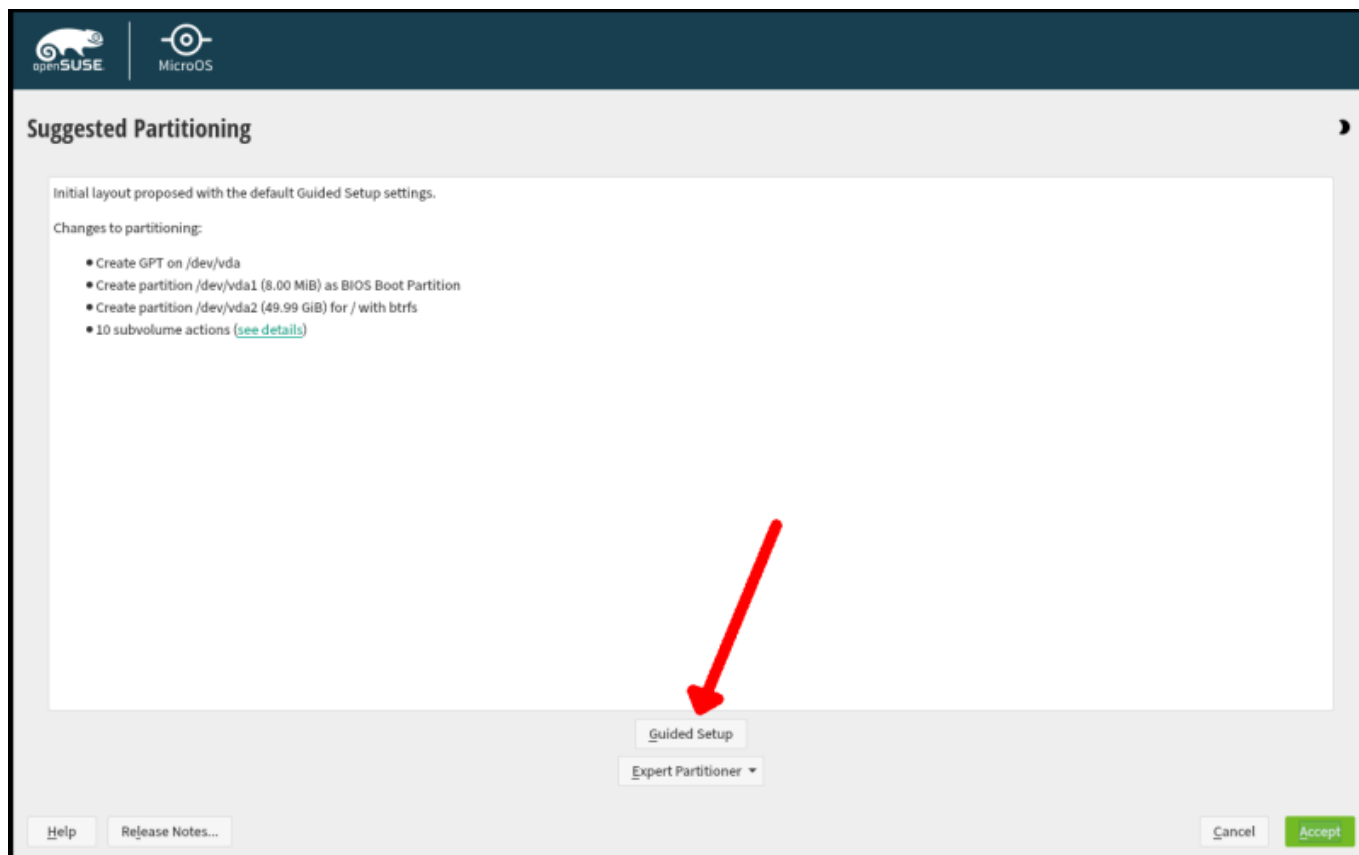
You can also use that password for the system administrator, as we will lock it later in the hardening part.
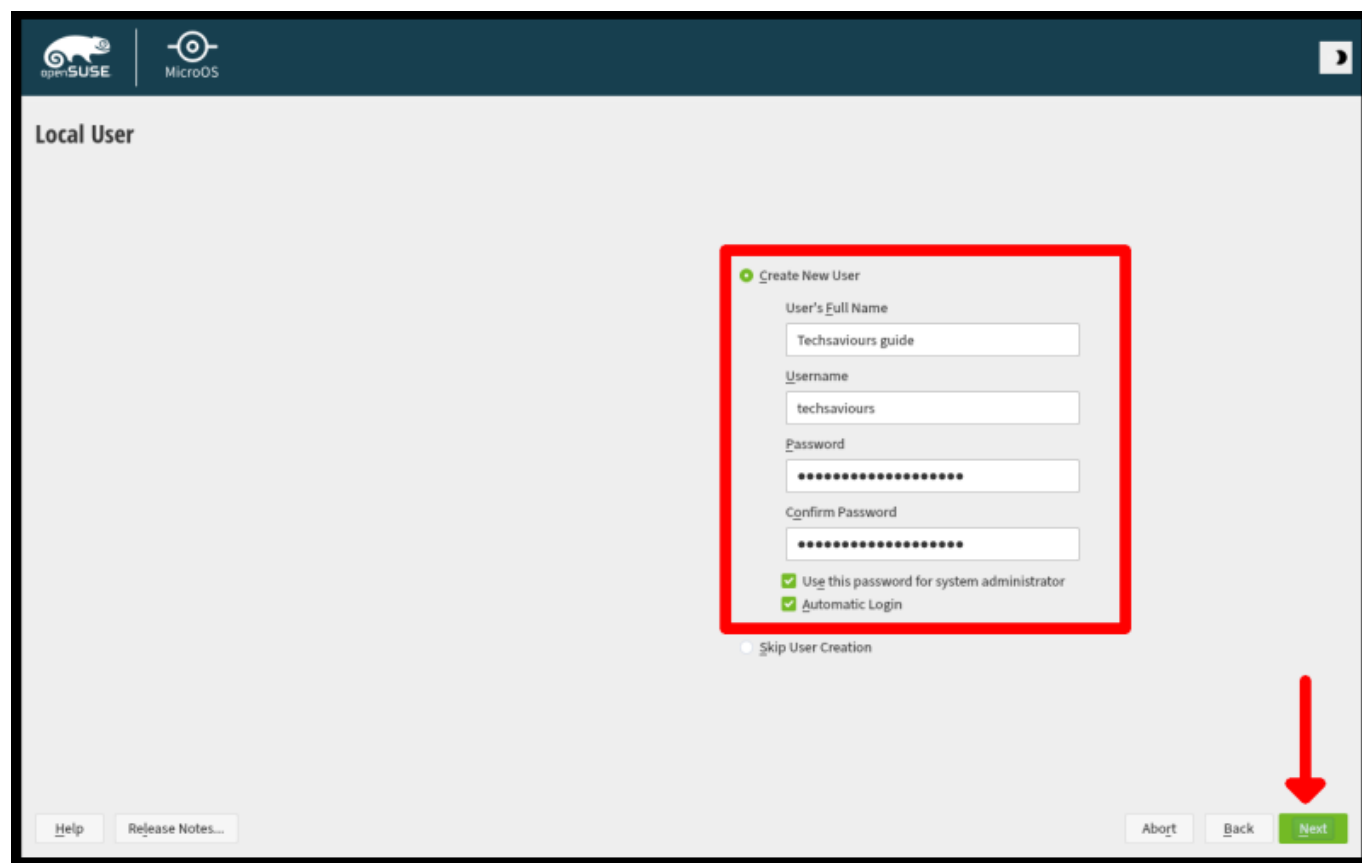

You should then arrive on the Installation Settings page, skipping the traditional partitioning and software selecting steps. First, go into Partitioning to enable encryption
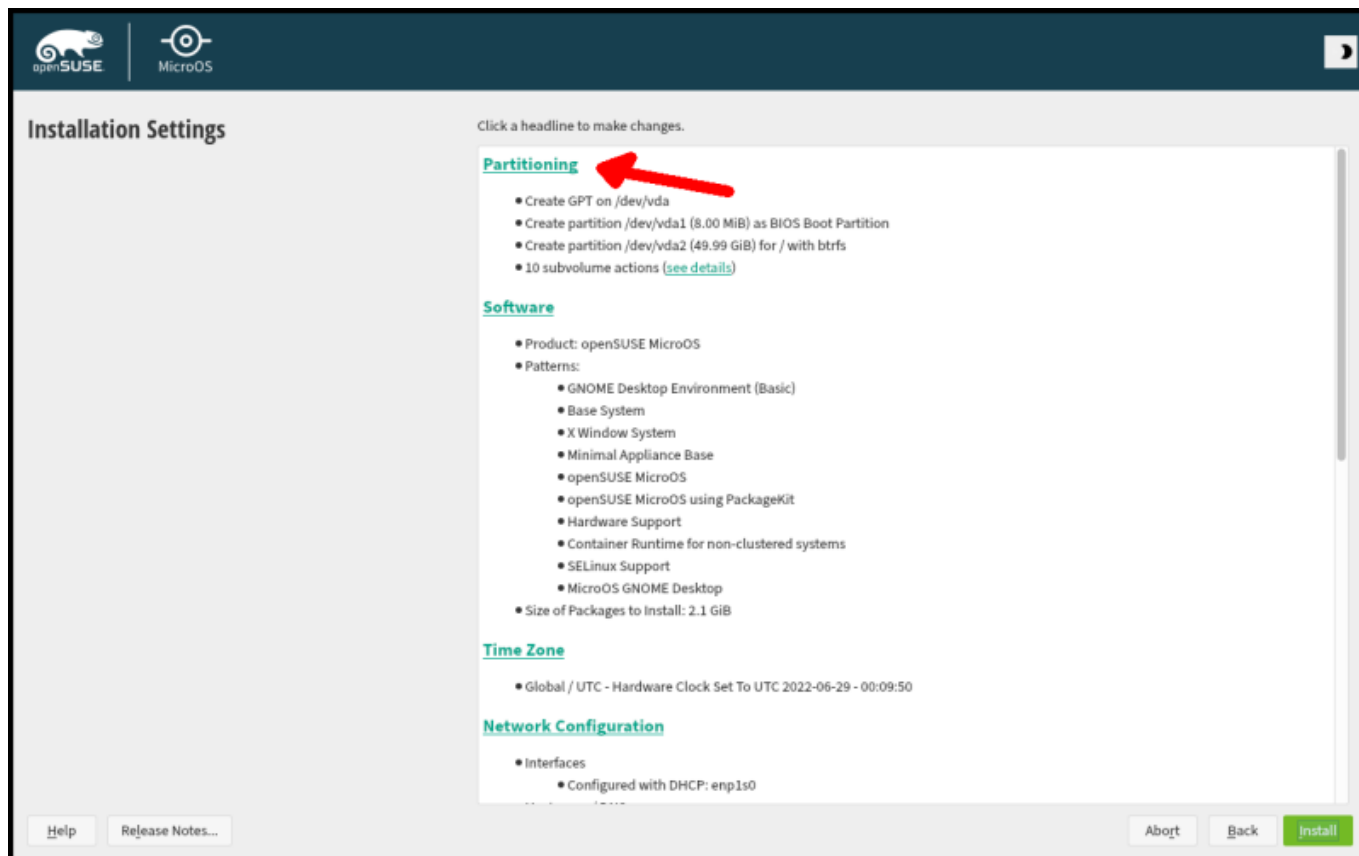
Next we will use the Guided Setup, because it is easier and feature complete.

Now enable Disk Encryption and enter a strong passphrase that will be asked every time you start your computer.
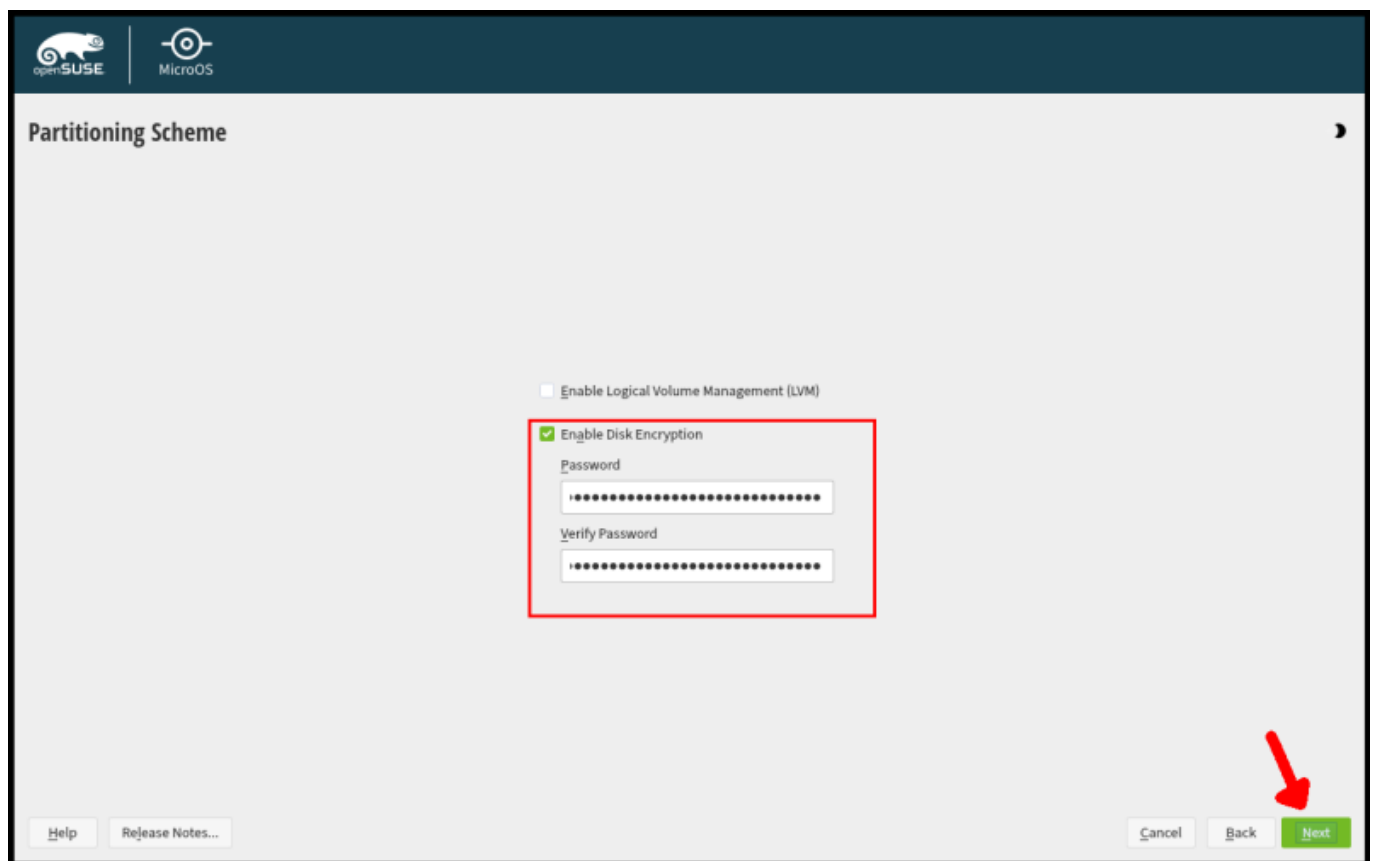
Next it will ask what File System to use for the Root partition, keep Btrfs.

Keep the defaults for any other options until you return to the Installation Settings menu.

Once encryption is setup, you can proceed to the install. Everything else that need to be configured will be configured later.
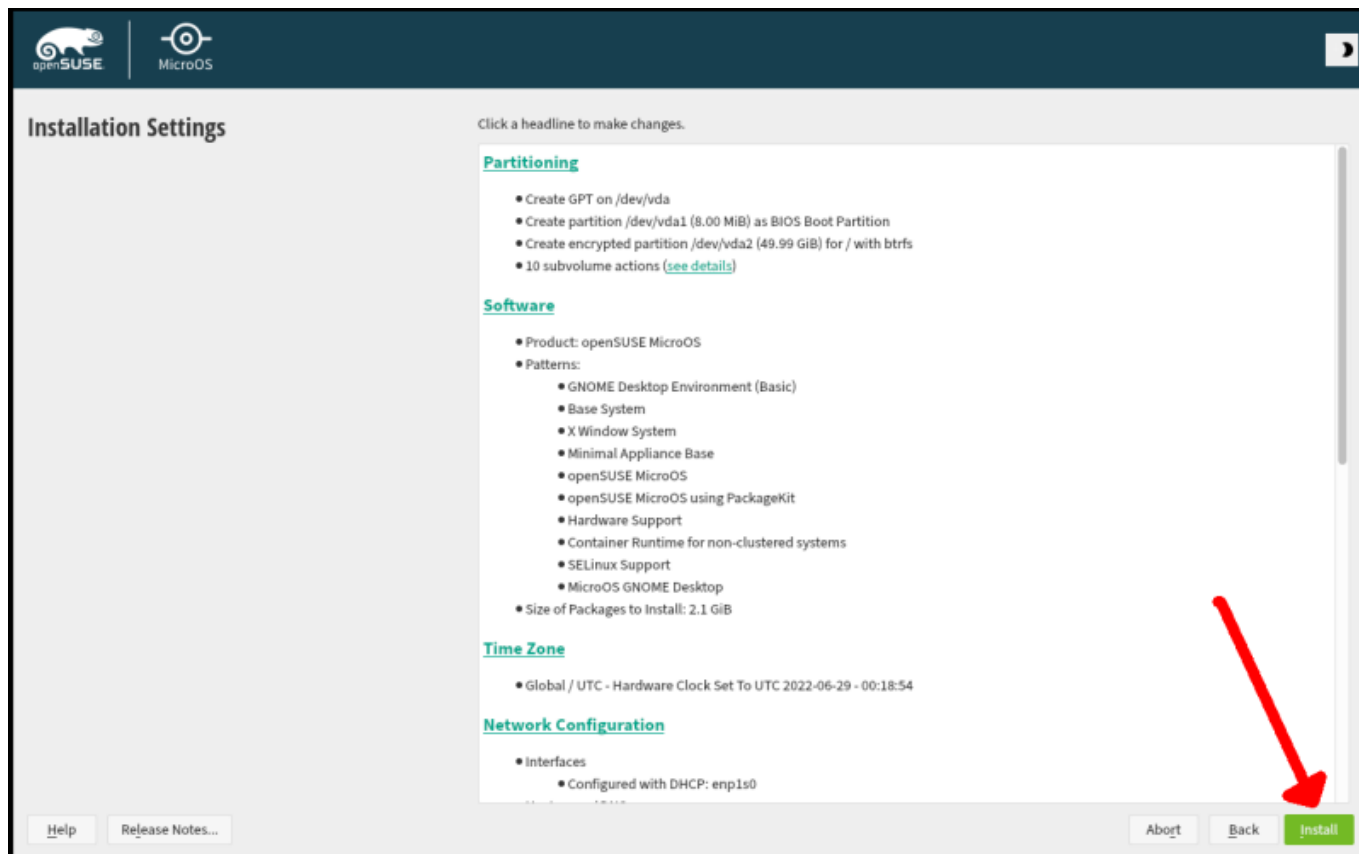
This will, again, take some time. So grab some chocolate 🍫 (because you're likely out of coffee at this point).

Once the install has finished, the system will automatically reboot...
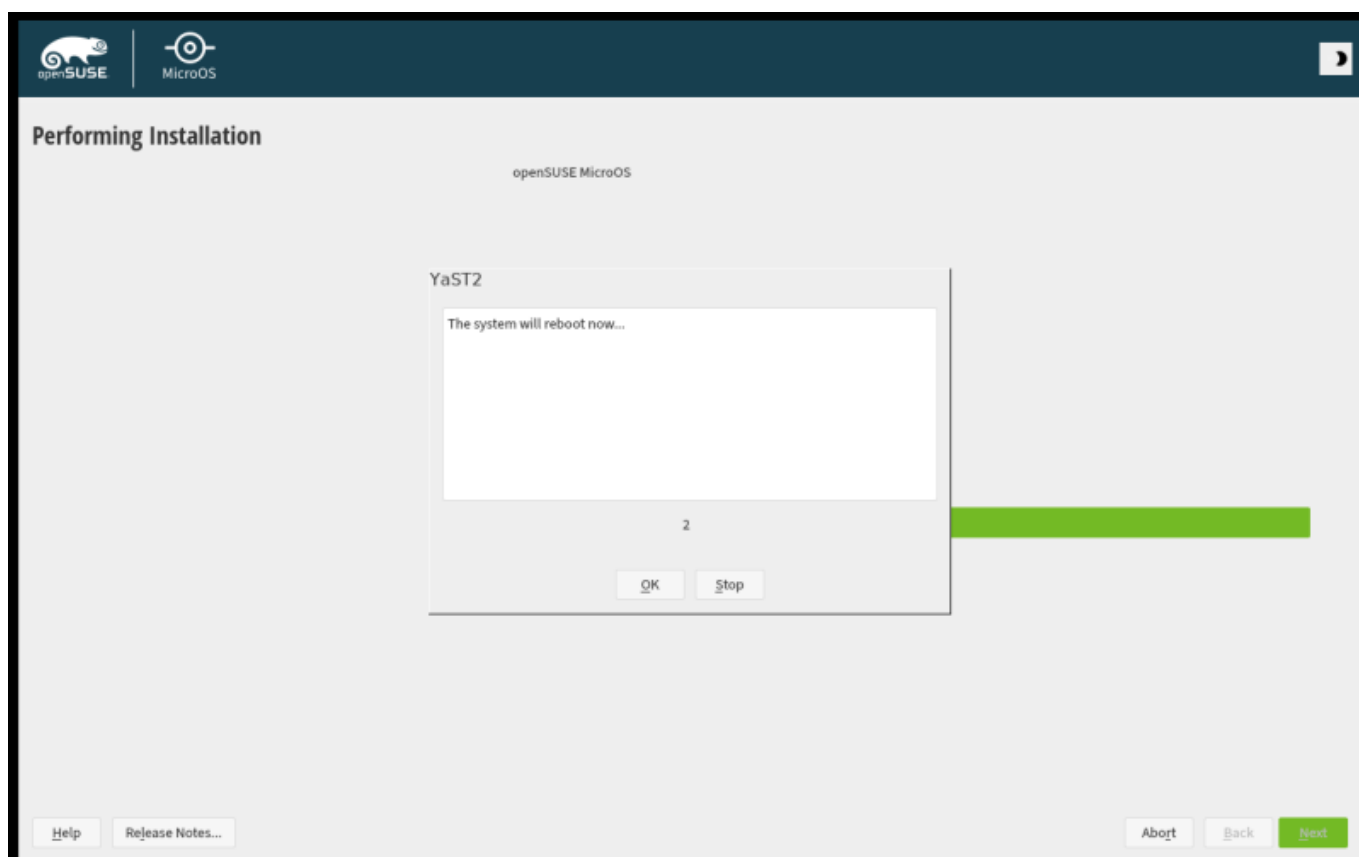
And you did it ! openSUSE is installed ! Now the fun begins, let's make it secure and set things up.

First boot

Just after rebooting, you will be prompted by GRUB that will ask you for your encryption passphrase:

It may look at bit different for you, this is how it looks in my virtual machine.

Once grub has been unlocked, openSUSE will boot automatically after 10 seconds, you can press enter to speed up the process.

openSUSE will ask you your encryption passphrase one more time to unlock the rest of the disk, as you have only unlocked the boot partition so far, which uses an older version of LUKS.

From:

http://wiki.techsaviours.org/ - **Your Digital Privacy DIY Solutions | TECH SAVIOURS .ORG**

Permanent link:

http://wiki.techsaviours.org/en/desktop/operating_systems/opensuse?rev=1656469377

Last update: **2022/10/24 08:24**