

Linux Desktop User Experience

A Beginner's Roadmap to Learning Linux

This guide primarily focuses on the desktop user experience of Linux operating systems for IT beginners and hobbyists. The information discussed within this guide serves as an introduction to basic aspects of Linux operating systems. Key topics are outlined in the table of contents below.

Contents

The Emergence of Linux Operating Systems	3
Virtualization vs Direct Installation of Linux	3
Popular Linux Software Applications	4
Users and Groups via the Command Line	5
Users and Groups via Graphical Interface	6
Understanding File Management in Linux	7
Three (3) Permission Types with the ‘chmod’ command	7
Understanding File Management in Linux – Symbolic Mode	8
Understanding File Management - Linux Numeric File Permissions	10
File Compression in Linux	12
File Compression in Linux Command Line	13
Storage Management	14
Managing Disk Using the Command Line	17
How to install ClamAV Antivirus	19
Configuring Firewall for Linux	20
Configuring Samba for Linux	22
Remote Desktop Connection via SSH and VNC	23
How to Troubleshoot Networking Issues	24
Setting up a static IP address	26
Effective Backup Methods for Ubuntu	27
How to keep your computer secure in Linux	30
Customizing Linux and GNOME Tweaks	31
How to Install GNOME Tweaks	31
Customizing Settings	32
GNOME Shell Extensions	33
Extension Manager	34
Neofetch	35
Steam Gaming on Linux	37
Linux Documentation	38

The Emergence of Linux Operating Systems

Linux drew inspiration from the Unix operating system, which was developed by Ken Thompson and Dennis Ritchie at AT&T Bell Labs in the late 1960s. In 1991, Linus Torvalds started a personal project to create an open-source operating system kernel. The first version of the Linux kernel was released on September 17, 1991.

In recent year, Linux has steadily gained prominence with significantly improved desktop. While Linux does utilize command lines in Terminal, most Linux operating systems offer several software applications and system tools that feature a graphical interface (GUI). Its growing popularity stems from Linux applications in servers, cloud computing, IoT, smartphones, and personal computers. Popular Linux distributions include [Ubuntu](#), [Fedora](#), [Linux Mint](#), [Manjaro](#), and [Zorin](#). Ubuntu is often considered the best Linux distro for beginners.

Virtualization vs Direct Installation of Linux

Even though a Linux operating system can be installed directly on a laptop or desktop computer, virtual machines is an excellent way to become familiar with the Linux desktop environment. Virtualization allows one to experiment with Linux or even older versions of Windows. The virtual machine is contained separately without affecting the current (host) operating system installed on the computer. In case that the virtual machine has significant technical issues, it is possible to remove the virtual machine and create a new one in its place.

Popular virtual machines software applications are:

1. [Oracle VirtualBox](#) (Windows, Linux, and MacOS) (Free)
2. [VMware Workstation Pro](#) (Windows 10/11 or Linux versions) ([Free for personal, education, and business](#))
3. [VMware Fusion](#) (for MacOS) ([Free for personal, education, and business](#))
4. [Hyper-V](#) (Windows 10/11 Pro versions only)
5. [Parallels](#) (MacOS)

Ubuntu Desktop virtual machine using VirtualBox 7 guide can be found [here](#). Zorin OS also has a VirtualBox 7 instructions available [here](#). Each Linux distribution often provides useful documentation.

The [Ubuntu Desktop Guide](#) is the essential starting point to learn the first steps on how to become familiar with the Ubuntu desktop experience. Here one can find useful support information for Ubuntu: [Ubuntu Help](#) and [Ask Ubuntu](#) forum. Linux command line for Ubuntu beginners can be found [here](#).

[Install Ubuntu Desktop](#) step-by-step guide provide a clear path for installing Ubuntu directly on a laptop or desktop computer as the primary operating system. (**Disclaimer:** It is highly recommended to back up your data prior to installation).

Popular Linux Software Applications

Internet Browsers

Mozilla Firefox is a fast, secure and customizable browser and is the browser of choice for many Linux users. Google Chrome and Chromium are also available for download.

E-mail Clients

[Thunderbird](#) is a popular, open-source e-mail client developed by Mozilla which supports e-mail, calendar, contacts, and chat functionality. Thunderbird mail client is pre-installed on many Ubuntu distributions. Key features include customizable with add-ons, built-in junk mail filtering and phishing protection. Thunderbird also supports POP3, IMAP, and SMTP.

Office Suites

[LibreOffice](#) is very popular on many Linux distributions. LibreOffice and Microsoft 365 are two different office productivity suites, with LibreOffice being open-source software and Microsoft 365 being a cloud-based suite from Microsoft. While they are not directly integrated, you can still create and edit documents in LibreOffice and collaborate with Office 365 users. LibreOffice is an all-in-one office suite which includes word processing, spreadsheets, presentations, and more.

Media Players

[VLC Media Player](#) is a free, open-source cross-platform media player.

[Audacity](#) is a good tool for basic audio editing tasks.

Graphics and Design

[GIMP](#) is a free, open-source image editor that offers a lot of tools for manipulating images.

[Blender](#) is a comprehensive 3D modeling and animation software.

[Inkscape](#) is a powerful vector graphics editor.

Backup and Synchronization

[Deja Dup](#) is a simple backup tool for personal use.

[Rsync](#) is a powerful command-line tool for file synchronization.

Anti-Virus

[ClamAV](#) is a free and cross-platform anti-virus software for detecting various malicious viruses and removing them from computers and servers. A few key features include, on-demand scans, virus database updates, and additional command-line tools.

Text Editor

Vim is a highly configurable and powerful text editor that is especially popular with developers and system administrators.

Nano is an easy-to-use, user-friendly command-line text editor with essential editing functions and keyboard shortcuts.

Video Conferencing

Zoom a popular and powerful video conferencing solution with key features including screen sharing, virtual backgrounds, and breakout rooms.

Microsoft Teams is available for Linux users with the web client or the full desktop version.

Users and Groups via the Command Line

For Linux administrators, managing user and groups is a fundamental aspect of Linux system administration as it allows one to control access to files, directories, and system resources. This process is crucial for security and productivity. As a rule, it is recommended to create an administrator account and a separate user account. The separate user account should be the daily account.

Each user has a unique account, typically assigned a User ID (UID), which determines their permissions. Groups allow multiple users to share permissions for files and system resources. Each file in Linux has ownership by a user and a group, with read, write, and execute permissions defined for the owner, group, and others. These commands provide a solid foundation for managing users and groups in Linux.

Displays user & groups of current users

`id`

To add a new user

`sudo adduser username`

To add a new user with home directory

`sudo useradd -m username`

Change password of user

`sudo passwd username`

To add a new user with administrative privileges

`sudo usermod -aG sudo username`

To add a new group

`sudo addgroup groupname`

To add a group named “developers”

`sudo addgroup developers`

To add a User to a Group

`sudo usermod -aG groupname username`

To add a user named “username” to the “developers” group

`sudo usermod -aG developers username`

To remove user from a group

`sudo gpasswd -d username groupname`

To delete a User

`sudo userdel username`

To delete user, home directory and mail spool

`sudo userdel -r username`

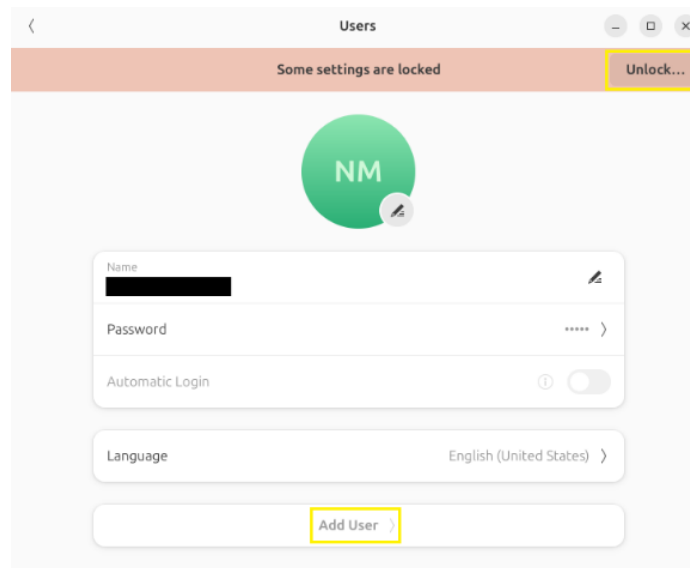
To understand User and Group IDs

`id -u username`

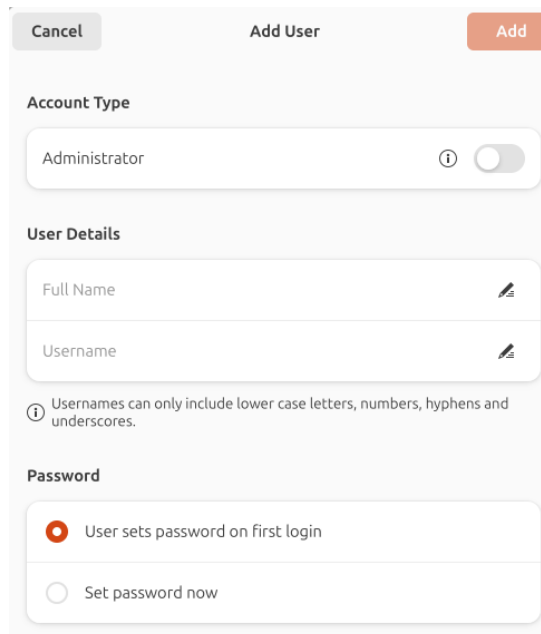
Users and Groups via Graphical Interface

The Linux command line might be daunting for beginners. Luckily, Linux desktop environments do offer a graphical user interface (GUI). Proceed to open **Settings** via the Apps and proceed to type **users** in the search bar. Click on **Users** to proceed forward.

Click **Unlock** and type in the admin password. Then, click on **Add User**. For security reasons, be sure that **Automatic Login** is turned off.



The new user account default is standard user. Only create an administrator account when deemed appropriate. It is good practice to use a standard account for daily usages and one administrator account when elevated privileges are required.



Understanding File Management in Linux

In this post, we will show how to understand basic file management in Linux for new users. **Nautilus** is the default file manager for Ubuntu's GNOME desktop environment. This graphical interface allows users to manage files and folders. However, it is highly recommended to learn how to manage file permissions via the Ubuntu terminal. Linux Permissions are simpler than Windows Active Directory.

The '**chmod**' is a command-line utility used to change permissions of files or directories in Linux, including Ubuntu!! This guide will solely focus on the '**chmod**' command.

Three (3) Permission Types with the 'chmod' command

There are 3 permission types that apply to 3 groups. The permissions are Read, Write and Execute which can be applied to the file/folder Owner, the Group Owner and Everyone.

Permissions for files

Read – Can view or copy file contents.

Write – Can modify file content.

Execute – Can run the file (if its executable).

Permissions for directories

Read – Can list all files and copy the files from directory.

Write – Can add or delete files into directory (needs execute permission as well).

Execute – Can enter the directory.

How To Read File Permissions

rwXrW-r--

This string refers to the permissions on a file/folder with three different sets of permissions.

- **rwX** Permissions for User Owner
- **rw-** Permissions for Group Owner
- **r--** Permissions for Others

r = read
w = write
x = execute
- = No Permissions Set

Setting Up File Permissions

Setting up file permissions in Ubuntu can be done using the '**chmod**' command. For file permissions in Linux, every file and directory have the following three permissions for all the three kinds of owners.

Understanding File Management in Linux – Symbolic Mode

Symbolic permissions in Linux are a way to change file permissions using symbols rather than numeric values. The symbolic notation consists of three parts:

1. **Who:** Specifies whose permissions are being modified. This can be represented by one or more of the following characters:
 - **'u':** User/Owner
 - **'g':** Group
 - **'o':** Others (everyone else)
 - **'a':** All (equivalent to 'ugo')
2. **Operator:** Specifies how the permissions are being modified. This can be one of the following characters:
 - **+:** Adds the specified permissions.
 - **-:** Removes the specified permissions.
 - **=:** Sets the permissions to exactly what is specified, overriding existing permissions.
3. **Permissions:** Specifies the permissions being added, removed, or set. These are represented by one or more of the following characters:
 - **r:** Read permission.
 - **w:** Write permission.
 - **x:** Execute permission.

Additionally, there are a few more symbols that can be used:

X: Execute only if the file is a directory or already has execute permission for some user

s: Set user or group ID (setuid/setgid)

t: Sticky bit

Symbolic File Management Examples

1. Add Permissions

To add execute permission for the user (owner) of a file.

chmod u+x file.txt

To add read and execute permissions for the group.

chmod g+rx file.txt

To add write permission for others.

chmod u+w file.txt

2. Remove Permission

To remove write permission for the user.

```
chmod u-w file.txt
```

To remove read and execute permissions for the group

```
chmod g-rx file.txt
```

To remove all permissions for others

```
chmod o-rwx file.txt
```

3. Set Specific Permissions

To set read, write, and execute permission for the users, and only read and execute permissions for the group or others.

```
chmod u-rwx, g-rx, o=rx file.txt
```

4. Apply Changes Recursively

To add execute permissions for the user and group recursively to all files in a directory.

```
chmod -R ug+x directory
```

5. Additional Examples

Add read and write permissions for the user.

```
chmod u+rw file.txt
```

Remove execute permission for the group.

```
chmod g-x file.txt
```

Set read and execute permissions for others, removing any other permissions.

```
chmod o=rx file.txt
```

Add execute permission only if the file is a directory or already has execute permission for some user:

```
chmod a+X directory
```

Understanding File Management - Linux Numeric File Permissions

Check Current Permissions

Before changing permissions, you can check the current permissions of a file or directory using **'ls -l'**

ls -l file.txt

The numeric file permissions in Linux are represented by a three-digit number, where each digit corresponds to a different set of permissions: owner, group, and other. Each permission is represented by a numeric value. To set permissions, one adds these faults together.

- Read (r) = 4
- Write (w) = 2
- Execute (x) = 1

Read allows the ability to read.

Write allows to modify, rename, and delete.

Executable allows script execution.

Simply add numbers together to get cumulative permissions.

Linux File Permissions		
Octal	String Representation	Permissions
0 (0 + 0 + 0)	---	No Permission
1 (0 + 0 + 1)	--x	Execute
2 (0 + 2 + 0)	-w-	Write
3 (0 + 2 + 1)	-wx	Write + Execute
4 (4 + 0 + 0)	r--	read
5 (4 + 0 + 1)	r-x	Read + Execute
6 (4 + 2 + 0)	rw-	Read + Write
7 (4 + 2 + 1)	rwX	Read + Write + Execute

Here is a quick reference on the Linux Numeric File Permissions.

777 = Owner, Members of Group Owner, Everyone have Full Control.

764 = Owner has Full Control, Group has Read and Write, Everyone has Read.

755 = Owner has full control, Group has read and write, Everyone has read permissions.

744 = Owner has full control, Group and Everyone has read permissions.

740 = Owner has Full Control, Group can Read, Everyone can do nothing.

Understanding File Management in Linux – Linux Numeric File Permissions

Numeric File Management Example 1

For example, to give read, write, and execute permissions to the owner, and only read permission to the group and others, you would use the octal number 744:

chmod 744 file.txt

This chmod command sets the permissions of file.txt to -rwxr--r--, where the first 7 is for the owner, the second 4 is for the group, and the third 4 is for others.

Numeric File Management Example 2

The command chmod 755 gives the owner full permissions (rwx) and read/execute permissions to the group and others (r-x). It sets the file permissions of a file to rwxr-xr-x.

chmod 755 file.txt

The first digit (7) gives the owner of the file (rwx).

The second digit (5) gives the group (r-x).

The third digit (5) gives others (r-x).

Numeric File Management Example 3

chmod -R 777 folder – Changes permissions of Folder and Contents so that Account Owner can RWX, Group Owner can RWX, and Everyone can RWX

Recursive Command for file permissions.

-R is for recursive which means the contents of the folder will be changed also

Changing Ownership

To Change User Ownership = sudo chown -R username file/folder

To Change Group Ownership =sudo chgrp --R groupname file/folder

-R for Recursive for Folders

File Compression in Linux

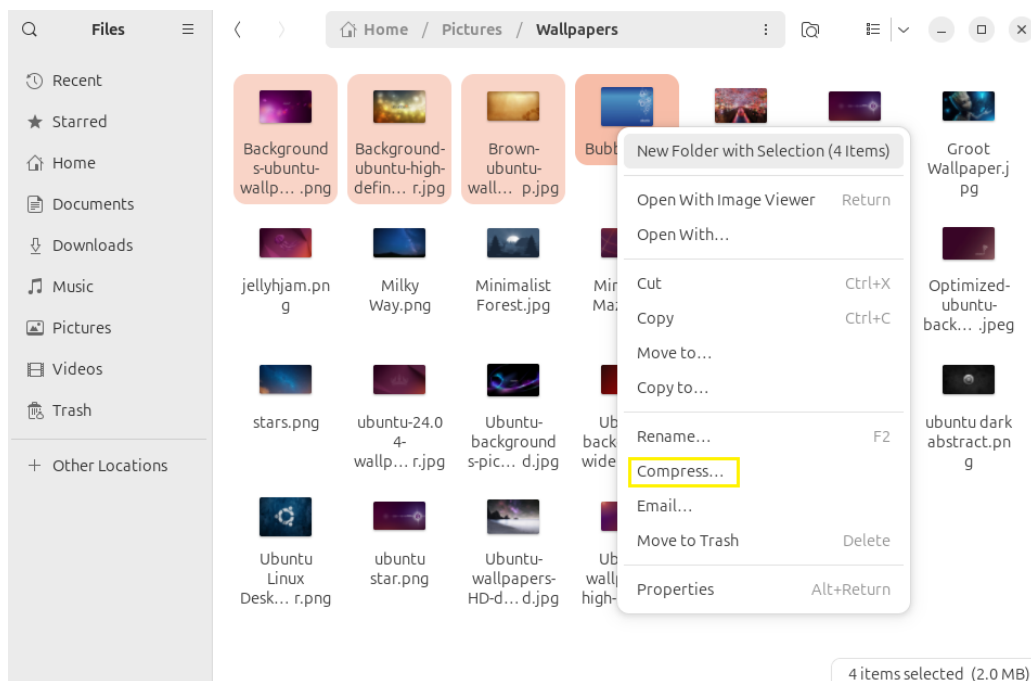
File Compression is an essential tool in Ubuntu for reducing file sizes and bundling multiple files together. Files can be compressed in a variety of formats. Compressing files reduces their size by encoding data more efficiently by:

- Saving disk space
- Reducing bandwidth when sending files over the internet
- Minimizing the time needed for backups or file transfers.

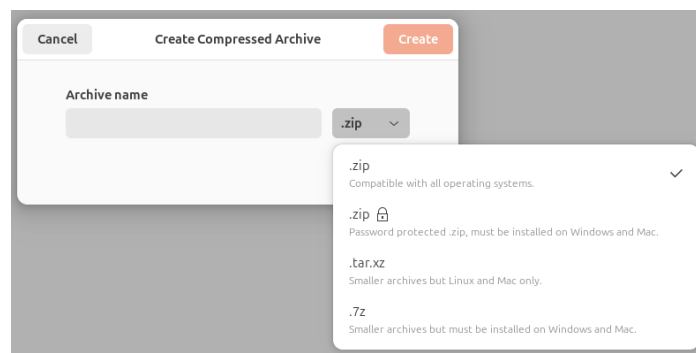
Ubuntu supports various compression formats, including ZIP, TAR.GZ, and TARBZ2. Each compression format offers unique features and use cases.

Basic Archives

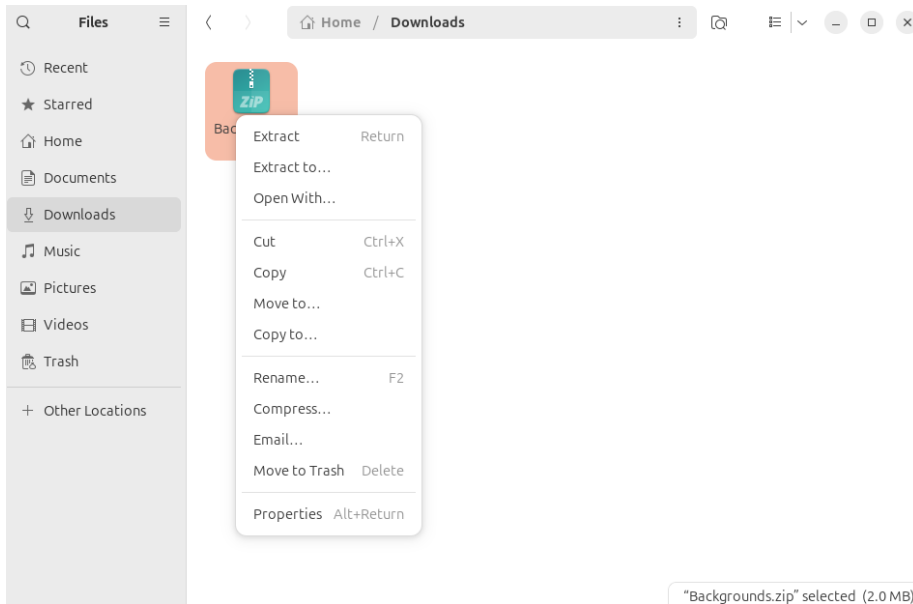
Within the Archive Manager, you can see the folders on the left pane. Here, under the /Home/Pictures/Wallpapers, select a few files and click on the right-click. Select **compress**.



Proceed to name the archive name. The default is **.zip**



In the case scenario, the zip file was named **Backgrounds.zip** Right-click on the zip file and select **Extract** or **Extract to** (a folder).



File Compression in Linux Command Line

Prior to installing software in Linux, proceed to update the operating system in Terminal:

sudo apt-get update

Install **zip** and **unzip** with the following bash terminal commands:

sudo apt-get install zip unzip

Creating a zip archive

zip archive_name.zip file1.txt file2.txt

This creates archive_name.zip containing file1.txt and file2.txt

Compressing an entire directory

Zip -r archive_name.zip directory_name

The -r flag recursively adds all files and subdirectories from directory_name into the zip archive.

Unzipping files. To extract file from a .zip archive

Unzip archive_name.zip

Each compression method has its advantages, with ZIP offering broad compatibility. TAR.GZ providing a balance between speed and compression. TAR. BZ2 achieving higher compression ratios. More information, visit Ubuntu's [file compression](#) section.

Storage Management

Managing disks in Ubuntu is essential for optimizing storage, organizing data, and ensuring efficient system performance. Ubuntu provides both a graphical user interface (GUI) and command-line tools for disk management. In this guide, we'll cover how to manage disks using the Disks GUI application and commands for mounting and unmounting disks in the terminal.

Managing Disks Using the GUI (Disks Application)

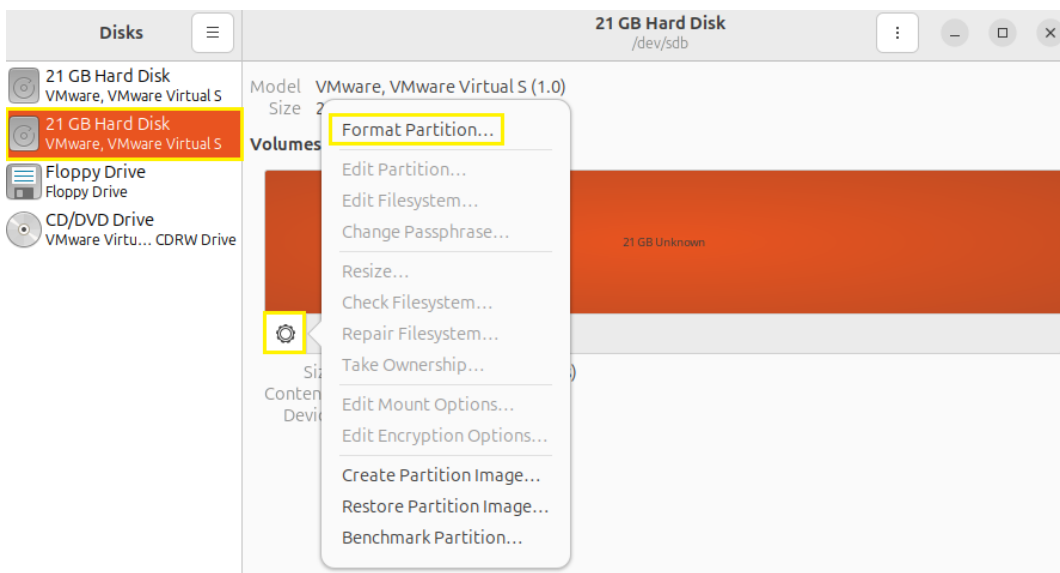
Ubuntu comes with a built-in **Disks** utility that provides a user-friendly interface for managing storage devices. You can use it to view partitions, format drives, mount and unmount disks, and create disk images.

Opening the Disks Application

1. Open the **Activities** menu and search for **Disks**.
2. Click on **Disks** to launch the application.
3. The left panel lists all available storage devices, including internal hard drives, SSDs, USB drives, and external storage devices.



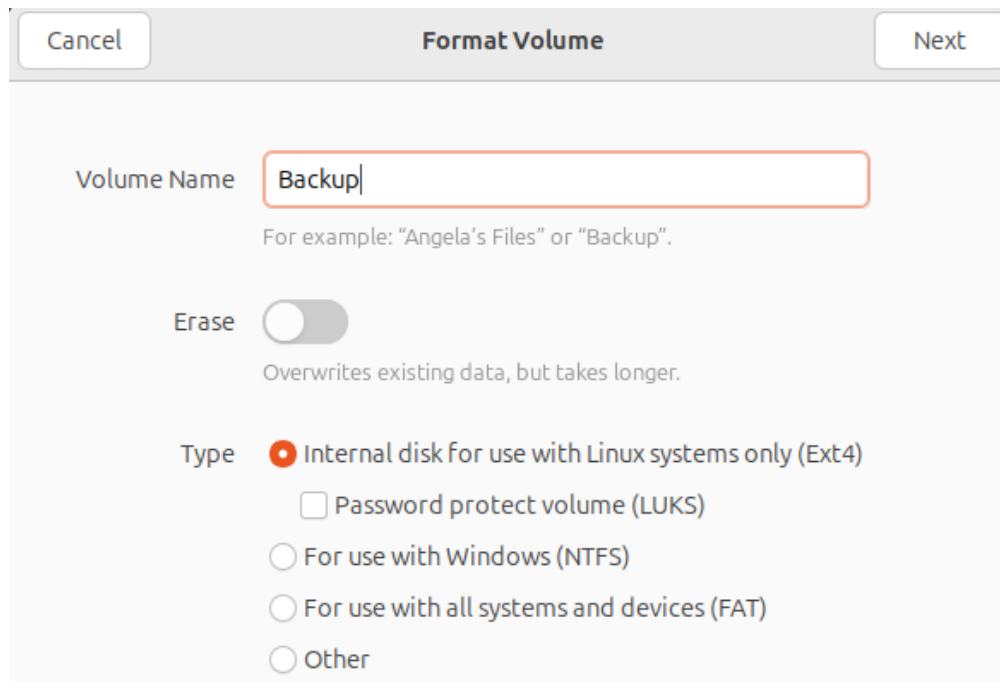
In this case scenario, a new hard disk was added. Select the gear icon and proceed to select **Format Partition**.



Formatting a Drive Using Disks

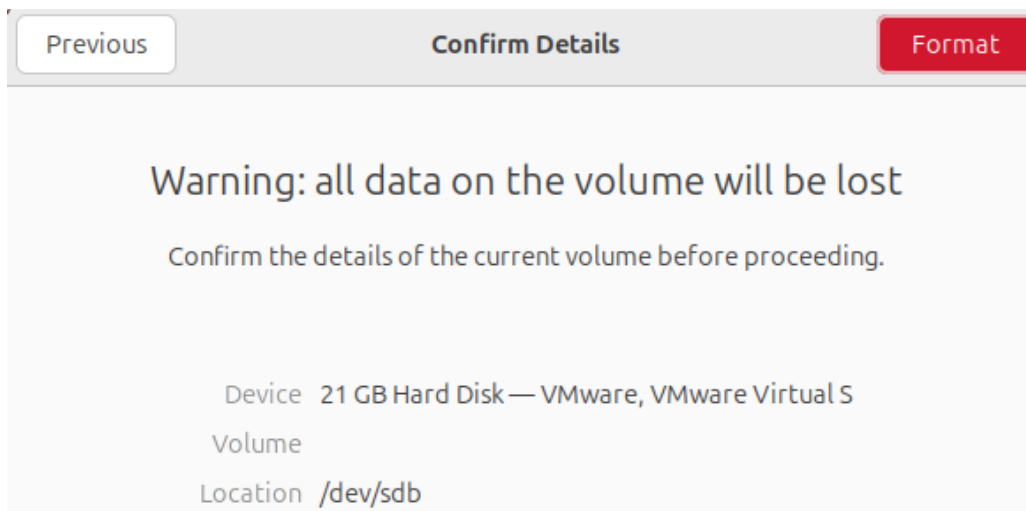
1. Select the disk and click the **gear icon** (⚙).
2. Choose **Format Partition**.
3. Select a filesystem (e.g., **ext4**, **NTFS**, **FAT32**) and confirm the format operation.

Proceed to assign a volume name. Here is **Backup** volume name is begin created. The default internal disk is **Ext4**.



The 'Format Volume' dialog box has a title bar with 'Cancel' and 'Next' buttons. The 'Volume Name' field contains 'Backup' with a hint 'For example: "Angela's Files" or "Backup"'. The 'Erase' toggle is off with the hint 'Overwrites existing data, but takes longer.'. The 'Type' section has four radio buttons: 'Internal disk for use with Linux systems only (Ext4)' (selected), 'Password protect volume (LUKS)', 'For use with Windows (NTFS)', and 'For use with all systems and devices (FAT)'. There is also an 'Other' option.

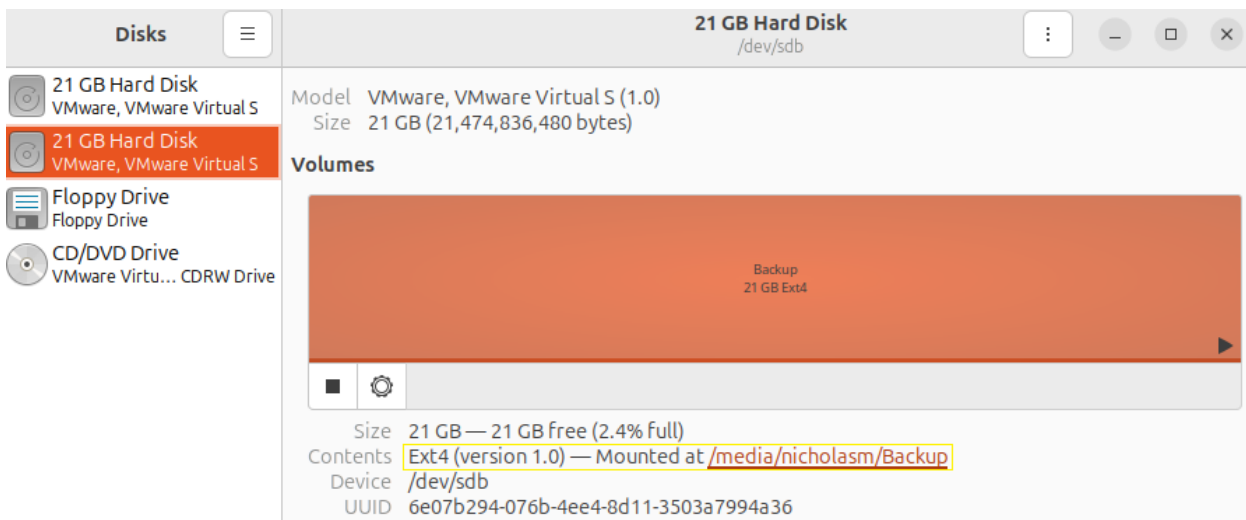
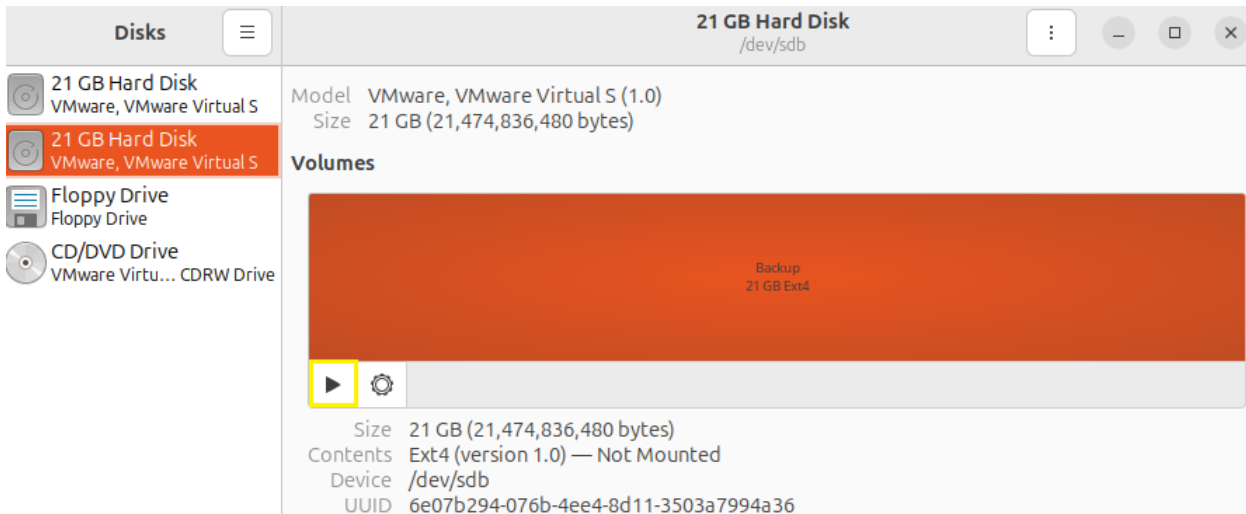
Click on Format. You will be prompted to enter admin password.



The 'Confirm Details' dialog box has a title bar with 'Previous' and 'Format' buttons. It displays a warning: 'Warning: all data on the volume will be lost' with the instruction 'Confirm the details of the current volume before proceeding.'. Below, it shows the volume details: 'Device 21 GB Hard Disk — VMware, VMware Virtual S', 'Volume', and 'Location /dev/sdb'.

Mounting a Disk Using Disks

1. Select the disk or partition from the list.
2. Click the **Play** button (▶) to mount the partition.
3. The mounted drive will appear in the **File Manager** under **Other Locations**.



Unmounting a Disk Using Disks

1. Select the mounted partition.
2. Click the **Stop** button (■) to unmount the partition.
3. The disk is now unmounted and cannot be accessed until remounted.

Managing Disk Using the Command Line

For users who prefer the command line, Ubuntu provides various commands to mount, unmount, and manage disks efficiently.

Listing Available Disks and Partitions

To view available disks and partitions, run in Terminal

lsblk

This command displays block devices in a tree structure, showing their mount points. To get detailed information, use:

sudo fdisk -l

Mounting a Disk Using the Terminal

1. Identify the disk partition you want to mount:

sudo lsblk -f

2. Create a mount point (if it doesn't exist):

sudo mkdir -p /mnt/mydisk

3. Mount the disk:

sudo mount /dev/sdXn /mnt/mydisk

Replace **sdXn** with your partition name (e.g., **sdb1**).

4. Verify the mount:

df -h

The partition should appear in the list.

Unmounting a Disk Using the Terminal

To unmount a disk, use either one of the following commands.

sudo umount /mnt/mydisk

sudo umount /dev/sdXn

Ensure the disk is not in use, or the unmount command will fail. If needed, you can force unmount with:

sudo umount -l /mnt/mydisk

Automatically Mount a Disk at Boot (Persistent Mounting)

1. Find the UUID of the disk:

```
sudo blkid
```

2. Open the **fstab** file for editing:

```
sudo nano /etc/fstab
```

3. Add an entry like this (modify according to your disk's UUID and desired mount point):

```
UUID=your-disk-uuid /mnt/mydisk ext4 defaults 0 2
```

4. Save the file (Ctrl + X, then Y, then Enter) and apply changes:

```
sudo mount -a
```

Backup and Recovery

For Backup and Recovery of files, consider tools like, **Timeshift** or **Deja Dup** for scheduled backups. For efficient backups in the command line, consider using the **rsync** command-line, such as:

```
rsync -av --progress /source /destination
```

RAID Configuration

Redundant Array of Independent Disks (RAID) ensures data redundancy and performance. In the terminal, proceed to install mdadm:

```
sudo apt install mdadm
```

Proceed to create a RAID array:

```
sudo mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sdX /dev/sdY
```

Monitor RAID arrays using **cat /proc/mdstat**.

For more information about RAID, check out my post [Explaining RAID](#). Ubuntu offers additional information regarding software RAID which can be found [here](#).

Disk management in Ubuntu can be done easily using both the **Disks** GUI application and the command line. While the **Disks** utility provides a simple way to manage storage visually, the terminal offers powerful options for advanced users. Whether you need to mount, unmount, format, or set up automatic mounting, Ubuntu provides the flexibility to handle your disks efficiently.

How to install ClamAV Antivirus

[ClamAV](#) is an antivirus software designed to detect trojans, viruses, malware, and other malicious threats.

1. Update Package List via Terminal

sudo apt update && sudo apt upgrade

2. Install ClamAV mfor manual scans using command-line tools

sudo apt install clamav

3. Install ClamAV's dameon for real0time scanning with a background service.

sudo apt install clamav-daemon

During the installation process, you might be prompted to configure 'clamd' to boot on start.

4. Update ClamAV's Virus Definitions.

sudo freshclam

5. Configure Automatic Updates (Optional):

It might be more convenient to setup automatic updates for ClamAV's virus database. Proceed to edit the 'Freshclam' configuration file.

sudo nano /etc/clamav/freshclam.conf

Proceed to find the line that says '# Comment or remove the line below.' And uncomment (remove the '#' symbol) from the line:

**# Comment or remove the line below.
DatabaseMirror database.clamav.net**

Save the file and exit.

6. Start the ClamAV Daemon (clamd)

sudo systemctl start clamav-daemon

7. Enable ClamAV Daemon to Start on Boot (Optional):

sudo systemctl enable clamav-daemon

You can scan files, directories, or your entire system using the 'clamscan' command. For example,

clamscan -r /path/to/scan

Make sure to replace '/path/to/scan' with the actual path you want to scan.

Configuring Firewall for Linux

This post is a part of a series of short, practical guides for beginners to Linux operating systems, especially Ubuntu. In this post, we will discuss the benefits of a firewall and subsequently, the setup guide. Setting of a firewall for Ubuntu lies in three primary reasons:

1. **Security:** A firewall safeguards your device controlling incoming and outgoing network traffic based on predetermined security rules.
2. **Access Control:** It allows you to specify which services or applications can be access from outside your network. This process will reduce the risk of unauthorized access.
3. **Network Segmentation:** Firewalls can help segment your network and limit the potential threat of malware or attackers within your network.

Steps to Set Up UFW in Ubuntu

The **Uncomplicated Firewall (UFW)** is a simple firewall application that is included with Ubuntu and can be installed on other distributions of Linux. By default, UFW is disabled.

In order to see the status of UFW, open Terminal and type in the following command line: **sudo ufw status**

```
~$ sudo ufw status
[sudo] password for ~:
Status: inactive
~$
```

To enable UFW, enter the following command: **sudo ufw enable**

```
~$ sudo ufw enable
Firewall is active and enabled on system startup
~$ sudo ufw status
Status: active
~$
```

By default, ALL incoming traffic is blocked. Here are a few command lines to allow UFW. Proceed to allow for SSH, HTTP and HTTPS.

sudo ufw allow 22	Allow 22 for SSH
sudo ufw allow 80	Allow 80 for HTTP
sudo ufw allow 443	Allow 443 for HTTPS
ufw default allow	Allow all connections by default
ufw default deny	Drop all connections by default
ufw allow port	Allow traffic on port
ufw deny port	Block port
ufw deny from ip	Block ip address
sudo ufw allow <app_name>	To allow application profiles
sudo ufw allow samba	Allows samba

Configuring Samba for Linux

To find out the status of the UFW, type in the following command line: **sudo ufw status**

```
root@ubuntu:~$ sudo ufw status
Status: active

To Action From
--
22 ALLOW Anywhere
80 ALLOW Anywhere
443 ALLOW Anywhere
22 (v6) ALLOW Anywhere (v6)
80 (v6) ALLOW Anywhere (v6)
443 (v6) ALLOW Anywhere (v6)
```

sudo ufw status verbose – Shows all Rules currently configured for ufw

```
root@ubuntu:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22 ALLOW IN Anywhere
80 ALLOW IN Anywhere
443 ALLOW IN Anywhere
22 (v6) ALLOW IN Anywhere (v6)
80 (v6) ALLOW IN Anywhere (v6)
443 (v6) ALLOW IN Anywhere (v6)
```

Additional useful UFW commands

sudo ufw status numbered – Shows rules in numbered order so that you can delete specific rules.

sudo ufw delete 1 – Deletes rule based on number.

sudo ufw disable – Disables ufw

sudo ufw reset – Deletes all rules and disables ufw

The default firewall configuration tool for Ubuntu is ufw. Developed to ease iptables firewall configuration, ufw provides a user-friendly way to create an IPv4 or IPv6 host-based firewall. By default, UFW is disabled. **Gufw** is a GUI that is available as a frontend.

Configuring Samba for Linux

A Samba file server provides seamless file sharing across different operating system platforms over a network. This beginner guide will cover the setup of Samba on Ubuntu. Ubuntu does offer an excellent [installation and configuration guide for samba](#).

Step 1: To install Samba, run the following command in Terminal.

```
sudo apt update
sudo apt-get install samba
```

To verify that the installation of Samba was successful, type in this command in Terminal.

```
whereis samba
```

The output show show as follows:

```
samba: /usr/sbin/samba /usr/lib/samba /etc/samba /usr/share/samba
      /usr/share/man/man7/samba.7.gz /usr/share/man/man8/samba.8.gz
```

Step 2: Setting up Samba.

It is now necessary to create a directory to share now that Samba has been successfully installed. This command line below creates a new folder **sambashare** in our home directory which we will share later.

```
mkdir /home/<username>/sambashare/
```

The configuration file for Samba is located at **/etc/samba/smb.conf**. To add the new directory as a share, proceed to edit the file by executing the following command line.

```
sudo nano /etc/samba/smb.conf
```

At the bottom of the file, add the following lines:

```
[sambashare]
comment = Samba on Ubuntu
path = /home/username/sambashare
read only = no
browsable = yes
```

To save the file, press **Ctrl-O** and **Ctrl-X** to exit from the nano text editor.

The **comment** section adds a brief description of the Samba share.

The **path** is the directory of the shared folder.

The **read only** permission allow one to modify the contents of the share folder is only granted when the value of this directive is no.

Here are the steps to use [Samba as file server](#).

Configuring Samba for Linux

The **browsable** section is set to yes so that file managers, such as Ubuntu's default file manager, will list this share under "Network" (it could also appear as **browsable**).

For the new shared configuration to take effect, proceed to save it and restart Samba for it to take effect with the following command line.

```
sudo service smb restart
```

Proceed to update the firewall rules to allow Samba traffic:

```
sudo ufw allow samba
```

Step 3: Setting up User Accounts and Connecting to Share

Since Samba doesn't use the system account password, we need to set up a Samba password for our user account:

```
sudo smbpasswd -a username
```

Special note: The username used must belong to a system account. Otherwise, it will not save.

Connecting to Share

A quick way to find your IP address in Ubuntu is using the **ip a** command in Ubuntu's terminal.

On Ubuntu: Open up the default file manager and click Connect to Server then enter: **ubuntuctn**

On macOS: In the Finder menu, click Go > Connect to Server then enter: **macosctn**

On Windows, open up File Manager and edit the file path to:

```
\\ip-address\sambashare
```

Note: **ip-address** is the Samba server IP address and **sambashare** is the name of the share.

As a final step, you will be prompted to enter your credentials to proceed to connect to the Samba folder.

Remote Desktop Connection via SSH and VNC

The **SSH** command establishes a secure, encrypted connection between two hosts across an unsecure network. It allows terminal access, file transfers, and application tunneling. Additionally, graphical X11 applications can be run securely over SSH from a remote location. For more details, check out [SSH Ubuntu](#) and [OpenSSH](#)

Virtual Network Computing (VNC) is a protocol widely utilized for sharing graphical desktops over a network. It is commonly employed for technical support and screen sharing purposes. Ubuntu has a guide on how to [access a remote desktop](#). Ubuntu community help wiki has a detail section on [VNC](#).

How to Troubleshoot Networking Issues

Resolving network connectivity issues can be a challenge in Linux. This guide focuses on how to resolve network issues in Ubuntu.

1. **Check network connections:** Ensure that your network cables are securely connected and that your wireless network adapter is turned on if you're using Wi-Fi.
2. **Restart networking service:** Open Terminal and type in the following code:

```
sudo systemctl restart networking
```

In case that '**sudo systemctl restart networking**' is not working, the error might be due to the '**networking**' service is not managed by system in your Ubuntu version. Proceed to use the following command line in Terminal.

```
sudo systemctl restart system-networkd
```

3. **Restart network manager:** If you are using NetworkManager, you can restart it using the following command:

```
sudo systemctl restart NetworkManager
```

4. **Check network settings:** Verify that your network settings (IP address, subnet mask, gateway, DNS servers) are configured correctly. You can do this by checking the network configuration files in **/etc/network/interfaces** or **/etc/netplan**.
5. **Check firewall settings:** Ensure that your firewall settings are not blocking the network traffic. A latter reference guide will be focusing on UFW (uncomplicated) firewalls. You can check the status of the firewall using the following command:

```
sudo ufw status
```

6. **Check for network interface:** Verify that your network interface is recognized by Ubuntu using the following command:

```
ip -a
```

Please note that the latest versions of Ubuntu may not use '**ifconfig -a**' command and would use the '**ip a**' command instead.

This will display detailed information about your network interfaces, including IP addresses, MAC addresses, and more. If you specifically need to see only the IP addresses, you can use:

```
ip a show | grep inet
```


IP route show

The **ip route show** command in Linux is used to display the routing table of the system. It shows the currently configured routes, including the destination network or host, the gateway (if any) used to reach that destination, and the network interface through which the traffic will be routed. This command is useful for troubleshooting network connectivity issues and understanding how network traffic is being routed on the system.

7. Use the **Ping** command in Terminal. For example, ping google website or another device in your network.

```
ping 8.8.8.8
ping google.com
```

8. In Linux, **dhclient** is a DHCP (Dynamic Host Configuration Protocol) client used to obtain an IP address and other network confirmation settings from a DHCP server. Here are a few common commands.

1. **Renew DHCP Lease:** Forces the client to renew its DHCP lease.

```
sudo dhclient -r    # Release current lease
sudo dhclient        # Request new lease
```

2. **Release DHCP Lease:** Releases the current DHCP lease

```
sudo dhclient -r
```

3. **Specify Interface:** Specify the network interface to use (eg. **eth0**, **wlan0**)

```
sudo dhclient etho
```

9. **Testing Latency, Download, and Upload speeds**

The **speedtest-cli** command will test your Internet connect to the nearest speedtest.net server and display the latency, download speed, and upload speed.

1. Proceed to Install **speedtest-cli**

```
sudo apt update
sudo apt install speedtest-cli
```

2. Run the speed test.

```
speedtest-cli
```

Setting up a static IP address

A static IP address can be useful in several situations.

1. **Networked Devices:** For devices that need a consistent IP address for network communication, such as printers, servers, or IoT devices.
2. **Port Forwarding:** When you want to forward specific ports to a device on your network, having a static IP address ensures that the forwarding remains valid.
3. **Network Stability:** Using a static IP address can help avoid conflicts and connectivity issues that may occur with dynamic IP addresses.
4. **Local Network Services:** For services like file sharing or media streaming within your local network, a static IP address can make it easier to access these services consistently.
5. **Remote Access:** If you need to remotely access a device on your network, having a static IP address simplifies the setup process.
6. Overall, setting a static IP address provides stability and consistency for devices that require reliable network connectivity and services.

The traditional method of editing the `/etc/network/interfaces` file.

1. Proceed to open terminal windows by pressing `Ctrl` + `Alt` + `T`. Or alternatively, select the terminal icon.
2. Edit the `/etc/network/interfaces` file using the `nano` text editor.

```
sudo nano /etc/network/interfaces
```

3. Locate the section for your network interface which might look similar to this:

```
auto eth0
iface eth0 inet dhcp
```

Proceed to change `dhcp` to `static` and add the following lines below to set your static IP configuration. Replace `eth0` with your actual interface name.

```
auto eth0
iface eth0 inet static
    address 192.168.1.10 # Set your desired static IP address
    netmask 255.255.255.0 # Set your subnet mask
    gateway 192.168.1.1 # Set your gateway IP address
    dns-nameservers 8.8.8.8 8.8.4.4 # Set your DNS server(s)
```

4. Save the changes and exit the text editor.

Setting up a static IP address

5. Restart the networking service to apply the new configuration.

Sudo systemctl restart networking

In case that ‘**sudo systemctl restart networking**’ is not working, the error might be due to the ‘**networking**’ service not managed by system in your Ubuntu version. Proceed to use the following command line in Terminal.

sudo systemctl restart system-networkd

6. Verify that the static IP address is set correctly by running the following command line.

ip addr show eth0 #Replace eth0 with your interface name

Effective Backup Methods for Ubuntu

Data loss can have a significant impact on home and business environments. Backing up files is crucial for safeguarding your data against loss due to hardware failures, accidental deletions, and malware attacks. Regular maintenance is vital to ensure that backups are stored securely and in a timeline fashion.

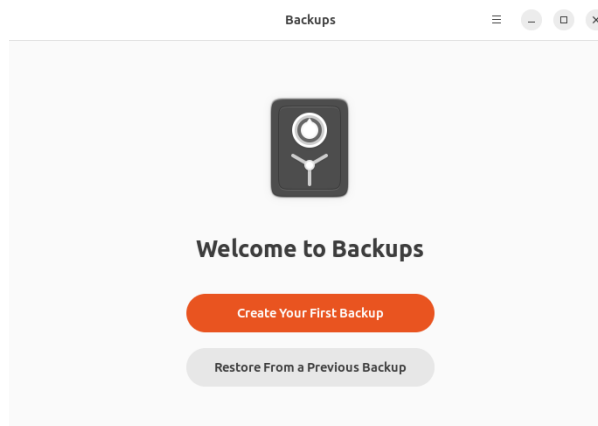
Deja Dup is a built-in utility in Ubuntu that is designed to be a user-friendly and is suitable for users, who prefer a simple backup solution with a graphical interface.

Here is a quick guide on how to setup Deja Dup.

1. Even though Deja Dup is often installed on Ubuntu by default, the application can still be installed in Terminal via the following command line:

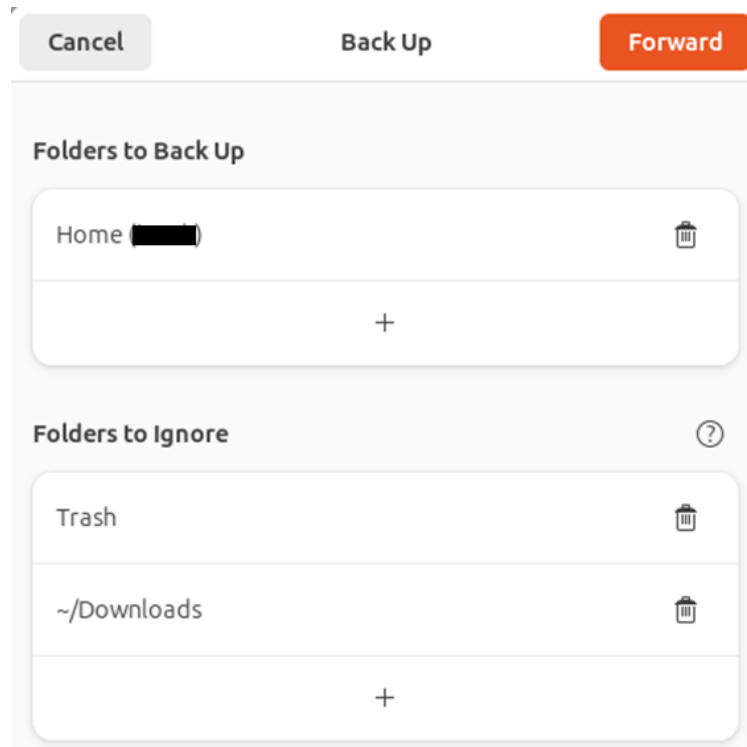
sudo apt install deja-dup

2. In the Applications menu, proceed to open **Deja Dup**. Alternatively, search for “Backup” or Deja Dup” and open the application.

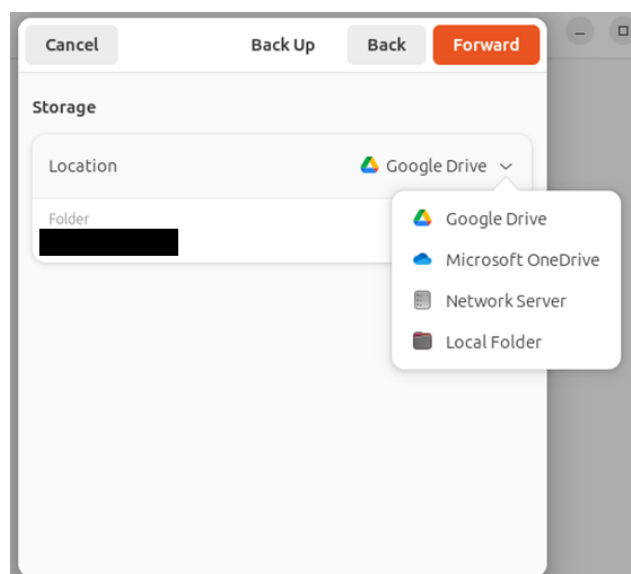


Effective Backup Methods for Ubuntu

- Once Deja Dup is opened, proceed to configure the backup settings. There are options for your backup location, schedule, and other preferences. The storage location can be local, network or cloud. Specify the desired folders to be included or excluded from backups.



When selecting **Forward**, in Location, there are options to save files to Google Drive, Microsoft OneDrive, Network Server and Local Folder. An external hard drive, USC Thumb Drive, or a WD My Cloud Home, Synology or Qnap NAS are also viable options for backup.



Effective Backup Methods for Ubuntu

4. **Set Encryption** (Optional) -> for added security, you have the option to encrypt your backup for added security. Be sure to remember the password. Click on **Forward** to complete the process.

Password Manager Software

Consider using a password manager application for saving passwords. Popular password applications include LastPass, NordPass and Bitwarden. This list is not exhaustive, and alternatives can be found online.

Backup Media

When selecting an encrypted USB drive, consider factors such as encryption strength, ease of use, durability, and the level of certification. Kingston, SanDisk, Verbatim, Lexar are a few popular brand names. Always check reviews and features online. External hard drives with password encryption are recommended. Synology and Qnap does offer excellent Network-Attached Storage (NAS) devices that are ideal for home and business uses.

How to keep your computer secure in Linux

Making Linux desktop computer more secure involves a combination of best practices, system configuration, and regular maintenance. Here are some key steps to enhance the security of device.

1. Software Updates

Regularly update your system and all installed software to patch security vulnerabilities. Use the following commands to update your system:

<code>sudo apt update && sudo apt upgrade</code>	<code># Debian / Ubuntu</code>
<code>sudo dnf update</code>	<code># Fedora</code>
<code>sudo yum update</code>	<code># CentOS (if applicable)</code>

2. Use Strong Passwords

Enforce strong password policies for user accounts. Consider using complex passwords with a minimum of 8 characters with at least one capital letter, number, and special character. Set a strong password for your user account and use a password manager to generate and store complex, unique passwords for your various accounts. Change passwords every 60 to 90 days.

3. Disable root login:

Avoid logging in as the root user. Instead, use **sudo** to perform administrative tasks.

4. Configure a firewall:

Use a firewall like ufw (Uncomplicated Firewall) or firewalld to control incoming and outgoing network traffic. Only open necessary ports.

5. Full disk encryption:

Encrypt your entire hard drive using technologies like LUKS (Linux Unified Key Setup) during installation to protect your data in case of theft or physical access.

6. Use secure boot:

Enable Secure Boot if your laptop and Linux distribution support it. This prevents unsigned or unauthorized code from running during boot.

7. Regular Backups

Create and maintain regular backups of your data. Ensure that backups are stored securely and are regularly tested for restoration. Be sure to save work files on the SharePoint and/or OneDrive.

8. Employ strong authentication:

Consider using two-factor authentication (2FA) for your user account, especially for remote login and sudo access.

9. Lock your screen and change your screensaver settings

Set a screensaver and configure your laptop to lock the screen when not in use. Use a strong password or PIN for unlocking.

10. Install and configure antivirus software:

While Linux is generally less prone to malware than some other operating systems, you can still install antivirus software to scan for threats. Check out [Ubuntu Guide on ClamAV](#).

How to keep your computer secure in Linux

11. Employ a password manager:

Use a password manager to store and autofill complex, unique passwords for your accounts.

12. SanDisk USB Flash Drive

SanDisk USB Flash Drive is a useful tool for saving files and folders. The device is only meant to be used as a temporary storage. Files and folders should be deleted when no longer needed.

Customizing Linux and GNOME Tweaks

GNOME Tweaks is a versatile tool designed to customize the GNOME desktop environment. It provides an intuitive, user-friendly interface for adjusting settings that go beyond the options available in the default GNOME Settings.

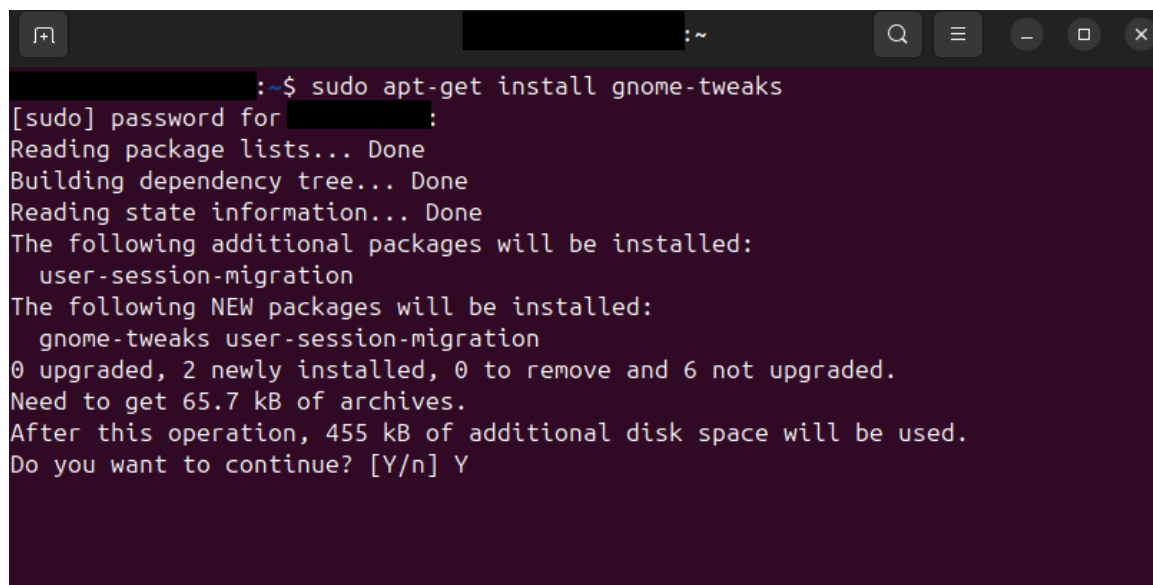
A few main features that GNOME Tweaks offers are:

1. Appearance Customization
2. Windows Management
3. Workspace and Keyboard
4. Startup Applications
5. Power and Hardware Settings
6. Advanced Tweaks

How to Install GNOME Tweaks

GNOME Tweaks can be installed via the GUI Interface via the APP Store. Alternatively, you can use the following command line in Terminal and select “Y” to continue.

sudo apt install gnome-tweaks

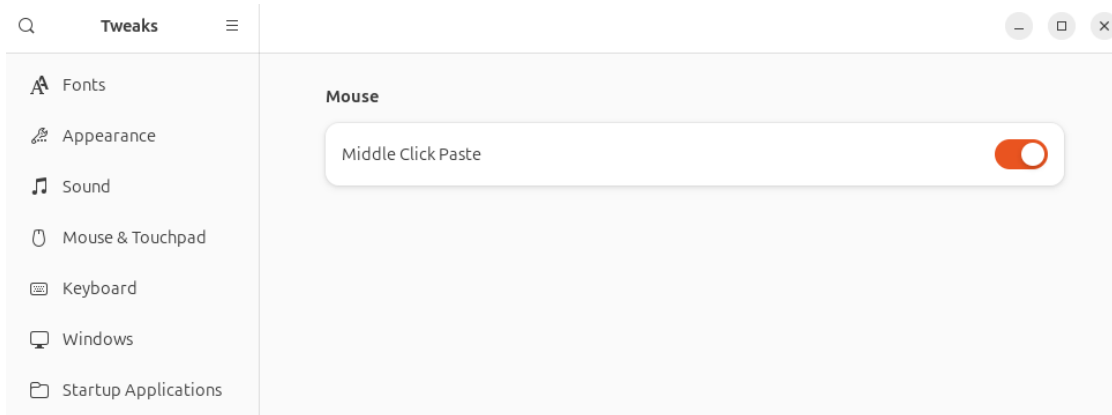
A terminal window with a dark background and light-colored text. The prompt is root@kali:~#. The command 'sudo apt-get install gnome-tweaks' has been entered. The terminal shows the output of the command, including package lists, dependency tree, and disk space requirements. The user has responded 'Y' to the confirmation prompt.

```
root@kali:~# sudo apt-get install gnome-tweaks
[sudo] password for root:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  user-session-migration
The following NEW packages will be installed:
  gnome-tweaks user-session-migration
0 upgraded, 2 newly installed, 0 to remove and 6 not upgraded.
Need to get 65.7 kB of archives.
After this operation, 455 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

To run GNOME Tweaks, open Terminal and type in the following command line:

GNOME-Tweaks

Begin to explore the GNOME Tweaks interface.

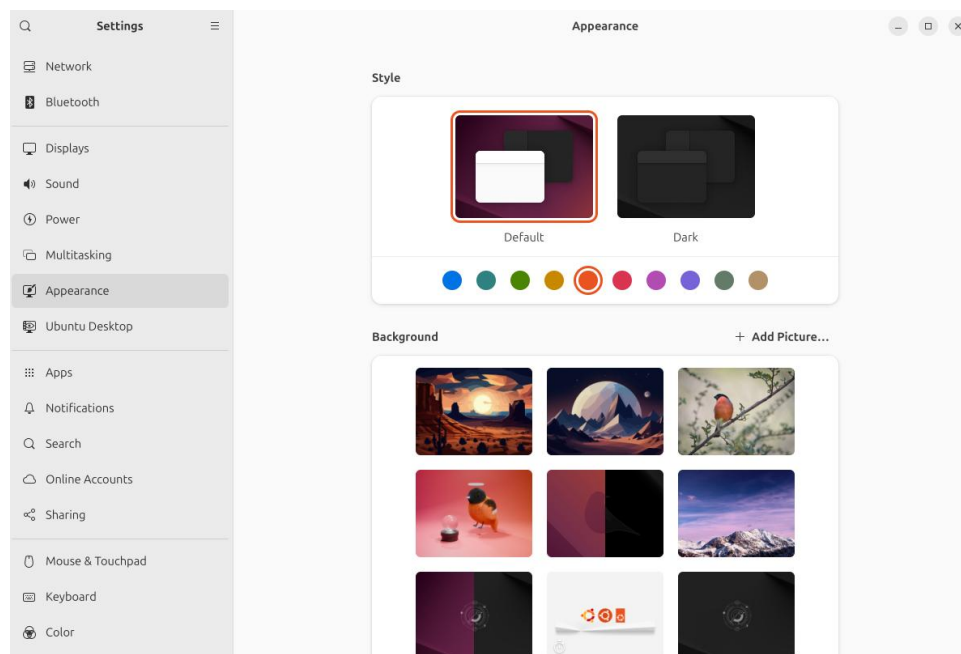


Customizing Settings

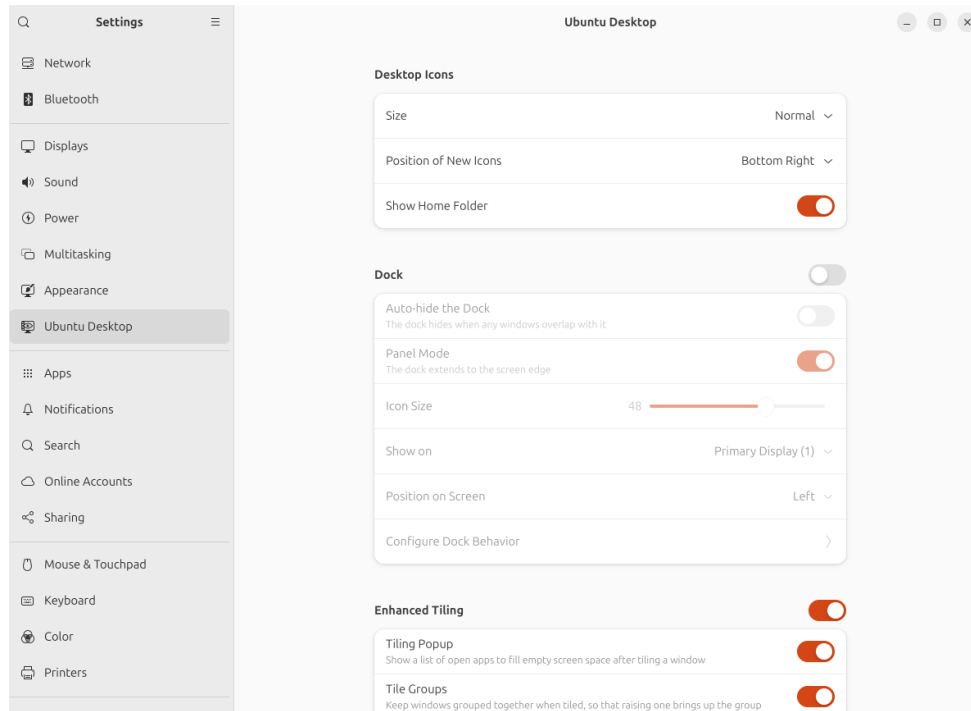
Select show Apps icon and proceed to search for **Settings**.



Under **Appearance** in the left pane, further customizations of the Linux desktop can be adjusted to personal preferences.



In the **Ubuntu Desktop** on the left pane, useful customization option includes the adjustment of desktop icon, dock, and enhancing tiling.

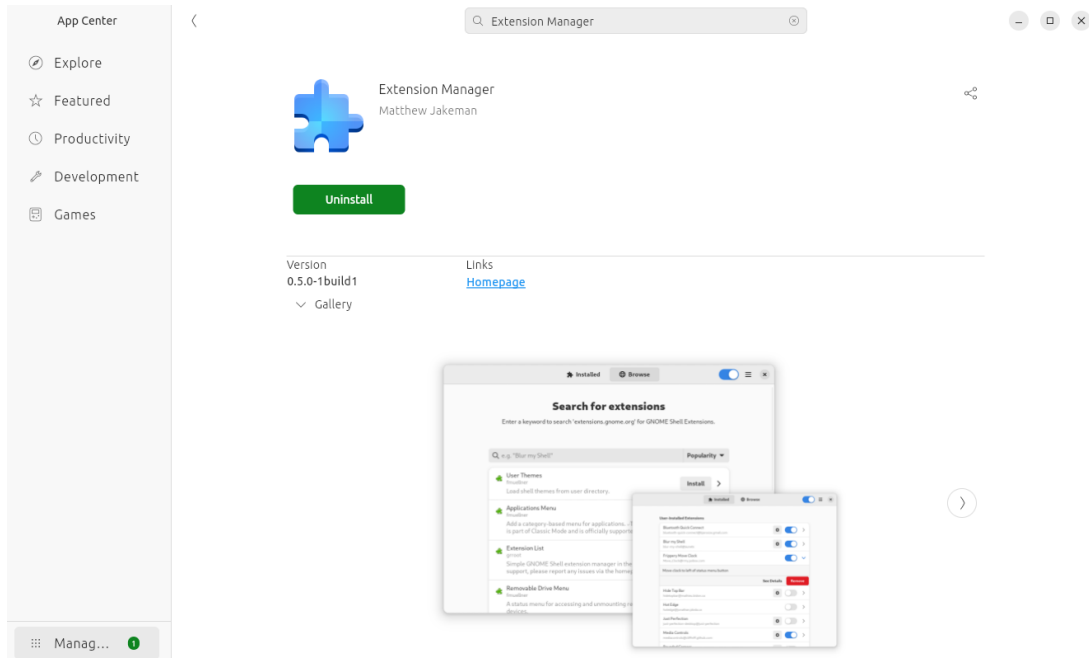


GNOME Shell Extensions

GNOME Shell Extensions enhance the functionality and appearance of the GNOME desktop environment. These extensions are like browser add-ons or plugins and allow users to customize their desktop experience. They allow users to customize and extend the behaviour of GNOME Shell beyond its default features. Effectively, users can use extensions on how one interacts with the desktop, and add new features, such as weather widgets, system monitors, or advanced task management tools. For more information, visit: <https://extensions.gnome.org/>

Extension Manager

Extension Manager is a utility for browsing, installing, and managing GNOME Shell Extensions. This utility provides a convenient way to handle your extensions. Within the Ubuntu App Centre, proceed to search for Extension Manager and click on install.



Blur My Shell creates a more visually appealing desktop experience by adding a blue effect to different parts of the GNOME Shell, including the top panel, and dash.

Dash to Panel provides a more traditional desktop experience by moving the dash to panel at the top of the screen.

Dash to Dock transforms that dash into a dock at the bottom of the screen.

User Themes allows users to easily change the GNOME Shell theme by applying different GTK themes.

Vitals shows system resource information like CPU, memory, network usage, disk usage, and temperature in the top panel, giving an overview of the system's performance.

Neofetch

Neofetch is a popular command-line system information tool written in Bash. It displays information about your operating system, software, and hardware in an aesthetic and visually pleasing way. Neofetch development was discontinued in April 2024. However, this tool still works well in Linux environments.

Installing Neofetch

1. Update your package list.

sudo apt update

```
~$ sudo apt update
Hit:1 http://ca.archive.ubuntu.com/ubuntu oracular InRelease
Hit:2 http://ca.archive.ubuntu.com/ubuntu oracular-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu oracular-security InRelease
Hit:4 http://ca.archive.ubuntu.com/ubuntu oracular-backports InRelease
All packages are up to date.
~$
```

2. Install Neofetch.

sudo apt install neofetch

```
nicholas@HAL9000:~$ sudo apt install neofetch
Installing:
  neofetch

Installing dependencies:
  caca-utils      libid3tag0      libopenexr-3-1-30
  chafa           libimath-3-1-29t64  libsixel-bin
  imagemagick     libimlib2t64     libsixel1
  imagemagick-6-common  libjxr-tools     libyuv0
  imagemagick-6.q16  libjxr0t64       netpbm
  jp2a            liblqr-1-0       toilet
  libavif16       libmagickcore-6.q16-7-extra  toilet-fonts
  libchafa0t64    libmagickcore-6.q16-7t64  w3m
  libgav1-1       libmagickwand-6.q16-7t64  w3m-img
  libgc1          libnetpbm11t64

Suggested packages:
  imagemagick-6-doc  gnuplot      mplayer      inkscape  dict-wn
  autotrace          grads        povray       figlet    dictd
  curl               graphviz     radiance     brotli    mailcap
  enscript           hp2xx        texlive-base-bin  cmigemo   w3m-el
  ffmpeg            html2ps      transfig     compface  xsel
  gimp               libwmf-bin   libraw-bin    dict

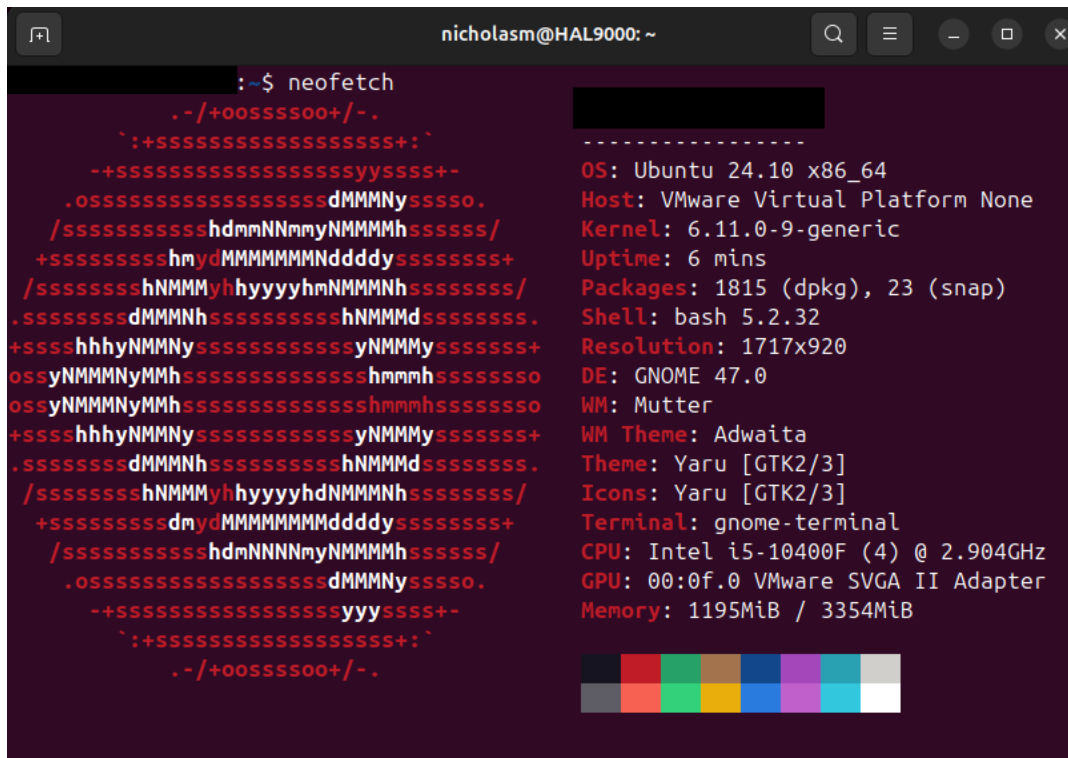
Summary:
  Upgrading: 0, Installing: 30, Removing: 0, Not Upgrading: 0
  Download size: 9,365 kB
  Space needed: 33.2 MB / 16.1 GB available

Continue? [Y/n] Y
```

Proceed to click on ‘Y’.

3. Run Neofetch

neofetch

A terminal window titled 'nicholasn@HAL9000: ~' showing the output of the 'neofetch' command. The output is split into two columns. The left column features a ASCII art logo for neofetch, rendered in red and white characters. The right column displays system information in red text, including OS (Ubuntu 24.10 x86_64), Host (VMware Virtual Platform None), Kernel (6.11.0-9-generic), Uptime (6 mins), Packages (1815 (dpkg), 23 (snap)), Shell (bash 5.2.32), Resolution (1717x920), DE (GNOME 47.0), WM (Mutter), WM Theme (Adwaita), Theme (Yaru [GTK2/3]), Icons (Yaru [GTK2/3]), Terminal (gnome-terminal), CPU (Intel i5-10400F (4) @ 2.904GHz), GPU (00:0f.0 VMware SVGA II Adapter), and Memory (1195MiB / 3354MiB). At the bottom right of the output, there is a small color calibration bar with 11 colored squares.

Customizing Neofetch

Neofetch is highly customizable through its configuration file. You can edit the file located at `~/.config/neofetch/config.conf` to change colors, add or remove information, and more. Here's a basic example:

```
background_color=ffffff
text_color=000000
# Add more customizations here
```

GITHUB

More information on Neofetch can be found at github at: <https://github.com/dylananaraps/neofetch>

Steam Gaming on Linux

Gaming on Linux has evolved dramatically in recent years. Steam has been on of the pivotal in making it easier to enjoy popular titles on Linux. Steam's integration with Linux significantly improved the gaming experience on the platform and made it more accessible to a wider audience.

Installing Steam

Installing Steam on Ubuntu is straightforward.

1. Update Your System.

```
sudo apt update  
sudo apt upgrade
```

2. Install Steam.

```
sudo apt install steam
```

3. Launch Steam in Terminal.

```
steam
```

4. Log In or Create an Account:

Once Steam is launched, log in with your existing account or create a new one. Follow the on-screen instructions to complete the setup. Steam boasts an extensive library of games, many of which are compatible with Linux. To find Linux-compatible games, use the "**SteamOS + Linux**" filter in the Steam store.

Optimizing Performance

1. Graphics Drivers:

Ensure you have the latest graphics drivers installed for the best performance. For NVIDIA users, use the proprietary drivers. AMD users can rely on the open-source Mesa drivers.

```
sudo apt install nvidia-driver-460
```

Replace 460 with the latest driver version if available.

2. Enable Proton:

Proton, a compatibility layer developed by Valve, allows you to play many Windows-only games on Linux.

Go to **Steam Settings > Steam Play**.

- Check the box for "**Enable Steam Play for supported titles.**"
- Optionally, check the box for "**Enable Steam Play for all other titles**" to use Proton for unsupported games.

3. Game Mode:

GameMode is a tool that optimizes your system's performance for gaming. Install it using:

```
sudo apt install gamemode
```

4. Configure Game Mode:

To use GameMode, you may need to modify the game's launch options. Right-click on the game in your library, select "**Properties**," and under "**Launch Options**" add:

```
gamemoderun %command%
```

Steam gaming has never been more accessible with a growing library of games and continuous performance improvements. Tools, like Proton and GameMode, help Linux to become a solid platform for gamers.

Linux Documentation

Learning Linux can be straightforward, especially with the wealth of tutorials, forums, and community support available. The [Ubuntu Desktop Guide](#) is the essential starting point to learn the first steps on how to become familiar with the Ubuntu desktop experience. Here one can find useful support information for Ubuntu: [Ubuntu Help](#) and [Ask Ubuntu](#) forum. Additionally, here is useful documentation for [Fedora](#) and [Zorin](#).

Ubuntu Desktop Guide

<https://help.ubuntu.com/lts/ubuntu-help/index.html.en>

Ubuntu Help

<https://help.ubuntu.com/>

Ask Ubuntu

<https://askubuntu.com/>

Linux command line for Ubuntu beginners

<https://ubuntu.com/tutorials/command-line-for-beginners#1-overview>

Fedora Documentation

<https://docs.fedoraproject.org/en-US/docs/>

Zorin Documentation

<https://help.zorin.com/docs/>

Linux Mint Documentation

<https://linuxmint.com/documentation.php>