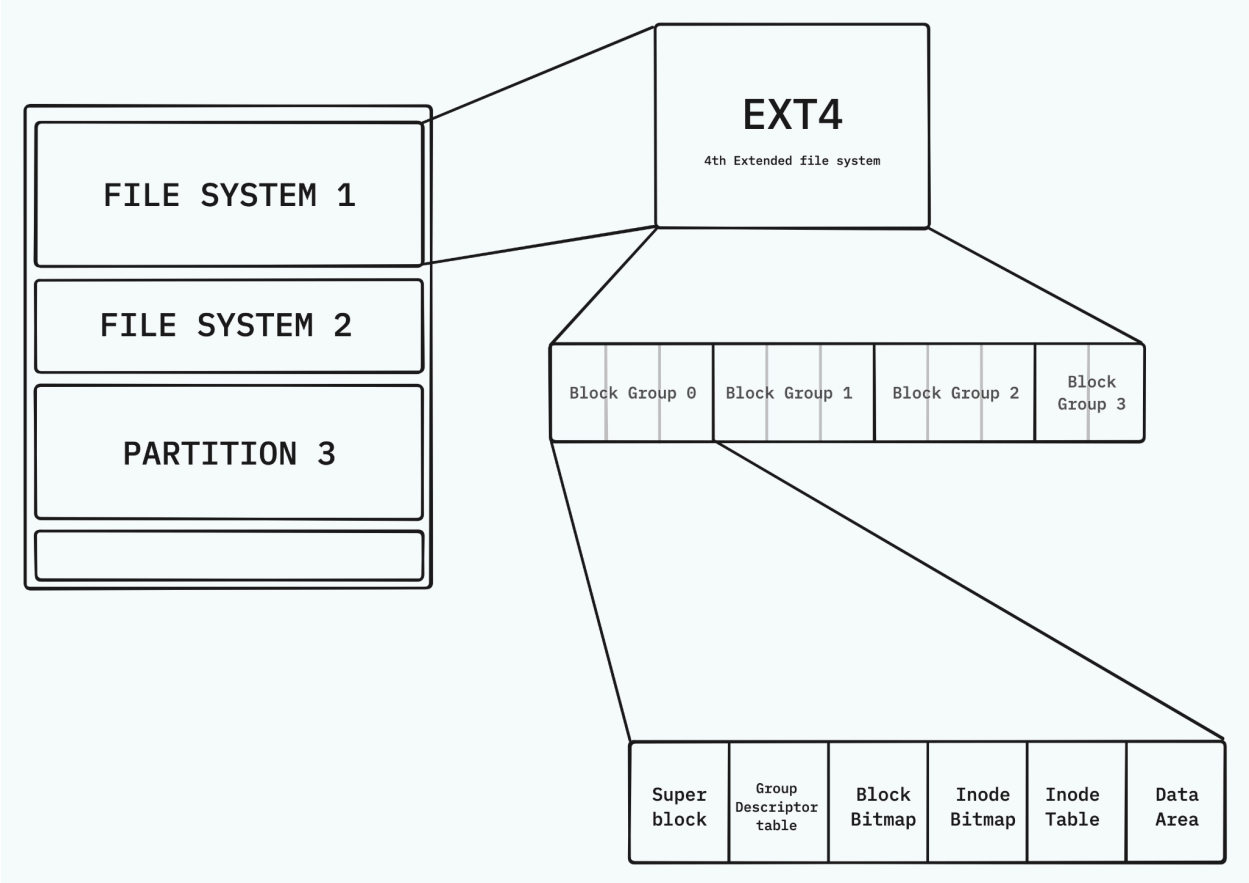
FILE SYSTEM

WHAT IS A FILE SYSTEM?

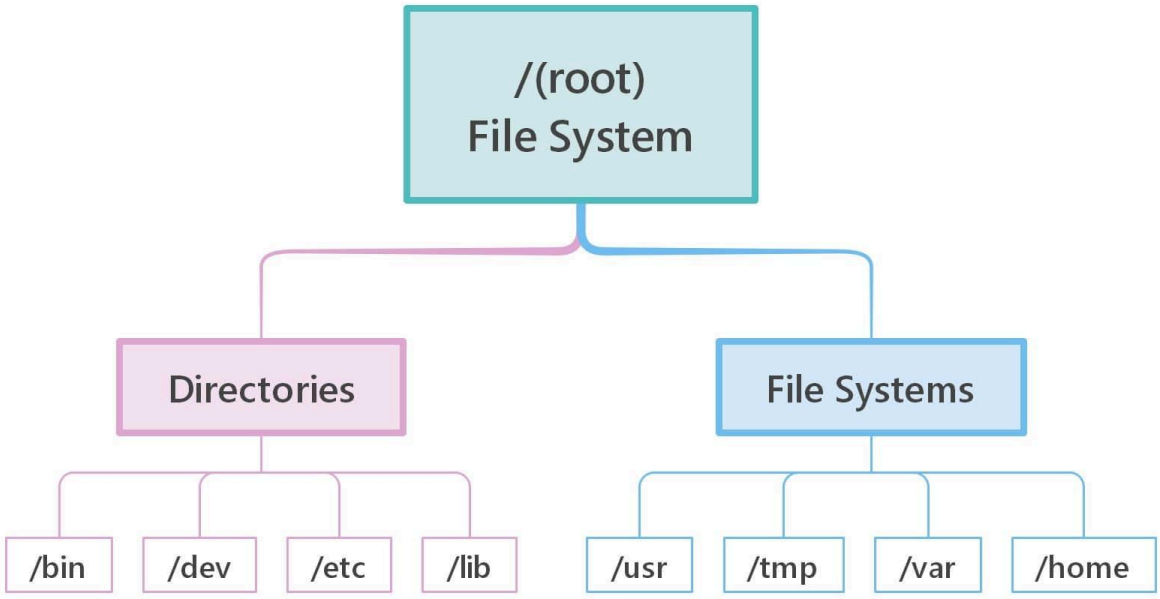
A Linux **file system** is a structured collection of files stored in the system's hard disk or storage. It's responsible for managing file names, sizes, creation dates, and other file-related information.

→ **ext4** is a journaling file system that keeps track of changes made to a file before they are committed to the file's main part. This allows for efficient data management and helps prevent data loss in case of a system crash.

The **ext4 file system** is stored as blocks of fixed size, and consecutive blocks are grouped together in block groups, with each group having the number of blocks except the last group. Within each block group, a unique layout of data structures is found, including the superblock, group descriptor table, block bitmap, inode bitmap, inode table, and data area.



THE STRUCTURE OF THE FILE SYSTEM



The directories on the right are file systems, they have separate sections of the hard disk allocated for their use.

Path	Description
`/`	root directory. Contains all the files required to boot the OS before other file systems are mounted as well as the files required to boot the other file systems.
`/bin`	Contains essential command binaries.
`/boot`	Consists of the static bootloader, Kernel executable, and files required to boot the linux OS.
`/dev`	Contains device files to facilitate access to every hardware device attached to the system.
`/etc`	Local system configuration files. Config files for installed applications may be saved here as well.
`/home`	Each user on the system has a subdirectory here for storage.
`/lib`	Shared library files used by the core system programs.
`/media`	Contains the mount points for removable suck as USB drives, CD-ROMS, etc.
`/mnt`	Contains mount points for removable devices that have been mounted manually.

Path	Description
`/opt`	Optional files such as third-party tools can be saved here.
`/root`	The home directory for the root user.
`/sbin`	This directory contains executables used for system administration (binary system files).
`/tmp`	The OS and many programs use this directory to store temporary files.
`/usr`	This directory is the largest one on the linux system. It contains all the programs and support files used by regular users.
`/var`	Is where data that is likely to change is stored. Various databases, spool files, user mail, etc. are located here
`/proc`	Is an illusionary file system that doesn't exist on disk but created in memory by the linux kernel to keep track of the running processes.

You will be using this later on:

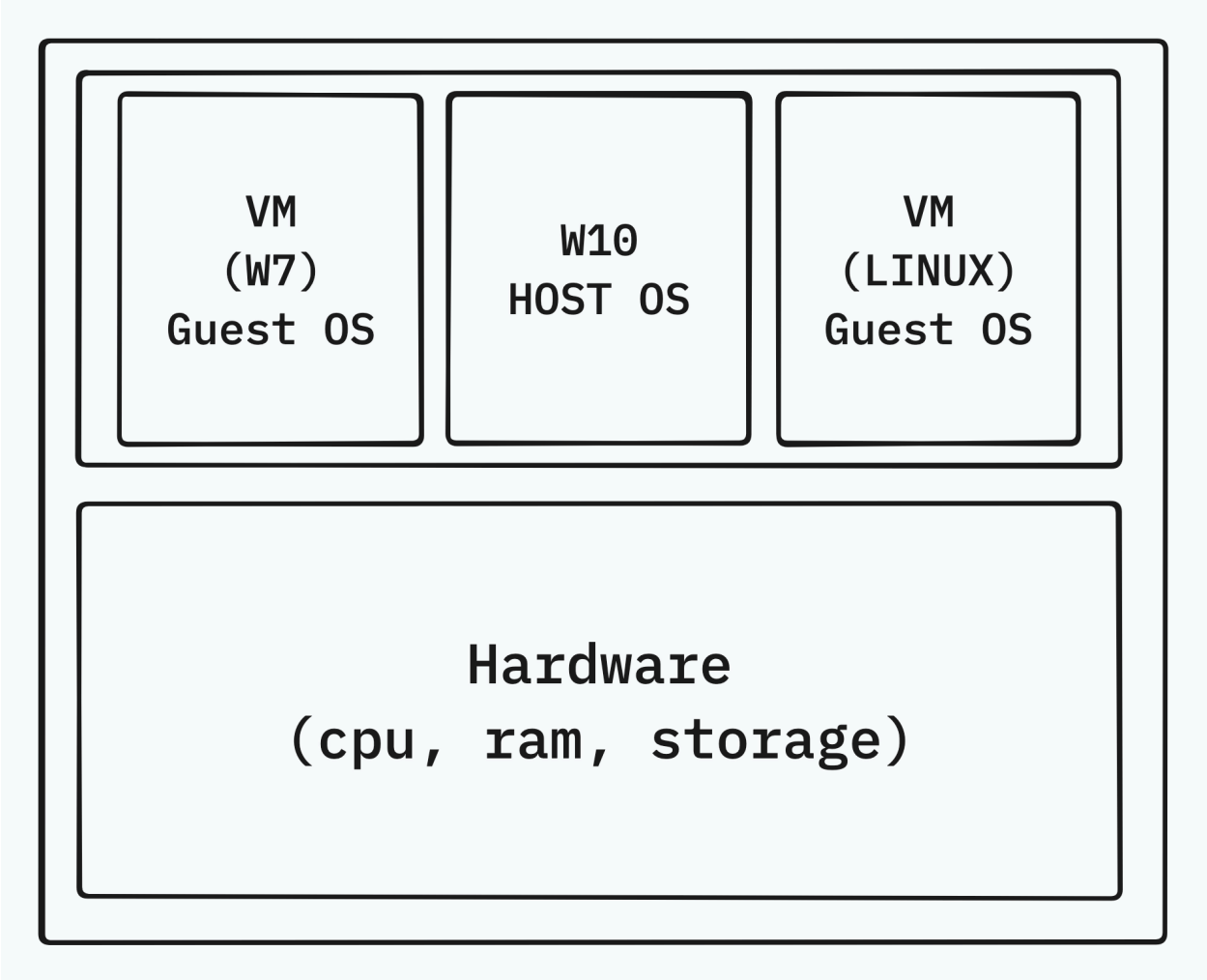
→ **Difference between**

/etc/login.defs sets default system-user account and password policy settings.

/etc/pam.d/common-password deals especially with password-related configurations during the authentication process.

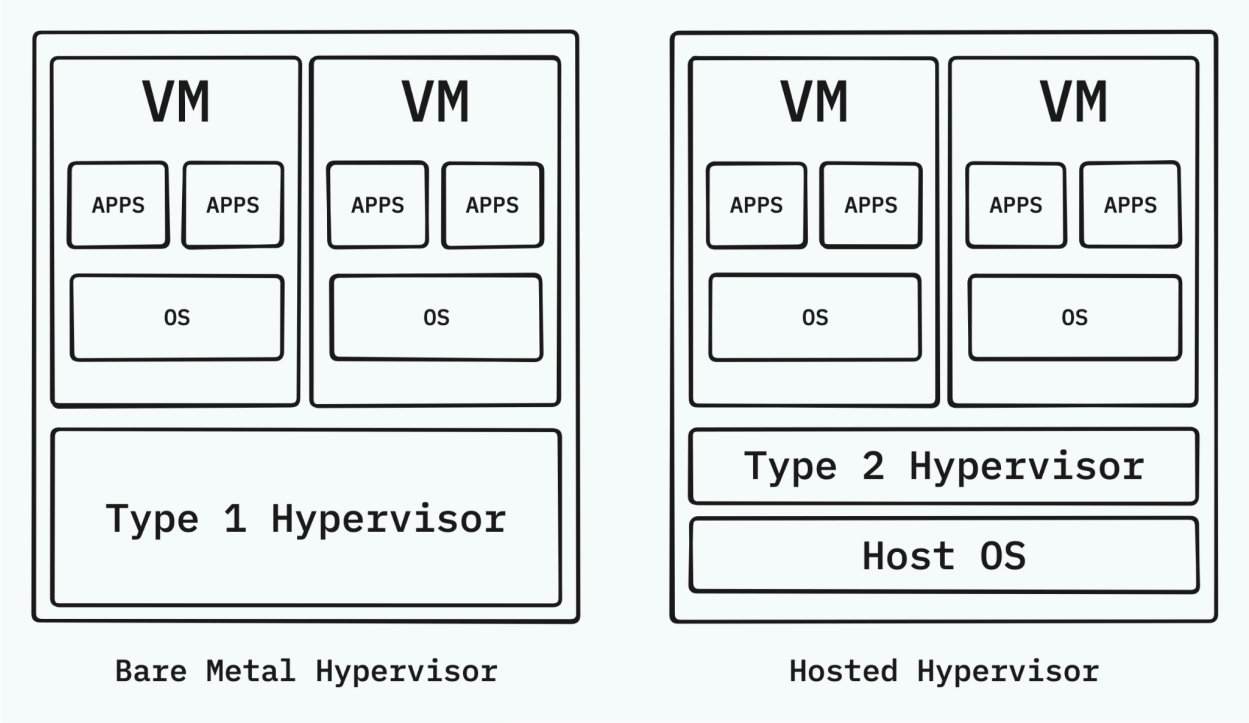
VIRTUAL MACHINE

Virtual Machine (VM) is a machine in your machine. (A virtual machine is a virtual representation, or emulation, of a physical computer).
Virtualization enables the creation of multiple virtual machines on a single physical machine, with each VM having its own operating system and applications.



HOW DOES 'VIRTUAL MACHINE' WORKS?

A **Virtual Machine** cannot interact directly with the physical Hardware. Instead a **HYPERVISOR (virtual machine monitor)** coordinates between the virtual machines and the underlying physical hardware, allocating resources and keeping the VMs separate to prevent interference.



WHY CHOOSING DEBIAN OVER ROCKY?

Rocky is more stable than Debian and supports enterprise applications. Does not have an upgrade path. It comes with many security in-built features that help protect from cyber-attacks using SELinux. It helps to reduce the vulnerabilities of privilege escalation attacks.

Debian, released and supported by the community, Debian has more software/packages available. Debian community members still maintain it. It comes with an easy installation package.

DIFFERENCE BETWEEN 'OS' AND 'KERNEL'?

The **OPERATING SYSTEM (OS)** is a complete system software that acts as an interface between the user and the computer hardware, providing various services and managing resources. On the other hand, the **KERNEL** is a core component of the operating system, responsible for **low-level** tasks such as memory management, process management, and device management.

WHAT DOES 'SWAP SPACE' MEANS?

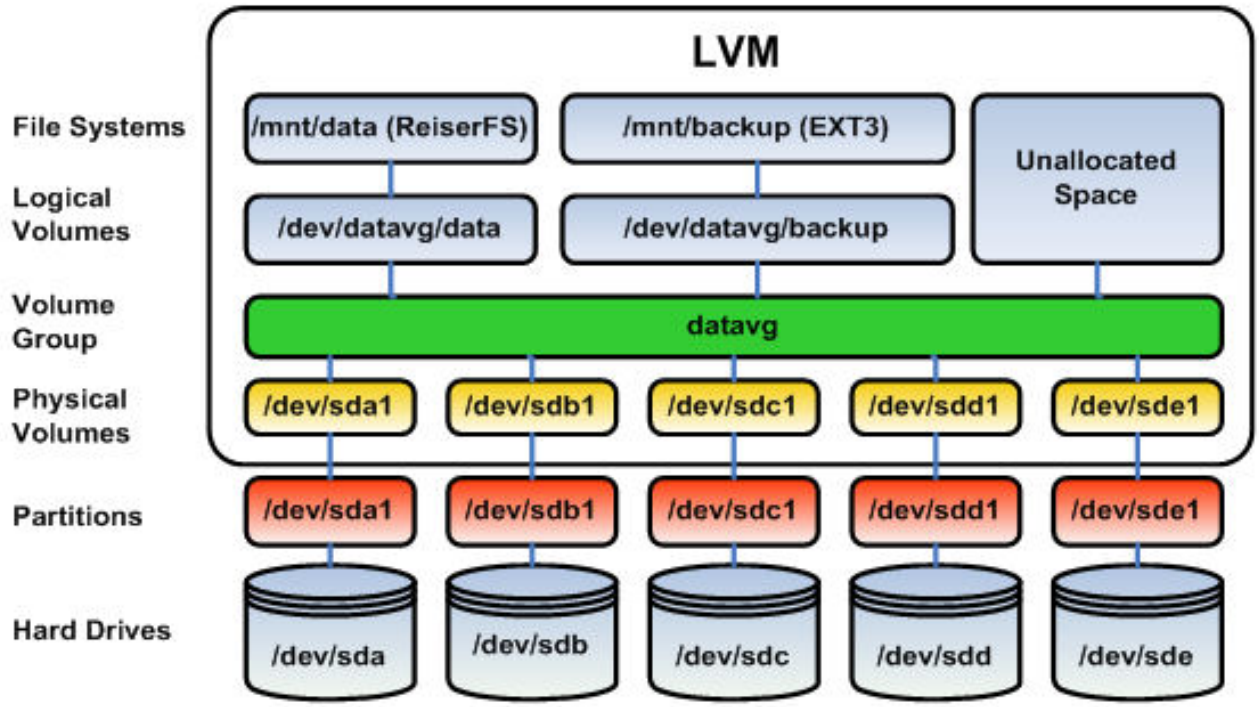
Swap Space provides a way for the OS to temporarily move data from RAM to Disk and back when the RAM is saturated. This process is known as "SWAPPING".

WHAT DOES 'LVM' MEANS?

LVM (Logical Volume Manager) allows the creation of groups of disks or partitions that can be assembled into a single *(or multiple)* filesystems.

- Can be used from nearly any mount point EXCEPT */boot*

WHAT IS THE DIFFERENCE BETWEEN 'LOGICAL VOLUME' AND 'PHYSICAL VOLUME' AND 'GROUP VOLUME'?



DIFFERENCE BETWEEN 'PRIMARY' AND 'LOGICAL'?

The main difference between **PRIMARY** and **LOGICAL** partitions is that ***primary*** partitions can be used as booting OS, and there can be 4 partitions for it, while ***logical*** partitions are not bootable and are used for storing data in an organized manner.

WHAT DOES 'MOUNT' MEANS?

Mounting a filesystem in Linux refers to the process of making a particular file system accessible at a specific location in the Linux directory tree.

1. **Insert the USB Drive:**
   - Physically insert the USB drive into a USB port on your computer.
2. **Identify the USB Drive:**
   - Open a terminal and use the `lsblk` command or `fdisk -l` command to list the available block devices and identify your USB drive. Let's assume it is `/dev/sdb`, but your actual device name may vary.
3. **Create a Mount Point:**
   - Create a directory where you want to mount the USB drive. For example:

```
$> sudo mkdir /mnt/usb
```

4. **Mount the USB Drive:**
   - Mount the USB drive to the specified mount point. Assuming the USB drive is formatted with the FAT32 filesystem:

```
$> sudo mount -t vfat /dev/sdb1 /mnt/usb
```

   Here, `/dev/sdb1` is the first partition on the USB drive, and `/mnt/usb` is the mount point.
5. **Access the USB Drive:**
   - The contents of the USB drive are now accessible under the `/mnt/usb` directory. You can navigate to this directory to view and modify the files on the USB drive.

WHAT IS THE DIFFERENCE BETWEEN 'APT' AND 'APTITUDE'?

The main difference between the two is that `apt-get` is a lower-level package manager (is straightforward command-line), `apt-get` tends to not install the recommended packages.

While `aptitude` is a higher-level package manager (user-friendly interface, it has a UI interface), `aptitude` tends to install recommended packages by default, and provide more features.

WHAT IS 'AppArmor'?

AppArmor allows the system administrator to restrict the capabilities of programs, it provides tools to isolate processes (like programs) from each other... and in turn isolate an attacker from the rest of the system when an application is compromised.
AppArmor has three main modes of operation:
- **Enforce Mode**, **AppArmor** actively enforces the security policies defined in the profiles.
- **Complain Mode**, **AppArmor** logs policy violations but does not actively enforce them.
- **Disabled mode**, **AppArmor** is completely turned off for a specific profile or for the entire system.

Meanwhile the **SELinux** security module uses a complex and comprehensive policy that controls every process and object (like programs and users) in the system.

WHAT IS 'wall' COMMAND?

The `wall` command is a Linux utility that displays a message, or the contents of a file, on the terminals of all currently logged-in users. It is typically used by root to send out shutting down messages to all users just before powering off the system. The command stands for "write to all".

WHAT IS 'UFW' (Uncomplicated Firewall)?

UFW is an interface to modify the firewall of the device without compromising security. You use it to configure which ports to allow connections to and which ports to close. This is useful in conjunction with SSH, and can set a specific port for it to work with.
UFW is not a firewall but a front-end for iptables, and iptables is a front-end for the netfilter kernel module that is performing packet filtering within the Linux kernel.

WHAT IS CRON?

Cron or **cron job** is a command line utility to schedule commands or scripts to happen at specific intervals or a specific time each day. Useful if you want to set your server to restart at a specific time each day.

WHAT IS BOOT LOADER ? (GRUB FOR DEBIAN)

BootLoader is a piece of code that loads the kernel into memory and sets the kernel with some specific parameters so that the OS starts.

WHAT IS PORT FORWARDING?

Port forwarding is a networking technique used to redirect a communication request from one address and port number combination to another while the data packets are traversing a network gateway, such as a router or firewall.

TCP is a communication protocol that ensures reliable data transmission.

(In General, IP *(Internet Protocol)* is an unreliable network protocol it will not guarantee the full transmission of the data sent, the data might be lost or unsorted or the data will not all be sent, but TCP will guarantee the full transmission of the data, he will guarantee that the data will not be lost and be fully arrived at its destination) (for more info read this article from KHAN ACADEMY)

"**Port** is just a number." If an IP address is like the address of a postal apartment in a building, a port is like a mailbox number. (Every service on the computer needs a unique identifier to be reachable. Ports are those unique identifiers).

WHAT IS SSH?

SSH (Secure Shell) is a network protocol that allows us to remotely connect to another server, computer, or something else in a way that the connection is secure and encrypted.

(for more info read this article from CLOUDFLARE SITE)

- How does SSH Work ?

Watch these videos, computerphile, ssh_keys.

SU & SUDO ?

su: switch user.

sudo: give the privileges to run a command as root (superuser) or another user.