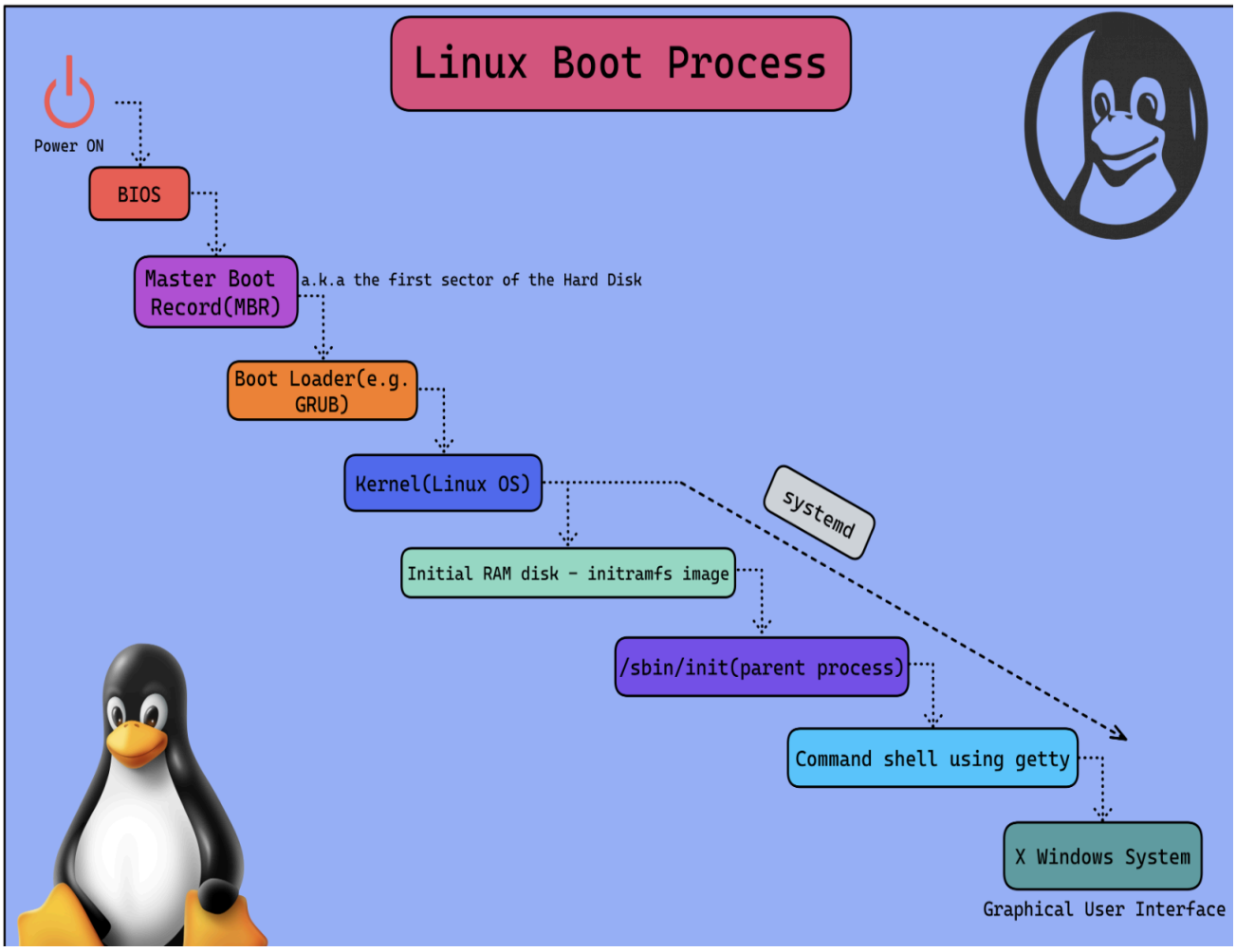
TOP 50 LINUX INTERVIEW QUESTIONS

1. What is Linux?
   It is a free, open-source, and kernel operating system.
   It is designed for systems, servers, embedded devices, mobile devices, and mainframes and is also supported on major computer platforms such as **ARM, x86, and SPARC**.
   Linus Torvalds developed Linux.
   It offers CLI and GUI

2. Explain Linux Boot process?



BIOS/UEFI	Basic Input/Output System. Located in ROM chip in motherboard Turn on your computer, the BIOS instantly runs POST (Power On Self Test) • POST is a part of the BIOS which performs plenty of diagnostic tests on the hardware components such as SSD/HDD, RAM, Keyboard, Mouse, USB, etc. • UEFI can be considered as a successor of BIOS. • An abbreviation for Unified Extensible Firmware Interface, it performs the same function as a BIOS with one major difference: it keeps all data regarding initialization and startup in an.efi file instead of storing it on the firmware. **>>** Pass control to MBR
MBR Master Boot Loader	• **MBR is the initial (main) sector of a hard disk that identifies the location of the operating system (OS) to**

	complete the booting process. Pass control to Boot Loader
Boot Loader	• **GRand Unified Boot loader (GRUB) is usually the first thing you'll see when you boot up your computer.**  Pass control to Kernel
KERNEL	• **Kernels are self-extracting and stored in compressed format to conserve space.** **Loads initramfs image**

Initramfs image	• **The initial RAM disk is an initial/temporary root file system that is mounted prior to when the real root file system is available.** • **This initramfs image is embedded in the Kernel and contains minimal binary files, modules & programs required for mounting the real root filesystem**
Init process (parent process)	**/sbin/init**
SHELL/GUI	**USER ACCESS**

3. What are the differences between ARM,X86 and Sparc?

ARM	SPARC	X86
ARM (Advanced RISC Machines) is a processor architecture that is used in a wide range of devices	SPARC processors use a *Reduced Instruction Set Computing (RISC)* architecture which means that they use a simplified instruction set that allows them to execute instructions quickly and efficiently.	X86 - 32 bit register X64 - 64 bit register *(CISC) includes a comprehensive instruction set* capable of handling more diverse tasks but may be less efficient in terms of cycles per instruction.
USE CASES **Used in Smartphones, tablets and embedded systems** **ARM processors are typically more energy-efficient and cost-effective**	**USE CASES:** **SPARC processors are known for their scalability, reliability and their ability to handle large workloads.** **Used in high-end server and workstation systems**	**USE CASES:** **Server and PC**

4. Name some Linux Distros?

   Because the Linux operating system is open sourced and released under the GNU General Public License (GPL), anyone can run, study, modify, and redistribute the source code, or even sell copies of their modified code.

Linux distributions are available as community versions or enterprise versions. A community distro is a free Linux distro primarily supported and maintained by the open source community. An enterprise—or commercial—Linux distro is available through a subscription from a vendor and does not rely solely on community support.

Distro	Description
Ubuntu	Ubuntu, developed by Canonical Ltd., is renowned for its user-friendly interface and extensive software repository. It's based on Debian and inherits many of its features.
Debian	Debian, often referred to as the "universal operating system," prides itself on its stability, reliability, and commitment to free and open-source software principles.
Centos	However, with CentOS 7 EOL on June 30, 2024 and all other versions having already been sunsetted, it is recommended to migrate to CentOS alternatives like Rocky Linux or AlmaLinux or make the switch to CentOS Stream.
Fedora	Red Hat is the primary corporate sponsor for the Fedora Project It is the upstream Linux distribution for redhat Linux
Redhat	Red Hat is the world's leading provider of enterprise open source solutions, using a community-powered

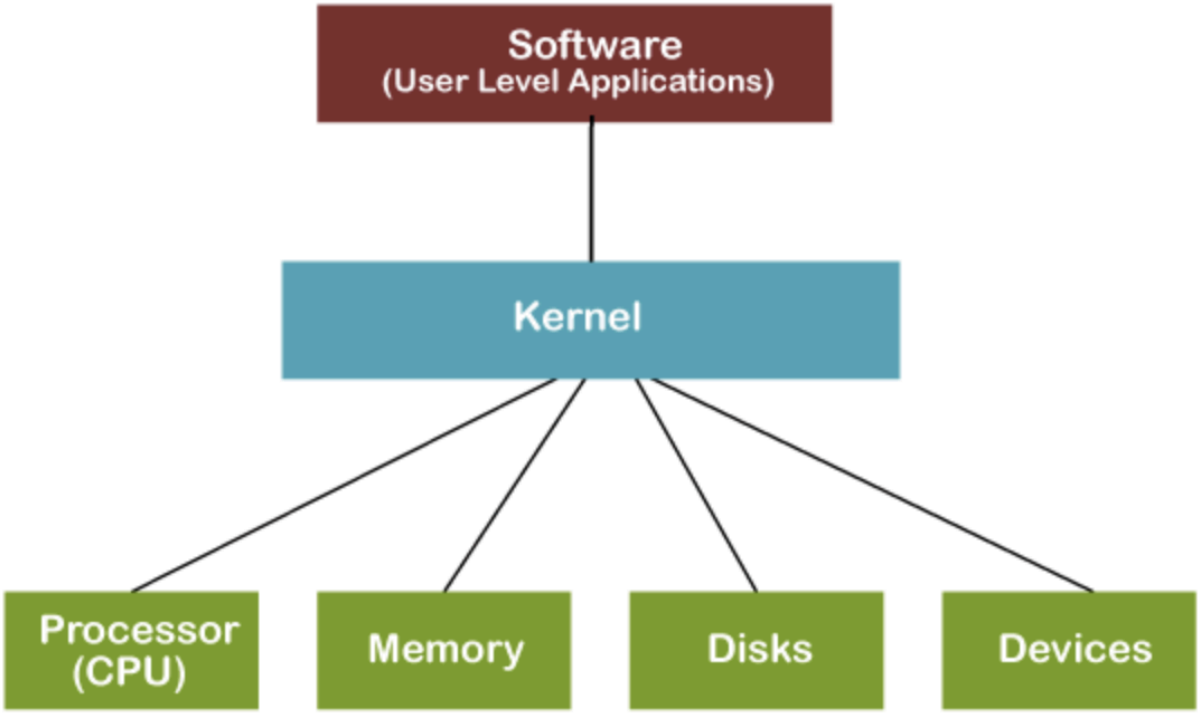
	approach to deliver high-performing Linux, hybrid cloud, edge, and Kubernetes technologies. It is a subsidiary for IBM

4) What are major differences between Linux and Windows?

	LINUX	WINDOWS
Cost	It is a free and open-source OS.	It is not open-source and is not free to use except trial version
Security	Linux is highly secure.	Windows is less secure compared to Linux.
Efficiency	More efficient	Less efficent
Use case	Very good for Servers	More UI, less efficient for servers than Linux

5) What is Linux Kernel?

The Linux® kernel is the main component of a Linux operating system (OS) and is the core interface between a computer's hardware and its processes. It communicates between the 2, managing resources as efficiently as possible.



The kernel has 4 jobs:

1. **Memory management:** Keep track of how much memory is used to store what, and where
2. **Process management:** Determine which processes can use the central processing unit (CPU), when, and for how long
3. **Device drivers:** Act as mediator/interpreter between the hardware and processes
4. **System calls and security:** Receive requests for service from the processes

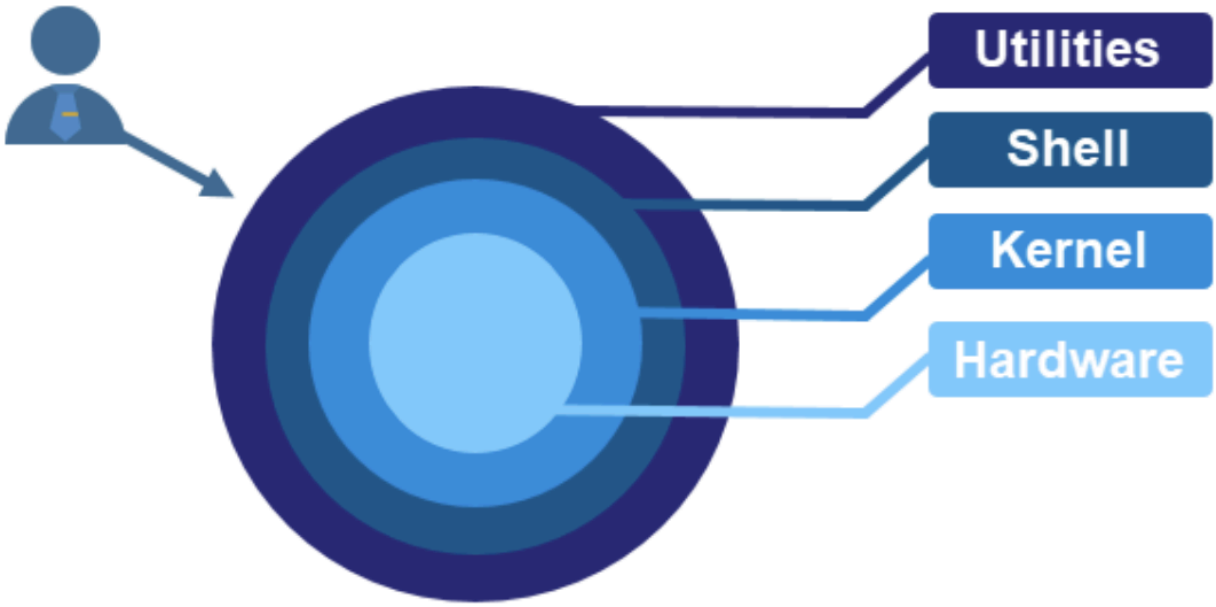
6) What is LILO?

LInux loader ,It loads the Linux operating system into memory and starts the execution.

7) What is the init process in Linux?

The init or also called the initialization process is the **first process that begins during the system boot**. It is responsible for initializing and processing the system in its functional state. Hence, init works as the parent process because its process ID is 1.

7) What is a Shell in linux?
A shell is a special user program that provides an interface for the user to use operating system services. Shell accepts human-readable commands from users and converts them into something which the kernel can understand. It is a command language interpreter that executes commands read from input devices such as keyboards or from files. The shell gets started when the user logs in or starts the terminal.



SHELL	COMMENTS
csh (C Shell):	Offers job control and spell checking and is similar to C syntax

ksh (Korn Shell):	A high-level shell for programming languages.
ssh (Z Shell)	This shell has a unique nature, such as closing comments, startup files, file name generating, and observing logout/login watching.
bash (Bourne Again Shell):	This is the default shell for Linux.

8) Why it is called Bourne Again Shell(BASH)?
The "Bourne Again" part signifies that Bash is an enhanced version of the original Bourne shell, incorporating features from other shells (like the C shell and Korn shell) and providing additional functionalities.
Bourne shell (sh), developed by Stephen Bourne at Bell Labs

9)**What is a root account?**
The root is like the user's name or system administrator account in Linux. The root account provides complete system control, which an ordinary user cannot do.

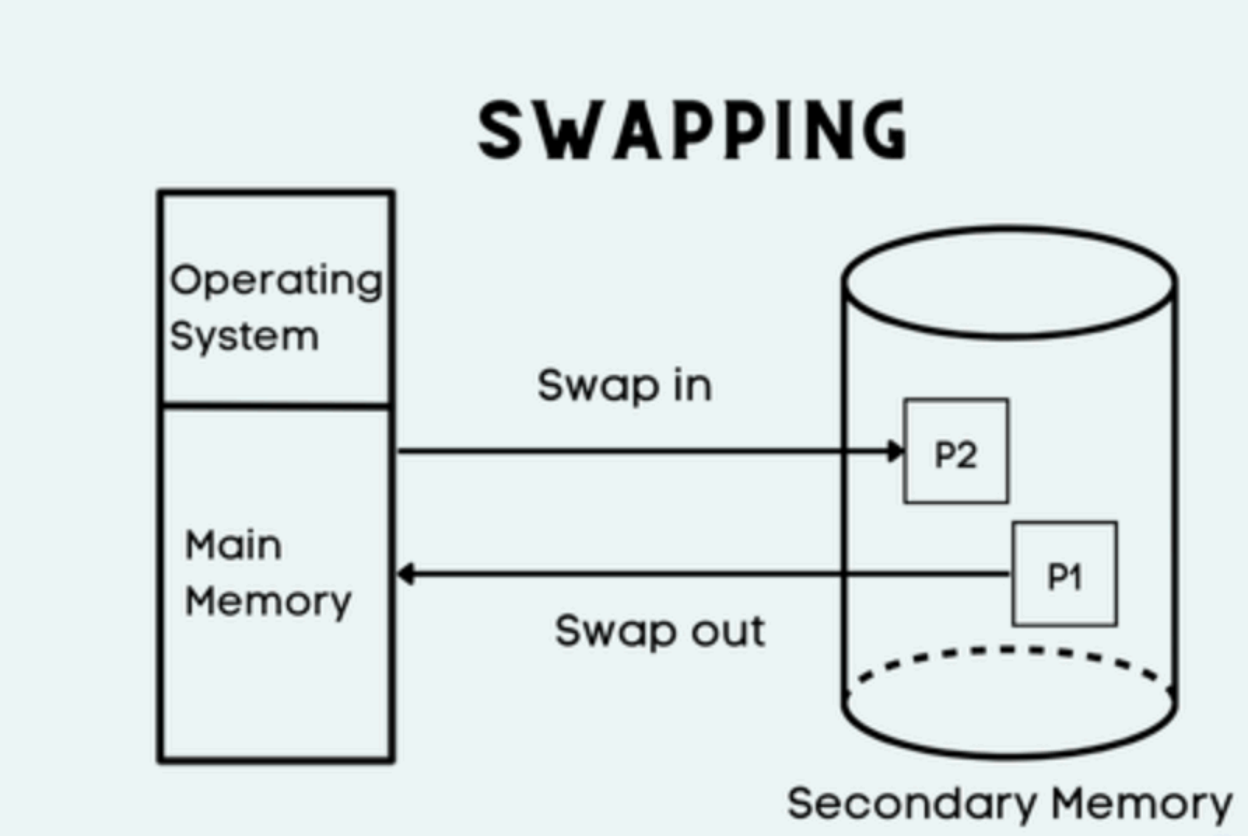
10) What is difference between CLI and GUI?

CLI	GUI
It is **command line interface**. It takes input as a command and runs the tasks of the system	**Graphical User Interface** or the human-computer interface. It uses icons, images, menus, and windows, which can be

	manipulated through the mouse.

11) What is Linux Swap space?

Linux uses swap space to expand RAM. Linux uses this extra space to hold concurrently running programs temporarily.

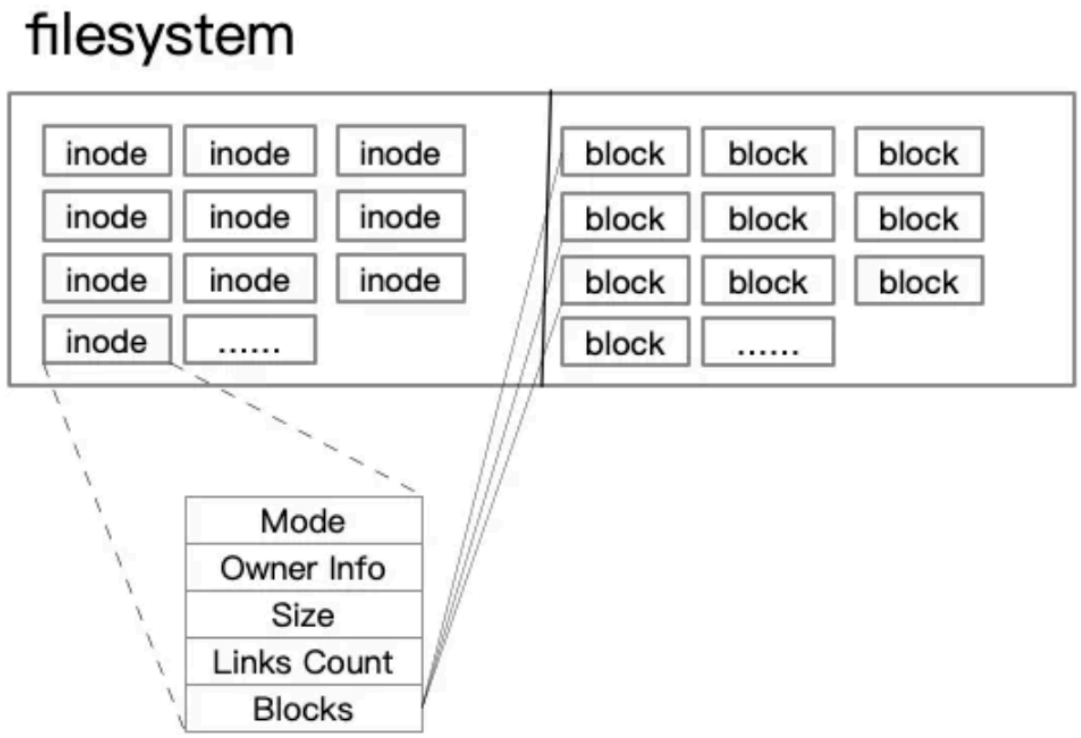


10) What is inode number?
Inode is index node
 This is File serial Number (Unique identifier of file)
It serves as a unique identifier for a specific piece of metadata on a given filesystem.

```
[tcarrigan@rhel ~]$ df -i /dev/sda1
Filesystem     Inodes IUsed  IFree IUse% Mounted on
/dev/sda1      524288   312 523976    1% /boot
```

You can see from the command syntax and the output above that we ran `df -i` on filesystem `/dev/sda1`. There are a total of 524,288 inodes on this filesystem, with only 312 of them being used (about 1%).

An inode (aka index node) is a data structure used by Unix/Linux like filesystems in order to describe a filesystem object. Such an object could be a file or a directory. Every inode stores pointers to the disk block's locations of the object's data and metadata



10) What is difference between Softlinks and Hardlinks?

HARD LINKS	SOFT LINKS
It includes original content. A hard link always points a filename to ***data on a storage device.*** ln test.txt hardlinkfile.txt Usecase: Backups	Symbolic link to original file Not pointing to harddisk content of file ln -s test.txt linkfile.txt Usecase: Shared libraries, java home path
Hard links are faster as compared to soft links.	Soft links are slower.
It shares similar inode numbers.	It shares different inode numbers.
It uses less memory.	It uses more memory.

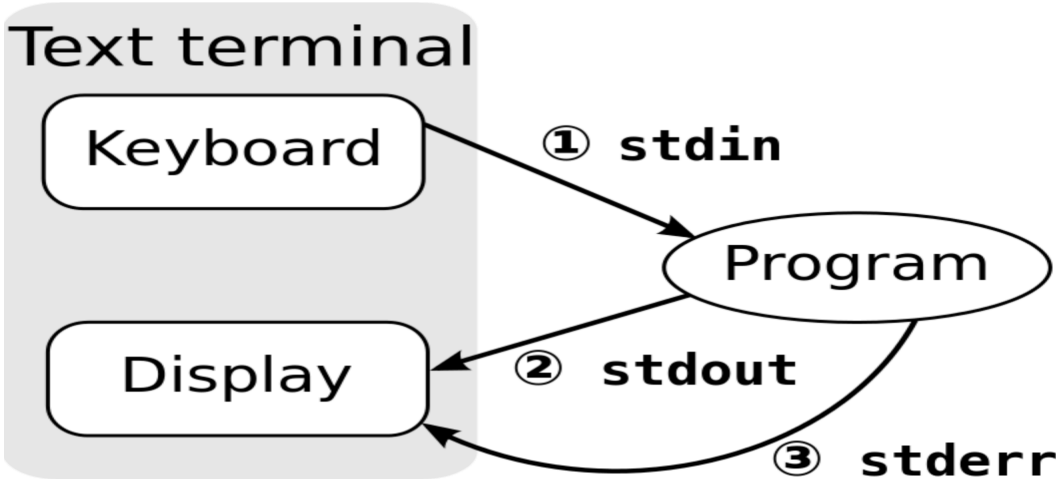
11) **How do users create a symbolic link in Linux?**
Symbolic links, symlink, or soft links are shortcuts to files and directories. Users can create the symbolic link in Linux through the' ln' command. The general command to create a symbolic link is as follows:

ln -s **<existing_source file> <optional_symbolic link>**

12) What are stdin, stdout,stderr?
These are three standard streams that are established when a Linux command is executed.
Whichever Linux command you're using provides one end of each stream

Output and input in Linux OS are divided into three standard streams:

- Stdin (standard input)
- stdout(standard output)
- stderr (standard error) lg 2> err.txt **or** lg 2> /dev/null



13) What is a file system? Commands to mount a file system

A file system is a structure used by an operating system to organize and manage files on a storage device such as a hard drive

You can explore linux file system using command

tree

#tree / -L 1 (View fileystem in / partition with Level 2)

/etc	Consists of mostly Configuration Files
/home	Contains Home directory

/lib	Libraries are files containing code that your applications can use
/proc	*proc*, like */dev* is a virtual directory. It contains information about your computer, such as information about your CPU and the kernel your Linux system is running. It is the essential interface to access the system, perform debugging tasks, check the Kernel functioning, find process-related information, and many more.

14) Scenario based Troubleshooting Techniques

Scenario	**Solution/ Troubleshooting**
Website Not accessible	nslookup <samplesite.com> traceroute <samplesite.com> curl -v <samplesite.com> Check for Firewall rules like Security group..
Server Load is high Check which process	top

occupies more load and analyze System Load	
Disk Space is filled up Check which folders occupies more space and clear please	du -sh /* |sort -hr|head -n 10 # List Files or directory which occupies more size in / dir
Check all running process in server	ps -aux
Check linux release and kernel	uname -a uname -r # kernel version
There is a nginx which is not starting and listening in a specific port. Troubleshoot…	netstat -tulp systemctl start nginx systemctl status nginx Check logs of service at /var/log/nginx/error.log
When I tried to copy more files from one location to another. It got disconnected. How shall I reinitiate the copy	Use rsync: `rsync` is a fast and versatile command-line utility for synchronizing files and directories between two locations over a remote shell It provides **fast incremental file transfer** by transferring **only the differences** between the source and the destination. # Copy from Local to remote rsync -a /opt/media/ remote_user@remote_host_or_ip:/opt/media/ # Copy from Remote to Local

	rsync -a remote_user@remote_host_or_ip:/opt/media/ /opt/media/
Run a script/Task at a particular time	**Cron** 0 2 * * * script1.sh # Run 2AM every day 0 0 1 12 * script2.sh # Run 1st December midnight **0 4 * * 2,4 script3.sh # Run 4 AM on Tuesday and Thursday** 

14) How to add user in Linux?

useradd user1
passwd user1

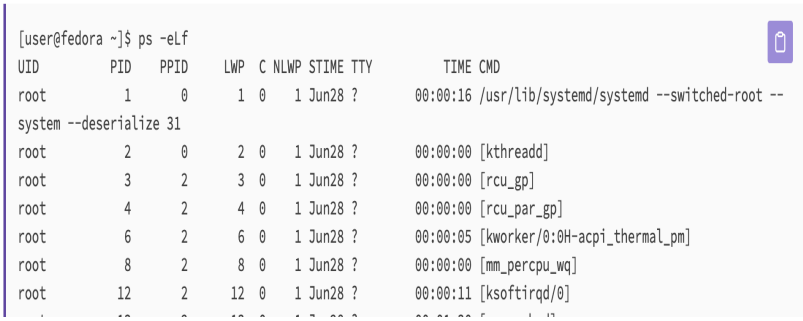
15) What is a Filesystem in linux and why mkfs is used?

Without a file system, applications could access the storage in incompatible ways that lead to resource contention, data corruption and data loss.

Every disk needs a filesystem in order to function correctly and support read and write operations, as well as other management tasks

mkfs is a command used to format a block storage device with a specific file system.

mkfs.ext4 <partition>
mkfs.xfs <partition>
mkfs.ntfs <partition>

Process	Thread
A process is a computer program under execution **Linux processes are isolated and do not interrupt each other's execution**.	**A thread is a lightweight process**. A process can do more than one unit of work concurrently by creating one or more threads.
# ps -ef command to view all process	Let's see an example and identify the process and its thread in Linux using the *ps -eLf* command. We're interested in PID, LWP, and NLWP attributes: • PID: Unique process identifier • LWP: Unique thread identifier inside a process • NLWP: Number of threads for a given process 

```
[user@fedora ~]$ ps -eLf
UID          PID    PPID     LWP  C NLWP STIME TTY          TIME CMD
root           1       0       1  0    1 Jun28 ?        00:00:16 /usr/lib/systemd/systemd --switched-root --
system --deserialize 31
root           2       0       2  0    1 Jun28 ?        00:00:00 [kthreadd]
root           3       2       3  0    1 Jun28 ?        00:00:00 [rcu_gp]
root           4       2       4  0    1 Jun28 ?        00:00:00 [rcu_par_gp]
root           6       2       6  0    1 Jun28 ?        00:00:05 [kworker/0:0H-acpi_thermal_pm]
root           8       2       8  0    1 Jun28 ?        00:00:00 [mm_percpu_wq]
root          12       2      12  0    1 Jun28 ?        00:00:11 [ksoftirqd/0]
```

16) What is ulimit?

It controls the resource limit for the user process

It set the limit on the system resource to prevent consuming the higher resources.

ulimit -a # Check ulimit values
ulimit -u 50 # Set Max number of process to 50

17) What is RAID?

The full form of RAID is the **Redundant Array of Independent Disk** that allows the system to combine the different physical disk drives into a logical unit. RAID is used to improve the system's disk performance and data integrity.

RAID Level	Description
RAID 0	It is called striping, which allows you to split the data into multiple disks without redundancy.
RAID 1	It is called mirroring, which allows you to create a complete copy of data on multiple disks.
RAID 5	It distributes the parity information and data on multiple disks.
RAID 6	It is the improved version of RAID 5 as it uses two sets of parity information to provide higher data redundancy.
RAID 10	It combines RAID 0 and RAID 1 to generate the set of mirror disks to improve performance and redundancy.

18) How to Harden a new linux server ?

Password	Strong password. But suggest using ssh key based authentication
Security	Use IPtables, security group(AWS), Run system updates

	Kernel tuning: /etc/sysctl.conf
Logging	EFK / Loki
Monitoring	Prometheus
Performance	Enable Swap memory (virtual memory in disk)

19) Some useful commands

Command	***Uses***
ls	
mkdir	
pwd	
top	
grep	
tar	
cat	
wget	
free -m	
df	
man	

20) Iptables command

The iptables command configures **Netfilter firewall rules** providing the network address translation, packet filtering, etc. iptables inspects the network packet and then manages them according to the defined rules.

Built-in chains that are included in tables.

- **INPUT :** A set of rules for packets destined to localhost sockets.
- **FORWARD :**for packets routed through the device.
- **OUTPUT :** It is locally generated packets, meant to be transmitted outside.
- **PREROUTING :** It is used for modifying packets as they arrive.
- **POSTROUTING : I**It helps in modifying packets as they are leaving

Syntax:

iptables [-t table] --append [chain] [parameters]

Iptables -L	List iptable rules
iptables -t filter --append INPUT -j DROP	Drops all the traffic coming on any port.

iptables -t filter --check INPUT -s 192.168.1.123 -j DROP	Drop packets from specific Ip address
iptables -I INPUT -s 78.14.25.106/32 -p tcp --dport 22 -j ACCEPT	Block User from ipaddress

21) What are Ports (Network Ports) in linux ? Name some standard Ports?

Within an operating system, a port is opened or closed to data packets for specific processes or network services. Typically, ports identify a specific network service assigned to them

Range 0 to 65535.
Commands to check open ports in Server

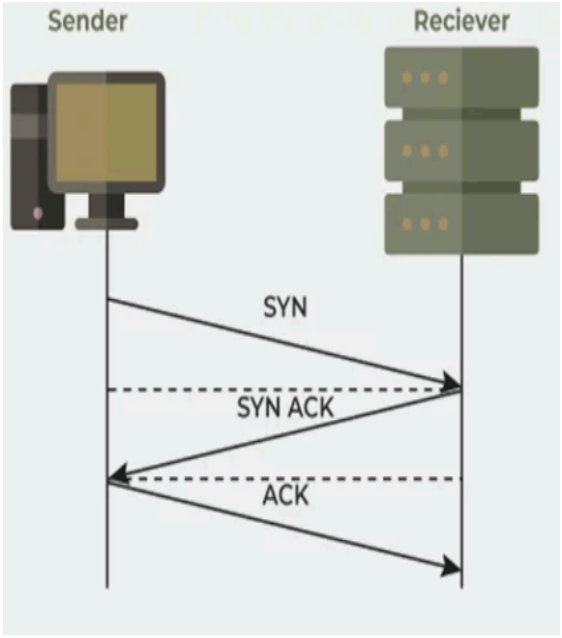
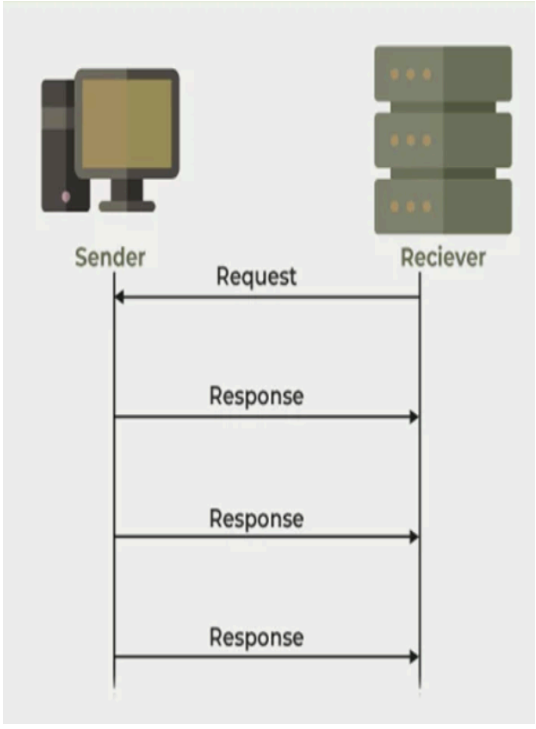
netstat
nc (Net cat)

Some of common ports

Port Number	Service
21	FTP(File transfer protocol) - Transfer files over network
22	SSH
23	Telnet
25	SMTP (EMAIL)

53	DNS service
80	http
443	https (Banking site..secure)

22) What is difference between TCP and UDP Protocol?

TCP	UDP
TCP (transmission control protocol)	UDP stands for user datagram protocol.
Connection-oriented — The device must establish a connection before transmitting data (handshake included) and close the connection after transmission 	**Connectionless** — No connection and no handshake are required to send data. 

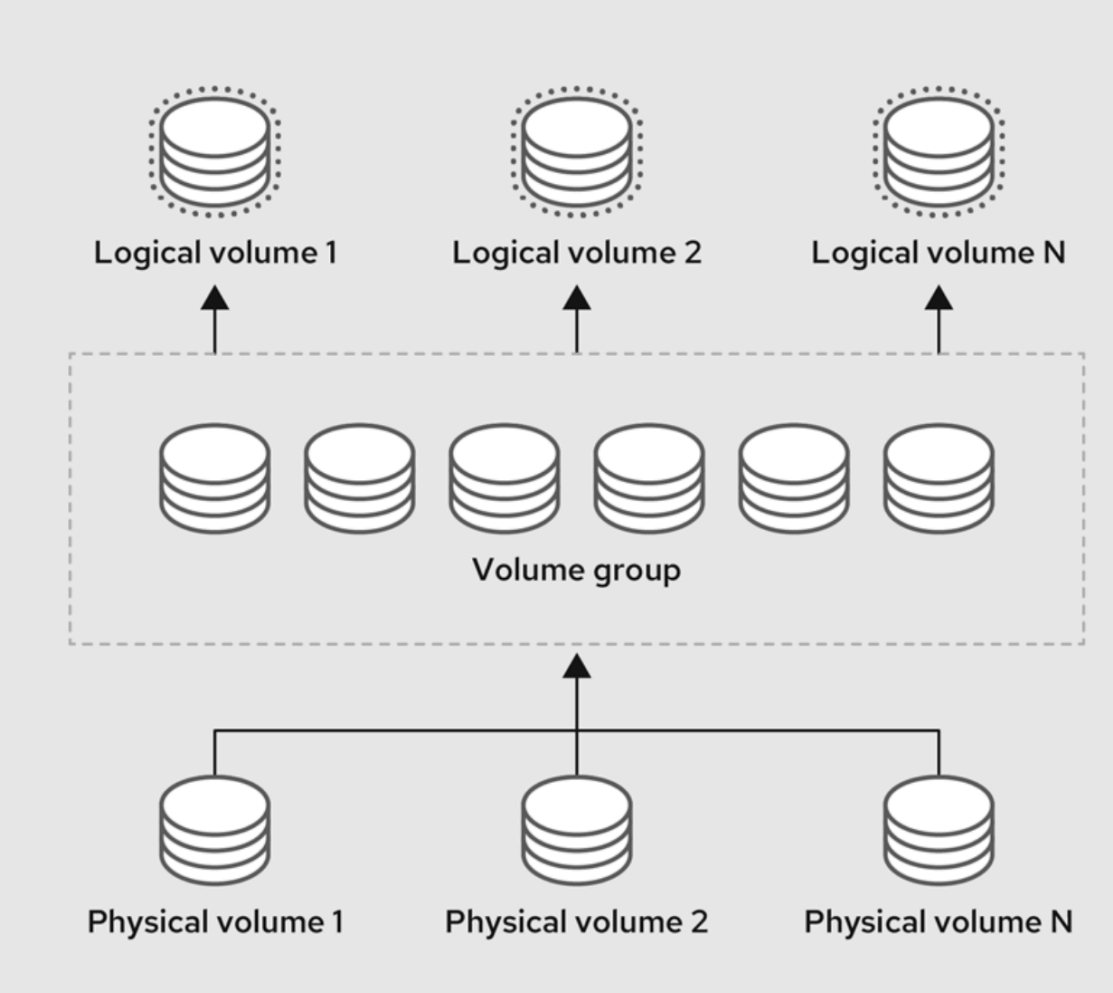
Reliable — Data packet delivery is guaranteed.	Unreliable — Datagrams delivery isn't guaranteed.
Stateful —The client and the server keep the information about the session.	Stateless — The server doesn't keep any information about the session.
Slower than UDP as it follows many steps to ensure accuracy.	Faster than TCP as it's a much simpler protocol.
Usecase: Web browsing. File transfer. Email (SMTP, IMAP/POP)	Video and music streaming. Online games, multiplayer games. Live broadcasts and video conferencing. Domain name system (DNS) Queries Voice over IP (VoIP).

21) What is difference between LVM and normal disk partition ?

Refer: https://www.redhat.com/en/blog/lvm-vs-partitioning

LVM: Logical Volume Manager
which provides an advanced disk management approach in Linux. It is a subsystem that allows a user to efficiently allocate the disk space on the physical storage device.

1. Resize storage capacity
2. Efficient dynamic storage allocation



22) What is Disk Formatting ?

Disk formatting is the process that prepares a storage partition for use.
It helps to arrange the file on the disk storage. It manages the file name, file size, creation date, and much more information about a file.

XFS	High-speed which is developed for parallel I/O processing. Supports **Maz size: 500 TB**
ext4	It is faster file system among all the Ext file systems. It is a very compatible option for the **SSD (solid-state drive) disks,** and it is the default file system in Linux distribution. **Maz size: 16 TB**
ext2/ext3	The major drawback of **Ext3** is that it does not support servers because this file system does **not support file recovery and disk snapshot.** Supports max **2TB** filesize

23) Create a partition,file system and Mount it please..

fdisk -l. # List disk and partitions
fdisk /dev/xvdb
 mkfs.xfs /dev/xvdb
mount -t auto /dev/xvdb /devops

24) What is sudo command in linux?

The word “sudo” is the short form of “Superuser Do” that allows you to run the command with system privileges. With this command, you can get the system’s administrative access to perform various tasks.

25) What is Private Key and Public key?

- The above output (0 0 2) shows that the access to the owner is 0, access to the group members is 0, and access to everyone is 2. This 2 is an octal value, to understand the access permissions, we would have to convert it to decimal, 2 is equal to 010 in binary, which can be clarified into 0 for read, 1 for write, and 0 for execute.

Permissions	Octal Value	Binary Value	Description
—	0	000	No permission
–x	1	001	only permission to execute
-w-	2	010	only permission to write
-wx	3	011	permission to write and execute
r–	4	100	only permission to read
r-x	5	101	permission to read and execute
rw-	6	110	permission to read and write
rwx	7	111	permission to do all three, i.e. read, write and execute

- So we can conclude that the above output says – only write permissions for everyone.

26) What is umask

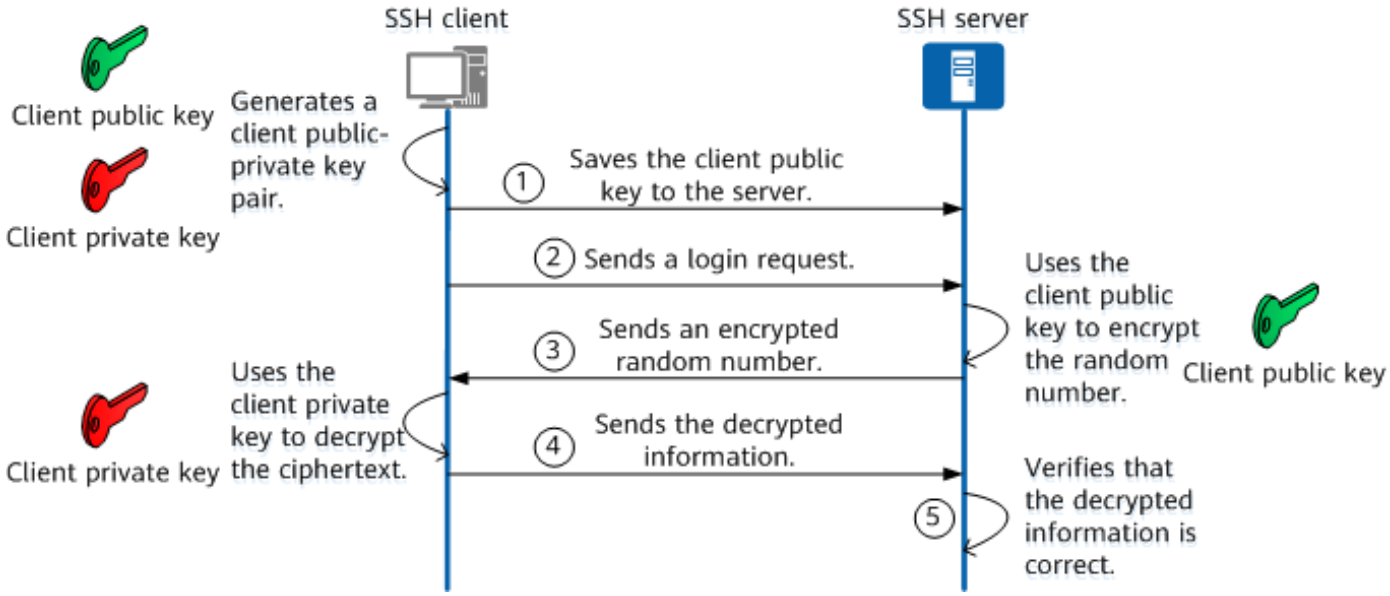
Umask is used to set default permission

022 (Mask write permission for group and others)

mkdir test

drwxr-xr-x 2 vd2 staff 64 31 Oct 18:54 test

27) SSH private and Public Key



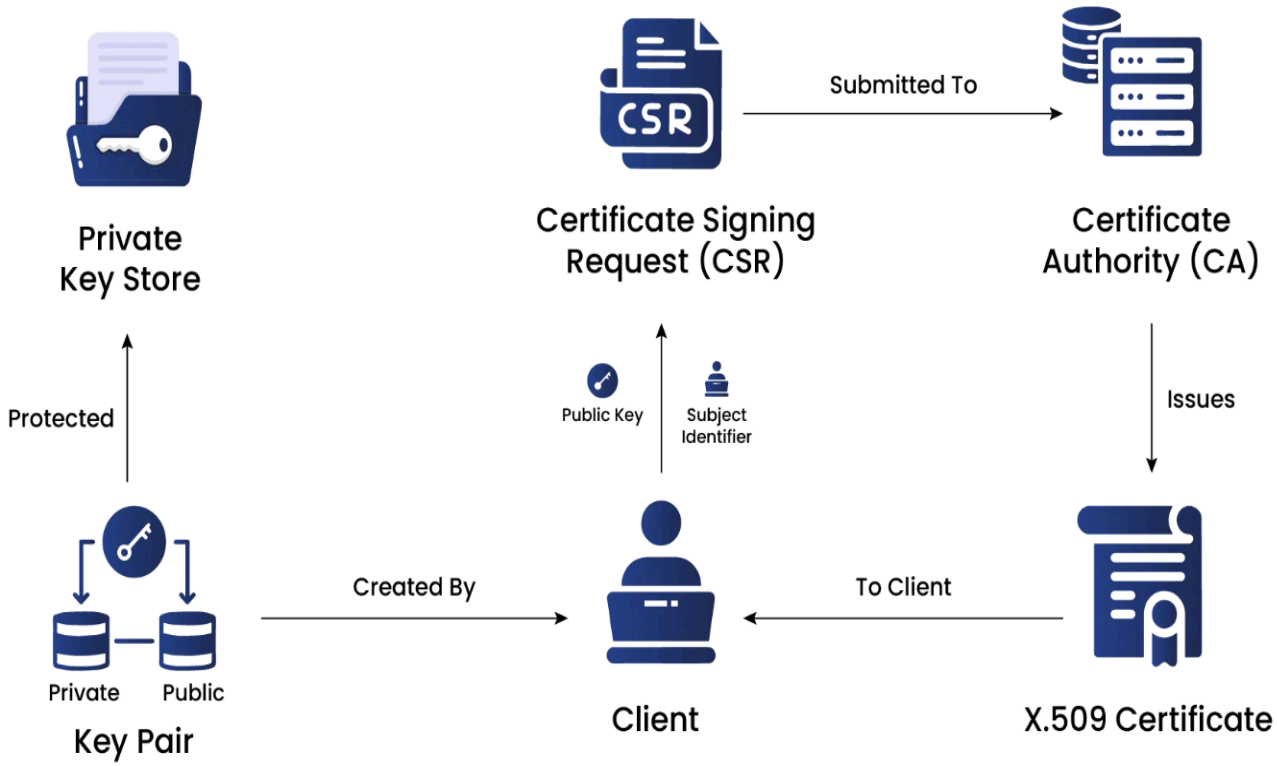
Steps:

a) ssh-keygen -t rsa

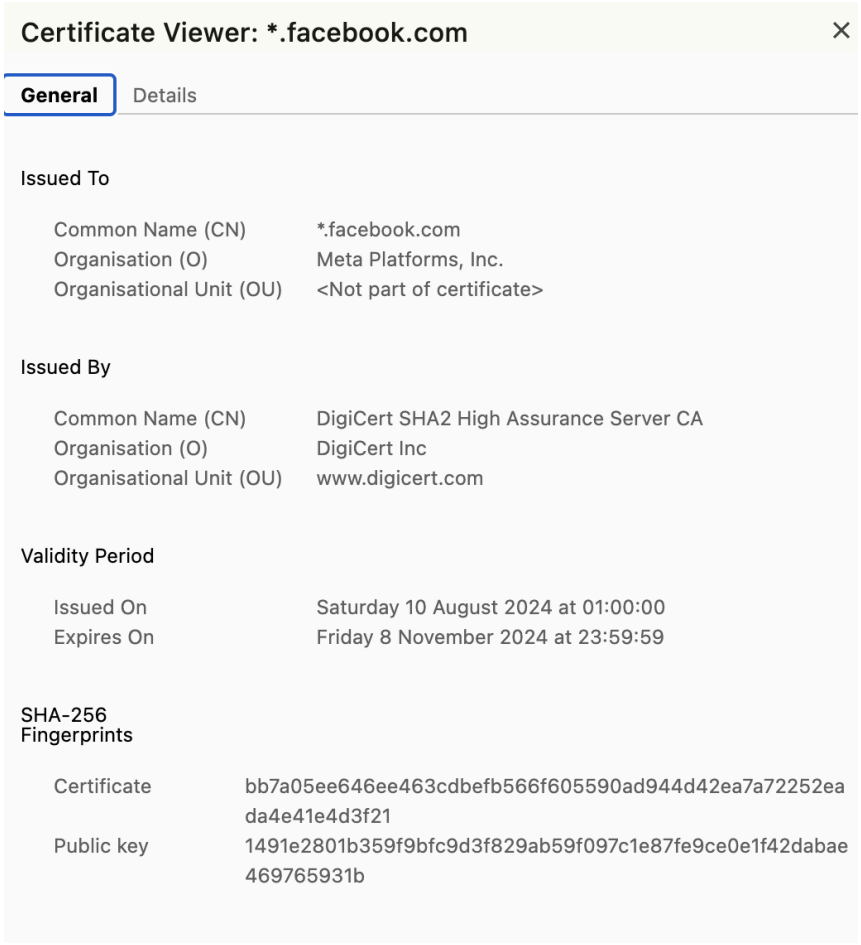
id_rsa.pub Public key
id_rsa : Private key

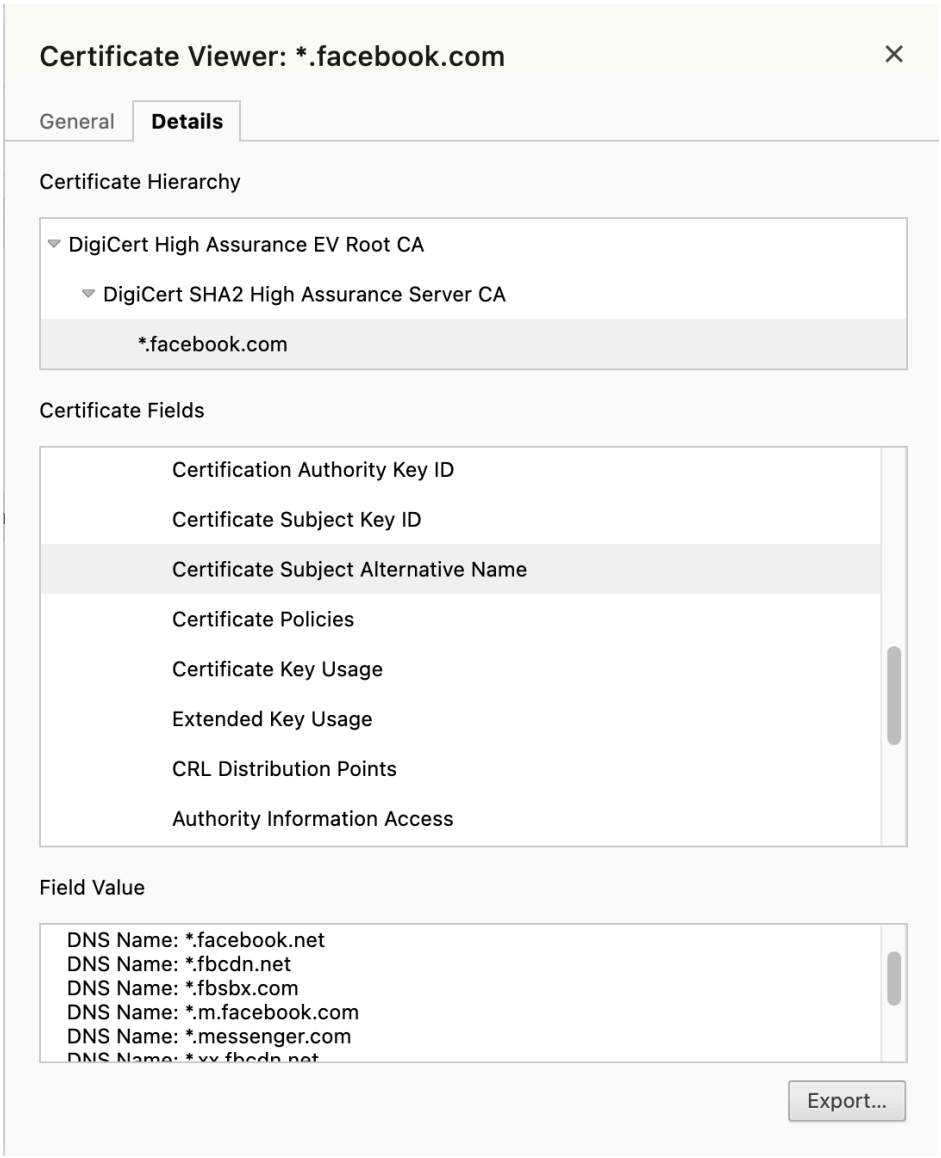
b) Store in .ssh/authorized_keys in remote server
c) Login to remote Server

28) What is an SSL certificate? What do you understand?
An SSL (Secure Sockets Layer) certificate is a ***digital file*** that verifies a website's identity and **encrypts** the connection between a user's browser and the website's server



Issued By: The CA(Certificate authority) which signs the certificate





29) What is Linux vi editor?

These are used to edit files, create new scripts ..etc

1. vi 2. nano

vi keystrokes
vi <filename>

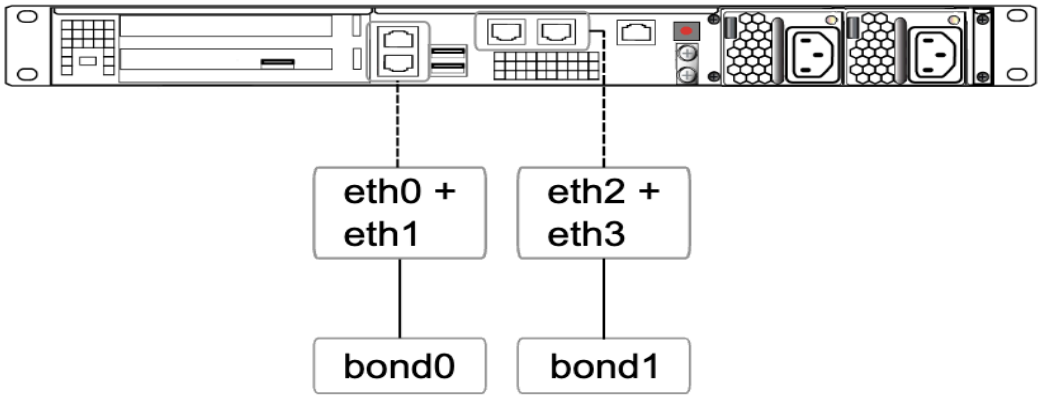
i	Switch to insert mode
:wq	Saves current work and exists
:q!	Exit without saving
x	Deletes current character
dd 5dd	Delete current Line Delete 5 Lines
YY 5YY	Copy line Copy 5 lines
p	paste
:5	Go to line number 5

30) What is Zombie process?
In Linux, a Zombie Process is also known as a dead or defunct process. It is a process that has *completed the execution, but its access remains inside the process table*. Usually, it happens because of insufficient correspondence between child and parent processes.

Effect:
Zombies do not use up your system's precious resources like a rogue app does, it can pose a *significant threat by retaining all PIDs (Process IDs).* Since a Linux system has a finite amount of PIDs, when numerous PIDs are zombied, no other process can easily be launched.

30) What is Network bonding?
Network Bonding as the name implies that it is the process of bonding or joining two or more than two network interfaces to create one

interface. It helps in improving the network throughput, bandwidth, redundancy, load balancing as in case any of the interfaces is down



31) What is Shell script

Shell Script is a script mainly written for the shell. It executes commands written in a file.

We can see some useful Bash script with scenarios

S.No	Aim	Script
32)	Input in bash	#!/bin/bash echo "Enter input" read inp echo "You have entered $inp"
33)	Set variables and execute bash commands and assign value to variable	#!/bin/bash user=$(whoami) pwd=$(pwd) dte=$(date) echo "I am $user and my current working dir is $pwd and date is $dte"

34)	Function to print a value	#!/bin/bash
		devops()
		{
		echo "This is a Test function"
		}
		echo $(devops)
		~

35)	Function
	Exit with failed status when status is 1 or failed
		#!/bin/bash
		devops()
		{
		echoo "This is test"
		}
		if devops; then
		echo "success"
		else
		echo "Failure"
		fi

36)	Pass arguments in script	#!/bin/bash t=$1 echo "Entered value is $t" ./script 5 **Output;** Entered value is 5

37)	Bash Command Status	**echo $?** - If previous command executed successfully **echo $#** It will print All positional arguments (as a single word) **echo $$** It will print process id of bash shell **echo $1** - Print first positional argument **echo $2** - Print 2nd positional argument **echo $_** - Print Last argument of previous command ./script1.sh devops test o/p will be test #!/bin/bash arg1=$1 arg2=$2 echo "1st Arg is $1 and 2nd Arg is $2" echo "Number of arguments passed is $#" echo "All positional arguments passed is $*" echo "process id of bash shell is $$" Run: ./script.sh 20 50

38)	Checks for Empty string
	
	(IF else condition)
		if [[-z $s2]]; then
		
		echo "This s empty string"
		
		else
		
		echo "This s non empty string"
		
		fi

	Equal	Equal: $s1 == $s2
39)	Find	• **Access timestamp (atime):** which indicates the last time a file was accessed. • **Modified timestamp (mtime):** which is the last time a file's contents were modified. • **Change timestamp (ctime):** which refers to the last time some metadata related to the file was changed. ctime: more explained When file ownership (usr/group) and access permission changed. When file/dir got metadata changes stat /file (show all the times of the file in a more convenient way.)
40)	Find files which was modified some days ago & other Factors	**find . -type f -mtime +20 # Modified more than 20 days ago** **find . -type f -mtime 20 # File Modified exactly 20 days ago** **find . -type f -mtime -20 # File Modified less than 20 days ago** **find . -type f -size +4G // Find files of size more than 4GB**

		find . -type f -size -4G // Find files of size less than 4GB **Find file size between30 and 40 M** **find . -size +30M -size -40M //less than 40 MB** **find /root/ -type f -name "*.txt"** **find /root/ -type f -name "*.txt" -o -name "*.py"** //or operator **find /root/ -type f -perm 0755** **find /root/ -type d -perm 0755** **find /root/ -type f ! -perm 0777** **# Find type file in /root/bash directory and change permission to 777** **find /root/bash -type f -name "*.txt" -exec chmod 777 {} \;**

41)	grep	**grep -E -w 'jenkins|vamsi' /etc/passwd** **egrep -w 'jenkins|vamsi' /etc/passwd** **grep -n jenkins /etc/passwd**
42)	Log	**grep error /var/log/cloud-init-v1.log** **grep -B 3 -A 3 error /var/log/cloud-init-v1.log** **grep -F '[xyz]' filename (FInd characters x or y or z)**
43)	List Top directories by size	du -sh /* |sort -hr|head -n 10 # List Files or directory which occupies more size in / dir
44)	awk	awk -F: '{print $1 "\t" $7}' /etc/passwd # print 1st and 7th column of /etc/passwd file
45)	sed	# Replace Or Substitute HELOO with HELO sed 's/HELOO/HELO/g' test.txt (To make changes permanently in file use -i) sed -i 's/HELOO/HELO/g' test.txt

		# Replace 2nd occurrence HELOO with HELO sed -z 's/HELOO/HELO/2' test.txt # Replace in range of lines from line num 1 till num3 sed '1,3 s/HELOO/HELO/' test.txt sed '1,$ s/HELOO/HELO/' test.txt # Delete 3rd line in file sed '3d' test.txt
46)	grep	grep -w "ec2-user" /etc/passwd|cut -d: -f6
47)	Read a File and iterate and print	#!/bin/bash while read line do echo $line done < test.txt
48)	Count Characters in a file	wc -c test.txt

49)	awk '$9==200 {print $0}' access_log	Display all lines from Apache log file if HTTP error code is 500 (9th field logs status error code for each http request):

50)	Health check of a website
	
	(curl)
		#!/bin/bash
		url=$1
		if [$# -eq 0]; then
		echo "Please enter proper input. Usage <script> <url>"
		exit 1
		else
		# Curl with max time of 3 seconds and -s is silent
		curl -m 3 -s "http://$url" > /dev/null
		#curl -m 3 -s $url > /dev/null
		if [$? -eq 0]; then
		echo "Site $url is up and running"
		else
		echo "Site $url is down"
		fi
		fi