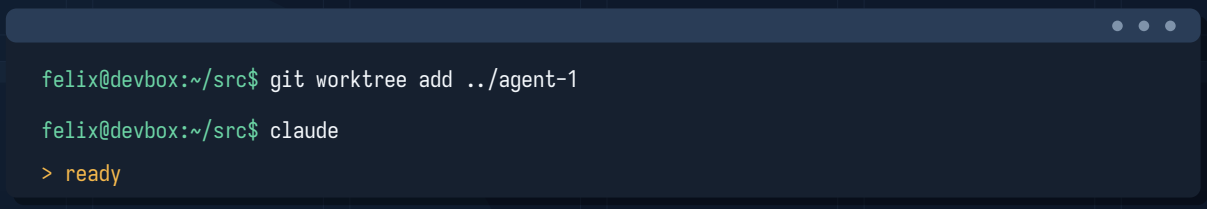
Linux
on the Desktop

A Practical Guide to Fedora® 45 and KDE Plasma
for Professionals

Wolfgang Kerschbaumer

SYSINIT PRESS





Linux on the Desktop

Preface and Installation Chapter

Wolfgang Kerschbaumer

Contents

Preface **1**
Who this book is for . . . 1
Why Fedora 45 and KDE Plasma . . . 1
Choose a reading path . . . 1
Commands and examples . . . 2
Coverage and limits . . . 2
Reporting an error . . . 3

Complete edition outline **4**
Front . . . 4
Part1 Foundations . . . 4
Part2 Plasma . . . 4
Part3 System . . . 4
Part4 Developer . . . 5
Part5 Under The Hood . . . 5
Part6 Appendices . . . 5

3 Installing Fedora 45 KDE **6**
3.1 Booting the live image . . . 6
3.2 The Anaconda Web UI . . . 7
3.3 Choosing the installation method . . . 8
3.4 Encryption . . . 9
3.5 Review and install . . . 11
3.6 Under the hood: what the installer built . . . 13
3.6.1 Partitions and file systems . . . 13
3.6.2 Btrfs subvolumes and mount options . . . 13
3.6.3 The LUKS container . . . 14
3.6.4 Installer logs . . . 15
3.7 Takeaways . . . 15

Preface

This book follows a Fedora® Linux 45 KDE Plasma workstation from installation to daily work and recovery. You will configure the desktop, manage files and applications, maintain the system, and work with remote machines. Development chapters cover Git, containers, language toolchains, and AI coding agents. The advanced sections explain the processes and configuration files behind the interface.

This is version 1.0, prepared on November 4, 2026, the day after Fedora 45 was released. The installation chapters were checked on a fresh installation from the release image, and the rest of the book against the release packages and the first updates (Plasma 6.8.2). Hardware-dependent procedures still need verification on your hardware. Read the coverage notes below before using a procedure on a machine you depend on.

Who this book is for

If you are new to Linux, read the foundations and desktop chapters in order. Sections headed "Under the hood" explain which process owns a setting, which file stores it, and which interface changes it. You can return to those sections after you have used the desktop, or start there if you already administer Linux systems.

The book is for professionals, developers among them, who depend on their workstation and want to understand it. Desktop, security, storage, networking, and recovery chapters apply across professions. The development chapters assume work with source trees, local services, and several toolchains. Install the tools your work requires, and keep a record of changes to your workstation.

Why Fedora 45 and KDE Plasma

Fedora ships current software on a six-month cadence with a thirteen-month support window, tracks upstream closely, and is the proving ground for technology that later reaches Red Hat Enterprise Linux. Since Fedora 42, KDE Plasma has been a full Fedora edition, built, tested, and released alongside Fedora Workstation. Plasma 6.8 uses Wayland, has a scriptable compositor, KWin, and stores many settings in readable text files. *Why Fedora and KDE Plasma* explains the choice and its maintenance costs.

Choose a reading path

- For a new installation, read *Preparing Hardware and Media*, *Installing Fedora 45 KDE*, and *First Boot and Plasma Setup*. The installation walkthrough erases a whole disk. It does not demonstrate dual boot or custom partitioning.

- For daily desktop use, continue through Part II. The shortcut and configuration-file appendices are references you can keep open while working.
- Before adding repositories or changing storage, read the relevant Part III chapter and *Backup and Recovery*. Set up a backup and restore a sample file before depending on it.
- For a development workstation, use Part IV after the first update. Read the container and security boundaries before giving an AI agent access to source code, credentials, or a remote service.
- For a fault, start with *Troubleshooting*. Collect the failure and relevant logs before changing configuration.

Commands and examples

Command blocks without prompts are examples to type. In transcripts, `$` is a normal user prompt and `#` is a root prompt; do not type the prompt character. Use `sudo` for an administrative command from your normal account. Lines after a command show captured output. An ellipsis means output was omitted, not text to enter.

Examples use the fictional account Felix (`felix`) on `devbox`; account names and home paths in transcripts follow that convention. Substitute your own username, device paths, UUIDs, and network addresses where the procedure tells you to. Never copy a disk-writing command until you have identified its target. Save work before logout, reboot, or a service restart, and read the whole procedure before running its first command.

The companion `examples/` directory contains scripts and configuration files arranged by chapter. Read a sample before running it: some change your desktop, install services, or remove demonstration resources. A configuration fragment explains a setting; it is not necessarily a complete replacement for an existing file.

Coverage and limits

Screenshots and most command examples use Fedora 45 with the first updates of November 3, 2026 in a virtual machine with UEFI, Secure Boot, and TPM 2.0. Some transcripts and a few screenshots of third-party applications were recorded earlier, on the Fedora 45 Beta or the release candidate; dated output retains the package versions present when it was recorded, and a Version note says so where it matters. Software installed for a particular example is not necessarily part of a fresh Fedora installation.

The following distinctions apply throughout this edition:

- Screenshots and recorded output show observed lab behavior. A package being present does not prove that every feature or end-to-end workflow works.
- Explanations checked against upstream documentation or installed manuals describe those interfaces. They are not evidence of a physical-hardware test.
- Version and note callouts identify procedures or UI behavior that remain untested. These include physical USB writing, dual boot, multi-monitor and HDR behavior, Wi-Fi, Bluetooth devices, laptop power management, NVIDIA and ROCm acceleration, hardware security keys, and some authenticated AI-service workflows.

- A full operating-system rollback, bare-metal restore, and an upgrade to a future Fedora release are not certified by this edition. Follow the tested file-restore examples and rehearse any larger recovery on a disposable system.
- *Upgrading from Fedora 44* is the one chapter whose transcripts come from physical hardware: the author's laptop, upgraded from Fedora 44 to the Fedora 45 pre-release repositories on October 19, 2026.

Updates after November 3, 2026 can change package versions, UI labels, and behavior. If your screen differs, start with *What Changed in Fedora 45* and the local version callout.

Reporting an error

Include the book version, chapter and section title, the command or instruction, the result you expected, and the result you observed. Add your Fedora release and relevant package versions. Remove tokens, passwords, recovery keys, and private project data from logs and screenshots before sharing them. A short reproduction on a fresh account or a disposable virtual machine is more useful than a full home-directory archive.

Complete edition outline

Front

- Front matter: Colophon
- Front matter: Preface
- Front matter: Version history

Part1 Foundations

- Chapter 1: Why Fedora and KDE Plasma
- Chapter 2: Preparing Hardware and Media
- Chapter 3: Installing Fedora 45 KDE
- Chapter 4: First Boot and Plasma Setup

Part2 Plasma

- Chapter 5: A Tour of the Plasma Desktop
- Chapter 6: Windows, Virtual Desktops, and Tiling
- Chapter 7: System Settings in Depth
- Chapter 8: KRunner, Search, and Shortcuts
- Chapter 9: Dolphin, KIO, and Files
- Chapter 10: Konsole and the Terminal
- Chapter 11: Displays, Scaling, Fonts, and Color
- Chapter 12: Keyboards, Pointers, and Input Methods
- Chapter 13: Audio, Bluetooth, and Notifications
- Chapter 14: The KDE Application Set

Part3 System

- Chapter 15: Software with DNF5 and RPM
- Chapter 16: Flatpak, Flathub, and Discover
- Chapter 17: Updates, Upgrades, and Rollback
- Chapter 18: Upgrading from Fedora 44
- Chapter 19: systemd on the Desktop
- Chapter 20: The Boot Chain
- Chapter 21: Storage, Btrfs, and Encryption
- Chapter 22: Networking, VPN, and Firewall

- Chapter 23: Users, Authentication, and SELinux
- Chapter 24: Hardware, Drivers, and Power

Part4 Developer

- Chapter 25: Shell and Modern Command-Line Tools
- Chapter 26: Containers: Podman, Toolbx, Distrobox
- Chapter 27: Language Toolchains
- Chapter 28: Editors and IDEs
- Chapter 29: Git, SSH Keys, and Signing
- Chapter 30: AI Coding Agents
- Chapter 31: Local Models and GPU Compute
- Chapter 32: Virtual Machines
- Chapter 33: Remote Desktop and Multiple Devices

Part5 Under The Hood

- Chapter 34: Wayland, KWin, and Portals
- Chapter 35: Plasma Architecture: Qt, Frameworks, KConfig, D-Bus
- Chapter 36: From Login to Desktop
- Chapter 37: Troubleshooting
- Chapter 38: Backup and Recovery

Part6 Appendices

- Appendix A: Keyboard Shortcuts
- Appendix B: Where Plasma Stores Its Settings
- Appendix C: What Changed in Fedora 45
- Appendix D: Fedora and Red Hat Ecosystem
- Appendix E: Index

3 Installing Fedora 45 KDE

This chapter installs Fedora 45 KDE Plasma Desktop Edition onto a whole disk, with an encrypted system and home directory. It then explains the partitions, Btrfs subvolumes, LUKS parameters, and logs the installer creates. The EFI system partition and `/boot` remain unencrypted. The example uses a 200 GiB disk, UEFI firmware, Secure Boot, and TPM 2.0.

> **Warning:** this procedure erases the selected disk. Back up its contents, test that you can restore needed files, and disconnect unrelated external drives before starting. For dual boot, read *Preparing Hardware and Media* first; the whole-disk method below does not preserve another operating system.

3.1 Booting the live image

Fedora ships the KDE edition as a live image: the ISO boots into a complete Plasma session that runs from RAM, and the installer is an application inside that session. Write the ISO to a USB stick as described in *Preparing Hardware and Media*, boot from it, and the GRUB menu of the live image appears.

The menu has three entries:

- **Start Fedora-KDE-Desktop-Live** boots the live session directly.
- **Test this media & start Fedora-KDE-Desktop-Live** is the default. It first verifies the checksum embedded in the ISO, which takes a minute or two on a USB 3 stick. Run it once per stick; a corrupted write is a common cause of baffling installer failures.
- **Troubleshooting** opens a submenu with a basic graphics mode for hardware whose GPU driver fails in the live session.

After about ten seconds the default entry starts automatically. The live session logs in without a password as the user `liveuser` and opens the Welcome Center with a single large button.

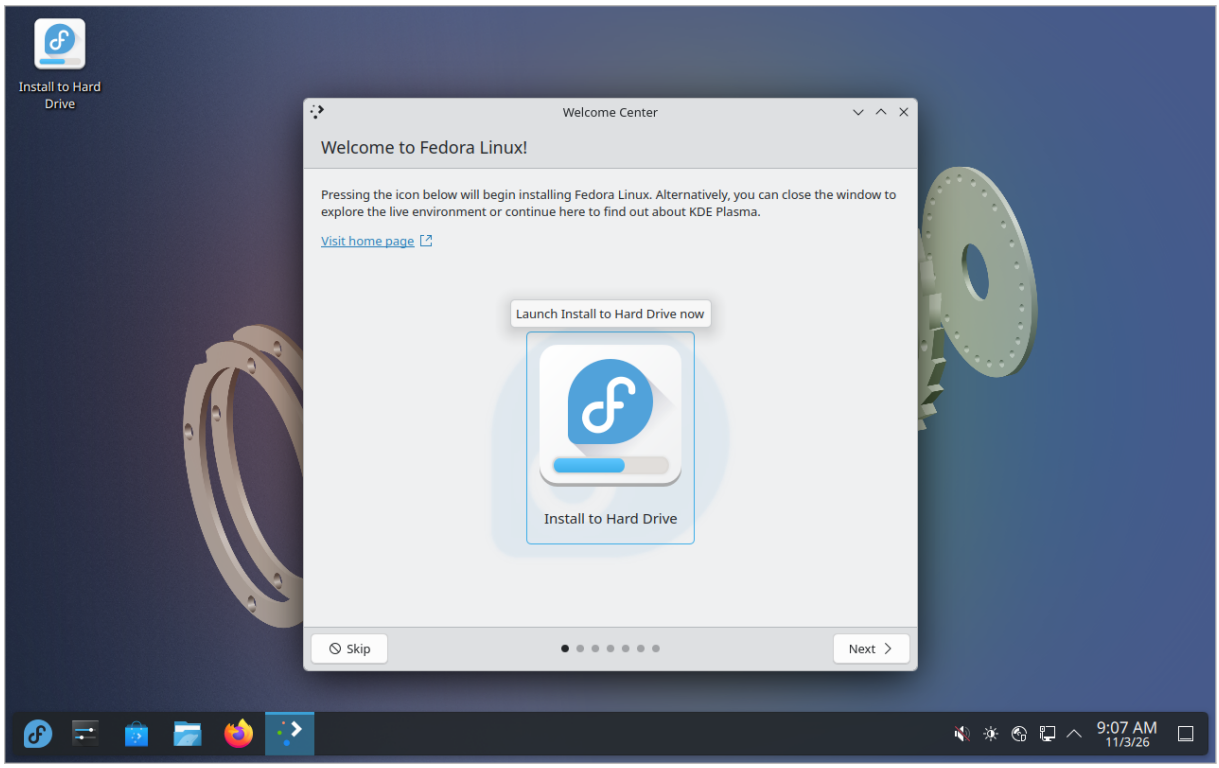


Figure 3.1: The live session greets you with the Welcome Center. Install to Hard Drive starts the installer.

The live session is a fully working Plasma desktop. Use it to check hardware before you commit: Wi-Fi in the system tray, sound from the speaker icon, external displays, the touchpad, and suspend. Repeat the tests after installation and updates, since the kernel, configuration, and power-management behavior can differ.

> **Under the hood:** the live image is a squashfs file system mounted read-only with an overlay for writes. The installer does not copy packages from a repository. It copies the live system's root file system to the target disk and then removes live-only packages and settings. That is why an offline installation of the KDE edition is complete and why it takes only a few minutes. The installer log confirms it: `packaging.log` records `Created the payload PayloadType.LIVE_OS`.

3.2 The Anaconda Web UI

Click **Install to Hard Drive**. Fedora's installer, Anaconda, opens with a browser-style interface: the Anaconda Web UI (package `anaconda-webui`, version 90 in the Fedora 45 release), which runs on Cockpit and is displayed in a dedicated web view. It is the same front end Fedora Workstation uses. The older GTK interface with its hub-and-spoke layout does not appear on this live image. Fedora's Anaconda rollout report documents the KDE transition for Fedora 43.

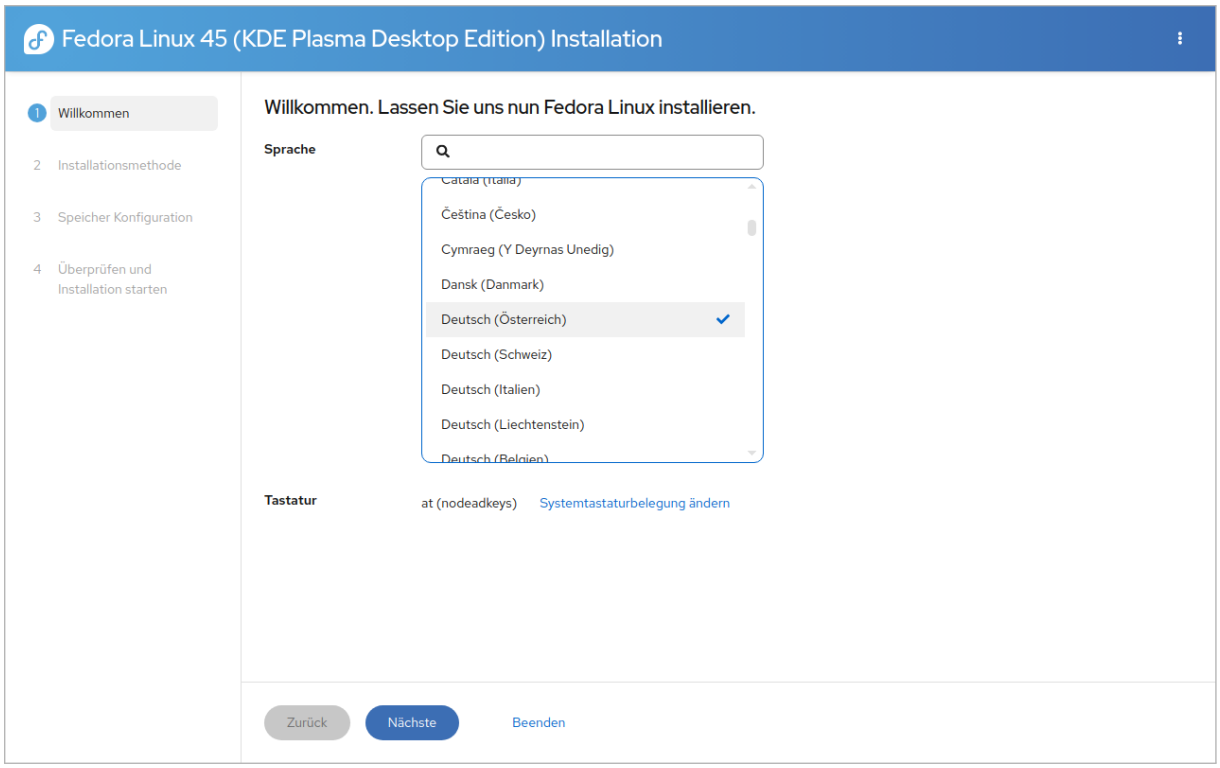


Figure 3.2: The installer opens in the language GeoIP guessed, here German (Austria).

The first page selects the language, and the installer has already guessed. It looks up the machine's public IP address and preselects the matching language and keyboard layout, here German (Austria) with the `at (nodeadkeys)` layout. The installer's own interface follows the selection immediately, so the page above is in German.

Type into the search field to filter the list. The book uses American English. After you choose **English (United States)**, the interface switches language, and the keyboard layout changes to `us` with it. If you want an English interface with a non-US keyboard, use **Change system keyboard layout** now: the layout chosen here is also the layout for the disk encryption passphrase at boot. The Fedora 45 Beta image showed a **Pre-release** badge in the header; the release image has none.

> **Warning:** the keyboard layout you install with is the layout the boot-time passphrase prompt uses. A passphrase typed on a German layout with `z` and `y` swapped will not unlock the disk on a US layout. Choose the layout you will type the passphrase on. Test that you can enter every character using that layout before committing to the installation.

3.3 Choosing the installation method

Next opens the second step, which picks the target disk and how to use it.

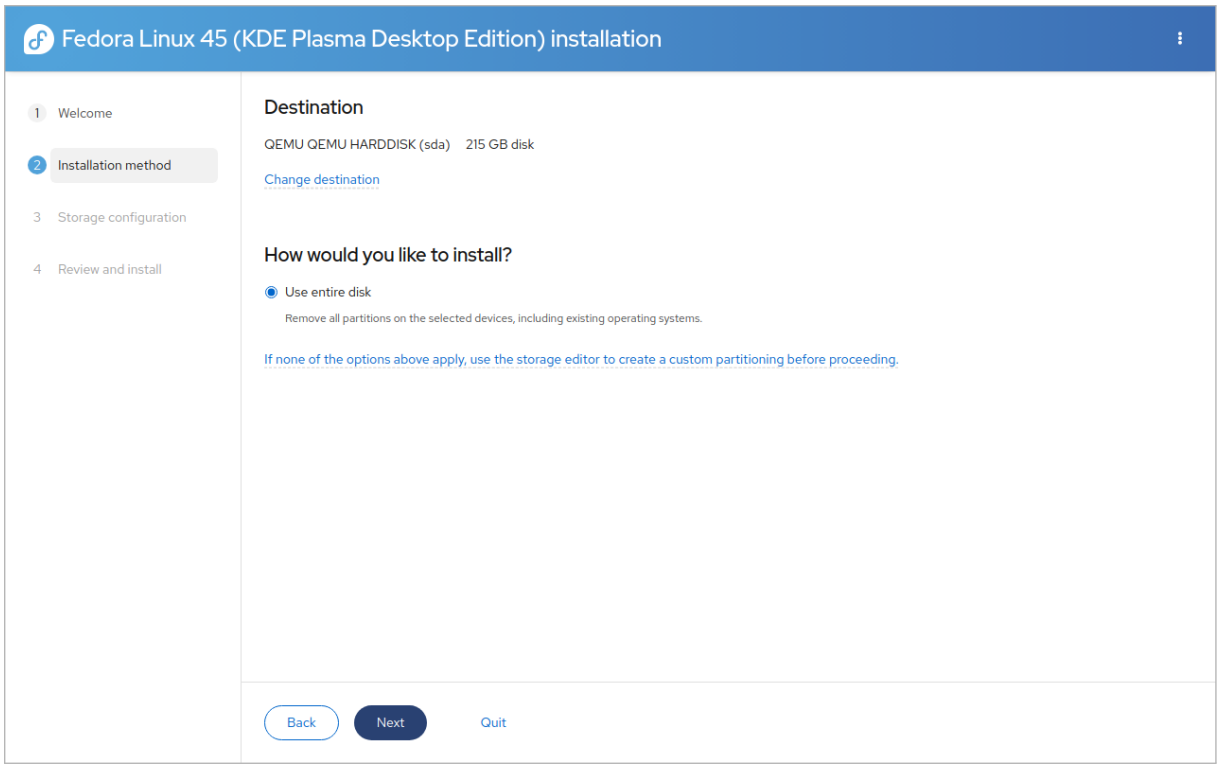


Figure 3.3: Installation method: one disk, one choice. Use entire disk erases everything on it.

On a machine with one empty disk the installer offers exactly one method, **Use entire disk**, and names the disk by model and size (here `QEMU QEMU HARDDISK (sda)`, 215 GB; the installer counts decimal gigabytes, so this is the 200 GiB virtual disk). **Change destination** selects another disk when several are present.

If the disk contains data, compare its model and size with your backup records. Other installation methods depend on the existing layout and were not tested for this edition. Stop if the screen differs in a way that makes the target unclear.

The link at the bottom, **use the storage editor to create a custom partitioning**, opens Cockpit's storage page inside the installer for manual partitioning. Manual partitioning is outside this edition's tested procedure. The automatic layout described below is the one the later storage chapters assume.

3.4 Encryption

The third step is about encryption, and it is off by default.

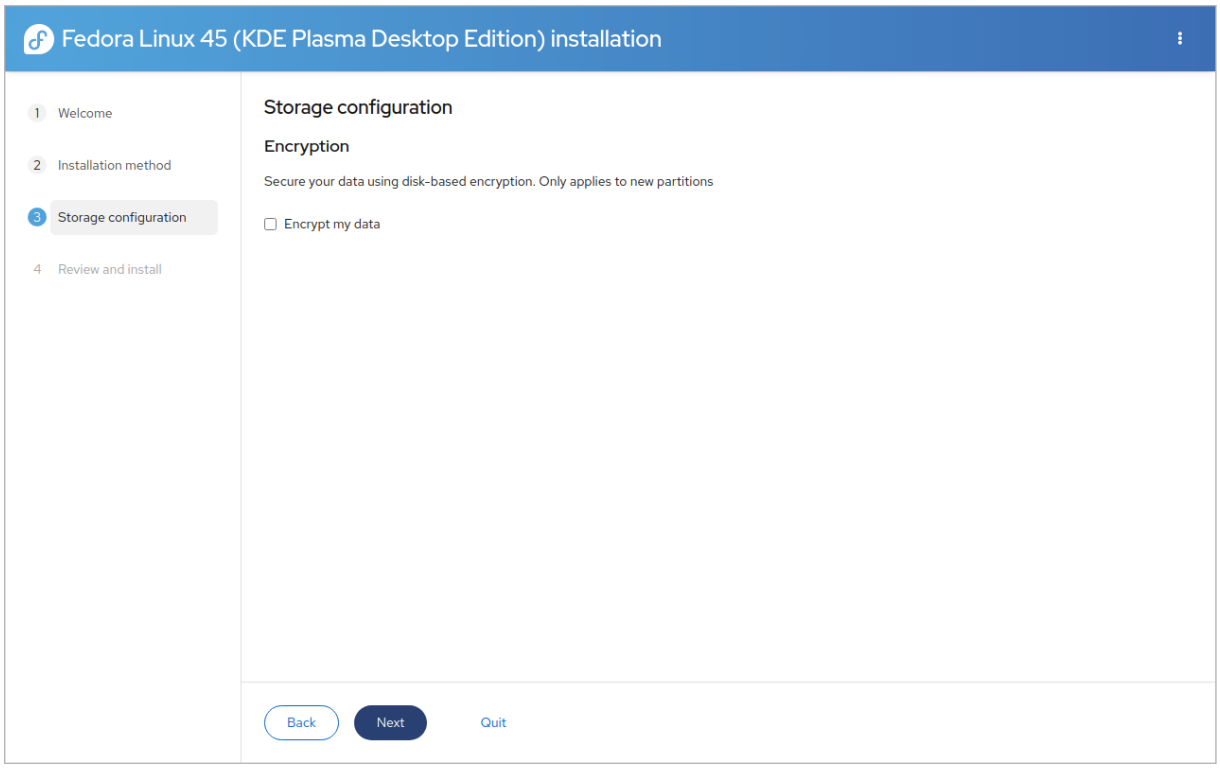


Figure 3.4: Storage configuration. Disk encryption is a single checkbox and it starts unchecked.

Turn it on. A work laptop holds private documents, saved credentials, and possibly SSH keys or confidential source code. A lost or stolen machine without disk encryption hands all of it to whoever finds it, and no login password helps, because the disk can be read from another computer. The cost is one passphrase at boot, and *Storage, Btrfs, and Encryption* explains optional TPM unlock and the security trade-offs it introduces.

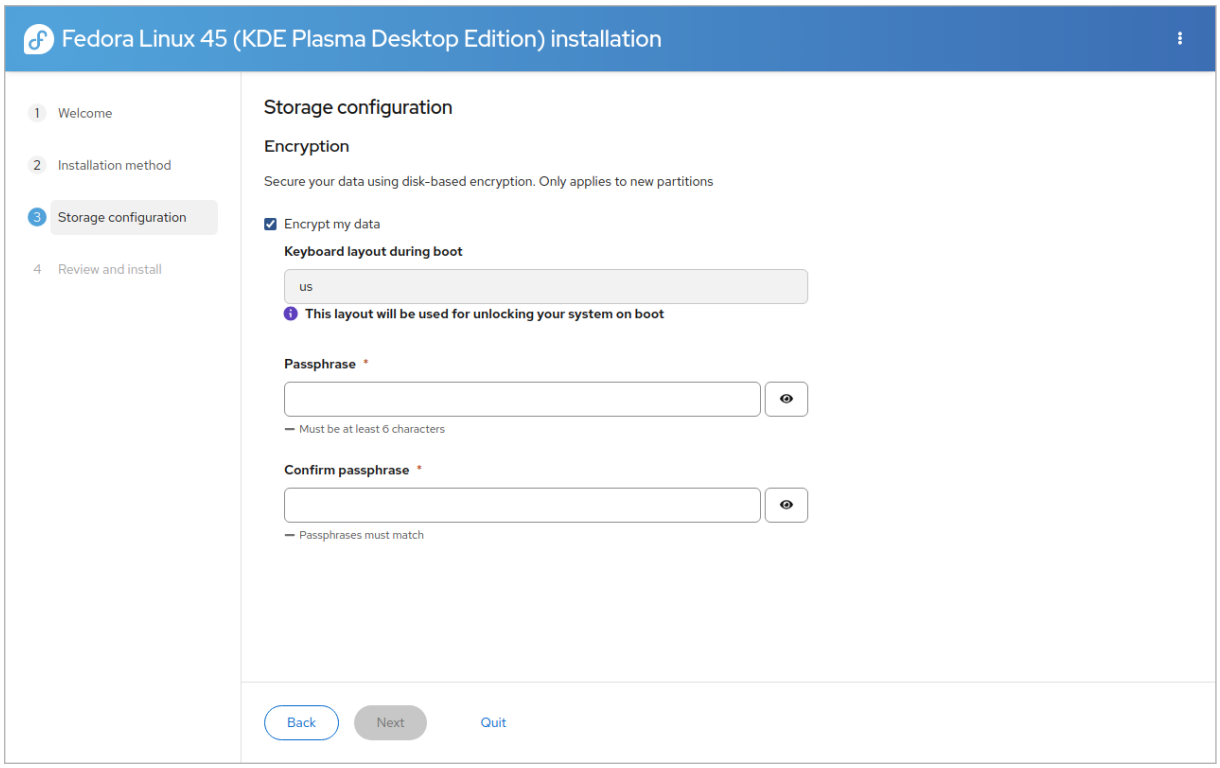


Figure 3.5: With Encrypt my data checked, the page asks for the boot keyboard layout and a passphrase.

The page now shows the keyboard layout that the boot prompt will use, read-only, and two passphrase fields. The installer accepts anything of six characters or more and rates its strength as you type. Choose a long passphrase you can type reliably with the boot keyboard layout. Use a password manager to generate and store a strong, unique value, and keep a recovery copy accessible from another device. Do not treat the installer's minimum length as a strength recommendation.

> **Note:** this passphrase protects the disk, not your user account. You set the account password later, in Plasma Setup on first boot. Use different values. Disk encryption protects data while the volume is locked; account authentication controls access to the running system. Neither substitutes for locking your desktop when you leave it.

3.5 Review and install

The last step summarizes everything and shows the partition plan.

Read the storage section carefully, because it is the only place the installer tells you what it will do to the disk:

Table 3.1: The default Fedora 45 KDE partition layout on a 200 GiB disk (sizes as the installer shows them)

Device	Size	Format	Mount point	Purpose
`sda1`	629 MB	FAT (EFI)	`/boot/efi`	EFI system partition with shim and GRUB
`sda2`	2.15 GB	ext4	`/boot`	Kernels and initramfs images, unencrypted

Device	Size	Format	Mount point	Purpose
sda3	212 GB	Btrfs in LUKS2	/	Subvolume root
sda3	212 GB	Btrfs in LUKS2	/home	Subvolume home

The hostname line says `transient, will use DHCP`. Without a static hostname the machine calls itself `fedora` or whatever name the DHCP server hands out, which changes between networks and appears in your shell prompt, in SSH known-hosts files, and in KDE Connect. Click **edit** and give the machine a name.

The example uses `devbox` as the hostname:

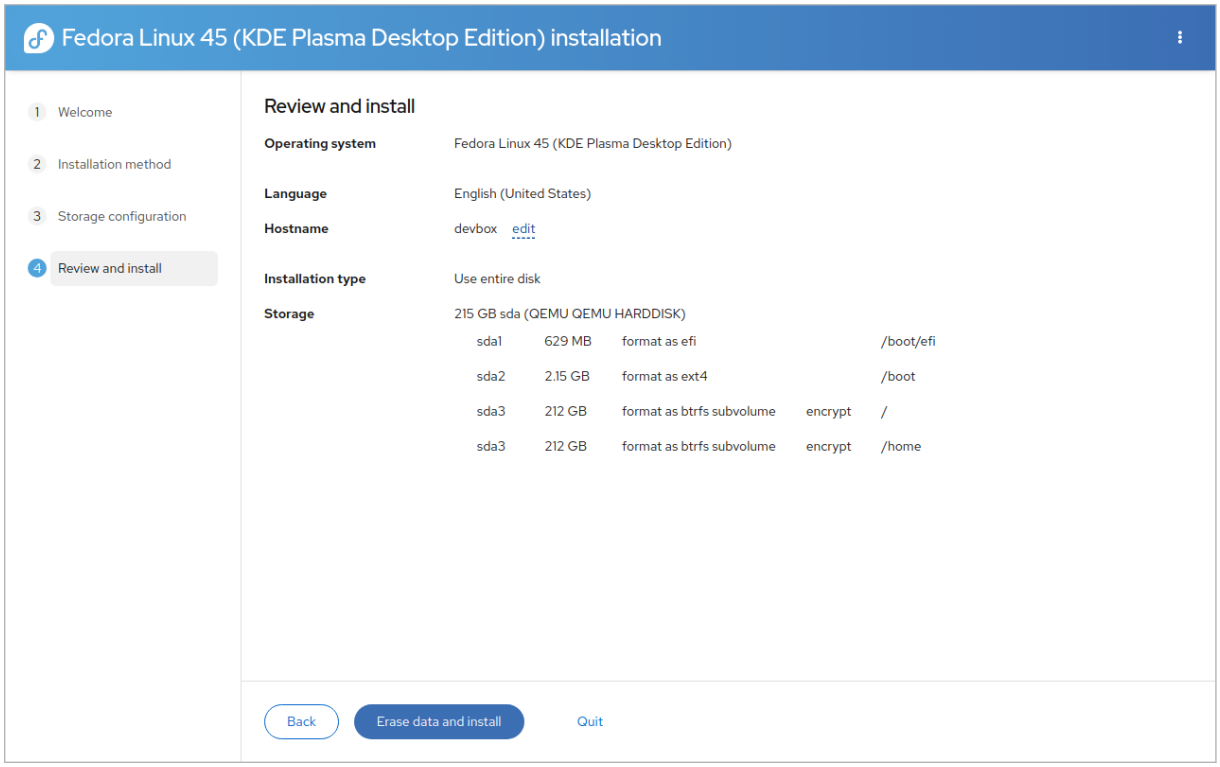


Figure 3.6: The final review with the static hostname devbox. Erase data and install starts the installation.

The live image supplies the software selection. Plasma Setup creates the first account and sets the theme and the time zone on first boot, as *First Boot and Plasma Setup* shows. Configure networking in the live session if you need it during installation.

Erase data and install is the point of no return. The progress page moves through four stages: storage configuration, software installation, system configuration, and finalization.

Most of the time goes into copying the live image. When it finishes, the installer offers to reboot or to return to the live desktop.

Click **Reboot**, then remove the USB stick when prompted or once the machine has left the live session. If it returns to the live-image boot menu, select the installed Fedora entry from the firmware's boot menu.

> **Note:** if shutdown stops at “Reached target System Reboot”, that message alone does not prove that every disk is unmounted. Allow shutdown to finish and use a forced power-off only as a last resort after installation has completed. Do not interrupt disk writes.

3.6 Under the hood: what the installer built

The rest of this chapter looks at the installed system from a terminal. You can read it now or come back after *First Boot and Plasma Setup*. All commands are read-only and show the system immediately after installation.

3.6.1 Partitions and file systems

`lsblk` shows the block-device tree, including the encrypted layer the installer table only hinted at:

```
$ lsblk -o NAME,SIZE,FSTYPE,MOUNTPOINTS
NAME                                          SIZE FSTYPE      MOUNTPOINTS
sda                                           200G
├─sda1                                        600M vfat        /boot/efi
├─sda2                                          2G ext4        /boot
└─sda3                                        197.4G crypto_LUKS
  └─luks-99415ae3-8e94-4502-a3a0-cf9c8948150e 197.4G btrfs       /home
                                                                 /
sr0                                          1024M
zram0                                           8G swap        [SWAP]
```

`lsblk` counts binary units (600 MiB, 2 GiB), the installer decimal ones (629 MB, 2.15 GB); the partitions are the same. Three things stand out:

- **`/boot` is not encrypted.** GRUB reads the kernel and the initramfs from the ext4 partition before anything can ask for a passphrase. The initramfs then unlocks `sda3`. Secure Boot verifies signed boot components, but this layout does not make every file in `/boot` authenticated. *The Boot Chain* explains the limits, including the separate initramfs.
- **One Btrfs file system holds `/` and `/home`.** They are subvolumes, not partitions, so they share the free space. There is no fixed size for the system and no “root partition full while home is empty” problem.
- **There is no swap partition.** Fedora uses `zram`, a compressed swap device in RAM. The package `zram-generator-defaults` sizes it with `zram-size = min(ram, 8192)`: as large as physical memory, at most 8 GiB. *Hardware, Drivers, and Power* explains why this is the right default, and what it means for hibernation.

3.6.2 Btrfs subvolumes and mount options

```
$ sudo btrfs subvolume list /
ID 256 gen 82 top level 5 path home
ID 257 gen 82 top level 5 path root
$ findmnt -no OPTIONS / | tr , '\n'
```

```
rw
relatime
seclabel
compress=zstd:1
ssd
discard=async
space_cache=v2
subvolid=257
subvol=/root
```

The installer writes the mount options into `/etc/fstab`. Leaving out the UUIDs and comments:

```
$ awk '!/^#/ && NF {print $2, $3, $4}' /etc/fstab
/ btrfs subvol=root,compress=zstd:1,x-systemd.device-timeout=0
/boot ext4 defaults
/boot/efi vfat umask=0077,shortname=winnt
/home btrfs subvol=home,compress=zstd:1,x-systemd.device-timeout=0
```

`compress=zstd:1` enables Btrfs's Zstandard compression at level 1 for eligible writes. Btrfs can skip incompressible data, and existing extents are not all recompressed when the mount option changes. `x-systemd.device-timeout=0` tells systemd to wait indefinitely for the device, because the device only appears after you type the passphrase. The kernel adds `ssd` and `discard=async` on its own after detecting a non-rotational disk.

3.6.3 The LUKS container

```
$ sudo awk '{print $1}' /etc/crypttab
luks-99415ae3-8e94-4502-a3a0-cf9c8948150e
$ sudo awk '{print $3, $4}' /etc/crypttab
none discard,x-initrd.attach
$ sudo cryptsetup luksDump /dev/sda3
Version:        2
...
Keyslots:
  0: luks2
        Key:        512 bits
        Priority:   normal
        Cipher:     aes-xts-plain64
        Cipher key: 512 bits
        PBKDF:      argon2id
        Time cost:  8
        Memory:     1048576
        Threads:    4
...
```

The container is LUKS2 with AES in XTS mode and a 512-bit key (two 256-bit AES keys, as XTS requires). The passphrase goes through Argon2id with 1 GiB of memory, which makes offline guessing expensive on GPUs. The first column of `crypttab` names the unlocked device, `luks-<UUID>`. The `none` in the third

column means “ask for a passphrase”; *Storage, Btrfs, and Encryption* keeps that field and adds `tpm2-device=auto` to the options in the fourth column. The `discard` option passes TRIM through the encryption layer. It exposes allocation patterns, a confidentiality trade-off that this installer enables by default. `/etc/crypttab` is readable only by root (mode 0600, as `systemd-udev` ships it), so run both `awk` commands with `sudo`.

3.6.4 Installer logs

Anaconda leaves its logs in `/var/log/anaconda/`:

```
$ ls /var/log/anaconda/
anaconda.log  dbus.log  journal.log  packaging.log  program.log  storage.log
```

`storage.log` records every decision about disks and is the first place to look when a layout is not what you expected. `program.log` lists every external command the installer ran, and `journal.log` is the system journal of the live session during installation.

3.7 Takeaways

- The KDE edition installs from a live image; the installer copies the running system, so it works offline and takes minutes.
- Anaconda’s Web UI asks only for language, target disk, encryption, and an optional hostname. User account, time zone, and theme come at first boot.
- The language and keyboard are preselected by GeoIP; the keyboard layout chosen here is also the boot-time passphrase layout.
- Encryption is off by default. The encrypted installation shown here uses LUKS2, AES-XTS-512, and Argon2id with 1 GiB memory.
- Default layout: 600 MiB EFI, 2 GiB ext4 `/boot`, and one Btrfs file system in LUKS with subvolumes `root` and `home`, compressed with `zstd:1`.
- Swap is `zram` in RAM (8 GiB in this example), not a partition.
- Set a static hostname on the review page; the default is transient and network-dependent.