1. lQUESTION: What is the difference between a soft and hard link?

The soft link is linked to the original file whereas the hard link is a file in its own.

|  |  |  |
| --- | --- | --- |
|  | Hard link | Soft link |
| Directory | Can be used but by superuser | Can be used |
| File system | Can’t be used across fs | Can be used across file system |
| Inode number | Hard links have the same inode | Soft links do not. |
| File deletion | Won’t affect | Will affect |
| speed | faster | slower |
| Data | Same data in source file | Only point to the filename |
|  | Backup file | Shortcut file |

* ln -s to create a soft link. Eg ln -s /home/text /home/text.sl.
* ls -li: to display links and the number b4 file owner is the number of links to that file.

A black screen with white text

Description automatically generated

1. QUESTION: How to find the location of the hard links in the system?

find / -xdev -samefile /home/vlateu/link: will display all the hard links of that file.

1. QUESTION: Port numbers.

* DNS works on 53 (the default protocol for DNS is UDP)
* NFS - 2049.
* FTP – 20, 21 on TCP
* SSH – 22
* Telnet – 23
* SMTP - 25
* DHCP – 67, 68 on UDP
* TFTP – 69 on UDP
* RDP - 3389

1. QUESTION: What is the difference between TCP and UDP?

TCP (transmission control protocol) and UDP (User datagram) are 2 of the most common transport layers used in computer networking. TCP uses a 3-way handshake to establish a connection between the source and destination device (which guarantees data transfer) whereas UDP is connectionless oriented and does not guarantee data transfer.

**A green screen with white text

Description automatically generated**

1. QUESTION: How to remove a duplicate package? Package-cleanup - -dupes
2. QUESTION: Can you explain the fields of /etc/passwd?

* The username
* Password hash
* UID
* GID
* Description
* Home directory
* Shell for user

1. QUESTION: How to enforce the user to reset the password after login? (chage -d 0 vlateu)

The chage command is used to set password aging for a specific user. If LAST\_DAY is set to 0 the user is forced to change his password on the next log on.

A screen shot of a computer

Description automatically generatedA screenshot of a computer screen

Description automatically generated

1. QUESTION: How to set a username and password to never expire? (chage -M -1 vlateu)

Passing the number -1 as MAX\_DAYS will remove checking a passwd’s validity.

1. QUESTION: How to change the user’s expiration date? Chage -E uname
2. QUESTION: How to change the user shell: usermod -s “/sbin/nologin” vlateu
3. QUESTION: How to change homedir: usermod -d “/opt/vlateu”

A screenshot of a computer code

Description automatically generated

1. QUESTION: How to change the homedir for upcoming users?

Vi /etc/default/useradd and change default home directory.

1. QUESTION: Issues faced using ssh?

* Key not found. I had to create a new key or send it at the right directory.
* User blocked from server end.
* User not allowed to use ssh
* Wrong port
* Ssh not started.
* Firewall blocking ssh
* Key permission issues.

1. QUESTION: Why /etc/passwd and /etc/shadow cannot be merged?

* /etc/passwd content users’ account information and can be read by other application to gather them. /etc/shadow content passwd hash of users and is only accessible by root. It is separate from /etc/passwd for security purposes. Merging those files together will create vulnerability in the system.

1. QUESTION: How to list open files (count files and processes) by PID? Lsof -p PID
2. QUESTION: Unable to unmount a file system. What is the reason?

* You may be in a directory of the fs you are trying to remove, so exit it.
* Some users are present in the directory and using its content; use fuser -mu /dev/sda to find out and then logout those users or send them a message to exit the directory.
* write vlateu tty1 and then send them a text message. Or pkill -u uname or pkill -U uid.
* Some of the files are open in the directory; do lsof /dev/sda7 to list open file and kill them using PID.

1. QUESTION: What could be the reason if server takes more time after reboot?

Filesystem got corrupt and its ext2 does not have journaling feature.

1. QUESTION: We are trying to create a file under any partition, but we are getting permission denied alert. What could be the reason? (it’s not a space or permission issue).

Sometimes df command report that you have available space, but you are actually out of inodes; so I will run the df -i and look at my inode utilization. If not more available inodes, I will check for unused files and delete them.

1. QUESTION: How to check routing table information?

Route -n, netstat -rn, ip route

1. QUESTION: What is sticky bit and how to set it?

It’s a special permission assigned to directories and files that grant full access to users, but only root and file owner can delete it. Chmod +t /home/vanick; chmod 1757. To make it setuid executable do chmod 4700 executable. -s setuid executable, -S not executable.

1. QUESTION: Which file is used to specify default gateway? /etc/sysconfig/network-scripts/ifcfg-enp0s3.
2. QUESTION: How to switch between 2 runlevel?

* Cat /etc/inittab to get info if you don’t remember.
* Systemctl get-default: to get the default runlevel
* Systemctl set-default graphical.target or multi-user.target.

1. QUESTION: What is NFS and its port number?

* Network File System is a protocol that allows you to set up storage locations on your network. Your users/clients treat the hard drive as if it were attached to their computer.
* Its port number is 2049.

1. Install and enable the service:

* Yum install nfs-utils
* Systemctl enable - -now nfs-server.
* Systemctl enable rpcbind - -now rpcbind (used for port mapping)

1. Set up a shared location.

* Mkdir -p /nfs/exports/myshare

1. Export the shared location by adding it to the /etc/exports file.

* /nfs/exports/myshare 192.168.122.0/24(rw,sync): With no space between network subnet and permission.

A screenshot of a computer

Description automatically generated

1. Set ownership: You want to make sure that users are allowed to read and write to the /nfs/exports/myshare. You can create a group and add them in it, and then set that group as group owner of the dir. Eg chmod root:sharegroup /nfs/exports/myshare. Chmod 770 /nfs/exports/myshare.
2. Export the exports:Update the NFS table using exportfs -a or -r
3. Configure firewall:

* Firewall-cmd - -add-service=nfs –permanent

1. Set up client:

* Mkdir -p /nfs/imports/myshare: create mount point for the NFS share.
* Mount 192.168.122.17:/nfs/exports/myshare /nfs/imports/myshare/
* Sudo mount | grep -i nfs.
* Add the fs to /etc/fstab for permanent change.

1. QUESTION: What is the nice value and how to set it? How would you increase the priority of the process?

* A nice value is a priority of the process. -20 to 19
* Nice -n 5 <command>
* Nice -n -1 pwd

1. QUESTION: What is the difference between FTP in TFTP (Trivial file transfer protocol)?

* TFTP uses port 69 on UDP, it’s lighter than FTP and doesn’t require authentication. FTP uses 20, 21 on TCP, more complex, has a lot of messages and requires authentication to access it.

1. QUESTION: How to extend a file system in linux?

* Using LVM the process is simple:
* Lvextend -L 2G -r /vg/lv-0
* Or Lvextend -l 100%free -r /vg/lv-0
* Use rezise2fs or xfs\_growfs to rezise.

1. QUESTION: How will you roll back the package after patching?

* Yum update vsftpd
* Yum history: provide your various installs and updates.
* Yum history info 8
* Yum history undo 8: to revert to previous change.

1. QUESTION: What is rsysnc and what is its syntax?

* It is a command line utility used for synchronizing files between source and destination. It is designed to minimize data transfer when synchronizing files. It achieves this by comparing the source and destination files and only transferring the differences (delta) between them. If you start sending data and there is an interruption, on the next try it will copy only the data that were not successfully sent unlike SCP.
* Rsync -cvf /data-to-copy ip-of-remote-server:/location-to-store

A screenshot of a computer screen

Description automatically generated

1. QUESTION: How to reduce the file system in linux? Fs reduction can happen online or no (no: well get the approval first)?

* Check size: df -h
* Unmount fs: umount /dev/vg/lv
* E2fsck -f /dev/vg/lv to for fs check
* Lvreduce -L 200M /dev/vg/lv
* Update the fs by Resizing it.
* Now run df -h again and mount it back.

1. QUESTION: Uptime is used to show the load average of the system. What is the meaning of its values? A load average is the amount of work (number of processes executed and, in a queue,) performed by the CPU/ system over a specified time.

A white background with blue text

Description automatically generated A white text with black text

Description automatically generated

1. QUESTION: How to set number of lines in vi? In command mode do :se nu
2. QUESTION: How to scan the disk in linux?
3. echo "- - -" > /sys/class/scsi\_host/host0/scan
4. echo "- - -" > /sys/class/scsi\_host/host1/scan
5. echo "- - -" > /sys/class/scsi\_host/host2/scan

* **c –** Channel on the HBA
* **t –** SCSI target ID
* l**–** LUN ID
* **n –** HBA number

31. QUESTION: What is /etc/fstab and explain its fields?

- it’s a file system table used to store the mounted filesystem in your server, It has 6 fields.

- the device name or fs to mount.

- the mount point.

- the FS type.

- mount option: defaults, noauto, user, owner.

- dumping 0 or 1: This is used by the dump program to determine if FS should be backup in case of corruption.

- Checking sequence: used by the fsck program to determine if FS should be checked at every reboot.

32. QUESTION: Can we create a soft link across a partition? Yes, because a soft link is just a shortcut to the partition and will have a different inode.

33.QUESTION: What is the location of NFS shared info when it’s mounted? /etc/fstab.

34.QUESTION: How to check if a particular port is open/listening to request? netstat -anp | grep 53. - a all display sockets (default: connected). - p program -n numeric

35. QUESTION: what is the difference between du and df?

-du (disk use) it iterates over a directory and tells you how much space is being occupied by each file. It may not output the exact info due to the possibility of unreadable files.

-df (disk free) provides the amount of space used, available, and free across your FS. It provides metadata of fs.

36. QUESTION: What is the concept behind journaling?

- Journaling, refers to a technique used to improve the reliability and integrity of the file system by keeping a detailed record, or "journal," of all changes and transactions that are about to be made to the file system. This journal allows for a quicker and more efficient recovery in case of system crashes, power failures, or other unexpected events.

-FS that supports journaling: ext3, ext4, xfs.

A screenshot of a computer

Description automatically generated

A blue background with white text

Description automatically generated

37. QUESTION: You try to patch a package and get an error message, what do you do?

- rpm -hiv vsftpd - -nodeps (Don’t do a dependency check before installing or upgrading a package).

38. QUESTION: Explain the booting process in Linux? See booting process document in Desktop.

The boot process in linux is divided into sequences.

1. BIOS (Basic inpout/output system)

* Runs the POST (Power On self-Test) which is a hardware diagnostic that ensures that the different hardware components are working prior to the booting process.
* It searches, loads, and executes the boot loader program (MBR). It looks for boot loader in floppy, cd-room, or hard drive. You can press F12 or F2 to change the sequence.

1. MBR (Master boot record) loads and executes the GRUB boot loader.

* It is in the 1st sector of the bootable disk (/dev/hda or /dev/sda).
* MBR is 512 Bytes and has 3 components: primary boot loader info has 446 bytes, partition table info in next with 64 bytes, and the mbr validation check in last 2 bytes.

1. GRUB Grand Unified Bootloader

* It loads and executes kernel and initrd images.
* It displays a splash screen, waits for few seconds and if you don’t interrupt it, it loads the default kernel image as specified in the /boot/grub/grub.conf file. So, this is where you specify the kernel to load. The bootloader package (Grub) has the knowledge of FS unlike LILO.

A screenshot of a computer

Description automatically generated

1. Kernel (core of the OS)

* It mounts the root FS as specified in the grub.conf file (Root=hd0…..)
* It executes the /sbin/init program. Init has a PID of 1 since it’s the 1st executed program.
* Initrd stands for initial RAM Disk (it’s temporarily used by kernel as root FS until kernel is booted and the real root file system is mounted). It also contains drivers compiled which help it to access partitions and other hardware.

1. Init

* Looks for the /etc/inittab file to decide the linux run level to boot into.
* 0 halt: used in emergency situations.
* 1- single user mode with only root allowed to be logging
* 2 multiuser modes with services disable.
* 3 multiusers with no GUI
* 5 multiuser X11
* reboot

1. Runlevel programs

* During bootup, you may see programs running or getting started, these are programs in the default runlevel.

A screenshot of a computer program

Description automatically generated

39. QUESTION: What is the meaning of PCPU and JCPU in W command?

- W: It’s a tool that allows admin to view logged in users along with uname, where they are logged from, and what they are doing. It also provides the system uptime and load average.

- JCPU is the time used by all processes attached to the user’s terminal. It doesn’t include past bg jobs.

- PCPU is the time used by the current process.

40. QUESTION: What happens when you open an URL in the browser and press enter?

1. [www.google.com](http://www.google.com)

2. DNS RESOLUTION: The browser goes in the DNS server (cache) and checks for the corresponding IP of google.com.

3. HTTP REQUEST: The browser establishes a TCP/IP connection (3way handshake) to the web server identified by the resolved IP.

- The browser sends the HTTP request to the webserver

-The webserver handles the request and looks for requested info.

- It then generates an HTTP response which includes (status code (200, 404), requested info (HTML, images), and response headers.

- 1XX Informational

- 2xx success

-3xx redirect the client to another URL

-4xx client errors

-5xx server errors

4. Display: The browser displays the HTML content.

41.QUESTION: What is the difference between RPM and YUM?

- Both RPM and YUM are used to manage (install, upgrade, and remove) packages in LINUX systems. RPM is often used for Local package management whereas YUM is a high-level package management tool built on top of RPM. YUM is used to manage repositories and can download from online repositories.

> rpm -qa | yum list installed (list installed)

> rpm -qa - -test: To check a package consistency.

> rpm -ivh | yum install.

42. QUESTION: WHAT IS ACL, HOW TO SET?

ACL is an extended permission used to grant access to a specific user or group over a component. Use setfacl to set and getfacl to check the permission -x removes an ACL.

43. QUESTION: What is an Inode?

An inode is a unique identifier of files and directories on the hard drive that contains metadata (size, type, ownership, permissions, timestamps, pointers to data blocks on disk).

44. QUESTION: Can you schedule 2 seconds in crontab? No, we can schedule a minute or more.

45. QUESTION: HOW TO CHECK WHO REBOOTED THE SERVER?

- last reboot | less or go into the /var/log/messages,syslog,dmesg.

46. QUESTION: How to extract a single file tar archive? tar -xvft abc.tar

47. QUESTION: Check memory space? Free -m, free -g

48. QUESTION: Command to check architecture in linux? uname -a, arch.

49. QUESTION: How to search text within multiple files? Grep search across a file and display the line that contains the specified Partain whereas find searches for a file and display its patch.

-find . -type f -name/iname “\*.logs” -exec grep ‘error’ {} \;

-iname: remove sensitivity

- mmin 10: File’s data was last modified 10 minutes ago.

-mtime +20: File’s data was last modified 20 hours ago.

-ctime +3: When the inode / permission attribute of the file was modified.

-size +5M: files over 5mb

- empty

- perm 777

50. QUESTION: How to delete logs that are 30 days older?



# find /var/log -name “messages\*” -mtime +3 -exec rm -f {} \; This will iterate over the /var/log/ directory, look for and delete any file that start with messages and that the content was modified 3 days ago. There is a space between {} AND \.

51. QUESTION: How to delete logs whose ownership changed 45 min before from root to dif user?

A white background with blue text

Description automatically generated

52. QUESTION: User is running ls-l command in server, but he is not getting any output. What could be the issue?

- The FS may have been corrupted so I will recommend unmounting it and perform and FS check using fsck. - umout /dev/fs; fsck /dev/fsck

53. QUESTION: What is a run queue and which command is used to check the run queue? List of processes waiting to be executed. Use the *SAR* command to check it. *Sar -q 1* (will refresh every second). Yum install sysstat.

54. QUESTION: Which file is used to change the default runlevel? /etc/inittab.

55. QUESTION: What is the difference between yum update and yum upgrade? They are both used to install the latest version of your packages, but yum upgrade will delete the obsolete version whereas update will not.

56. QUESTION: What is a file system? A file system is a method used by computer operating systems to organize, store, and manage files and data on storage devices, such as hard drives, solid-state drives, optical discs, and network shares.

58. QUESTION: How to list directory inside a directory by using find command?

- ls -d \*/ - find . -maxdepth 1 -type d

59. QUESTION: What is the difference between .tar and .gz? .tar is used to archive (organize the content in a same file) whereas .gz is used to compress (reducing the size of the file).

# tar -zcvf archive.tar.gz /file-to-archive-and-compress.

60. QUESTION: Timeout error prompt when trying to use telnet; what is the reason? Ensure that the telnet daemon is started and enabled; check connection between server and client using ping, ensure firewall is not blocking the connection or selinux; ensure you are using the right port.

61. QUESTION: What is a RAID and how did you create it?

62. QUESTION:

A table with text on it

Description automatically generated

63. QUESTION: Can we build a server without creating a swap partition? If possible, what could be the consequence? Yes, we can. Slowness of system in case RAM is full.

64. QUESTION: **DF command says your /opt is full, but you have deleted 10gb of files recently. What could be the reason and how will you troubleshoot? I will use lsof to list the opened files and grep the dir/file, locate its PID and kill it.**

65. QUESTION: Why do we use IP instead of MAC addresses? IP is a logical address whereas MAC is a physical address. IP (Internet Protocol) addresses and MAC (Media Access Control) addresses serve different purposes in networking, and they are used at different layers of the networking stack.

66. QUESTION: What is the difference between incremental and differential backup? Incremental only backs up the data that has changed since the previous backup whereas differential will backup data that has changed since the last full backup. During recovery, differential backup takes less time compared to incremental backups. Incremental backups will have less data compared to differential.

67. QUESTION: list opened files, and opened files by a specific PID?

# lsof, lsof -p pid, lsof -p pid | wc -l (list number of files opened by that PID).

68. QUESTION: How to find out port number used by daemon? Lsof -i -P | grep 4271.

69. QUESTION: How to troubleshoot I/0 related issues?

A screenshot of a computer

Description automatically generated

70. QUESTION: Which command can be used to display system summary information and current utilization? Which tool is used to see cpu, memory, nice value, zombie processes and more? Top.

71. QUESTION: How to display process details for specific user? Top -u root.

72. QUESTION: How to kill a process using top? Run the top command and press k, enter the PID.

73. QUESTION: How to find out the PID and process details of application? Ps -ef | grep <app name>. commonly used to check the status of the process.

74. QUESTION: How to kill a process? Kill -9 immediately kills a process whereas kill -15 is graceful kill.

75. QUESTION: How to troubleshoot network issues? You can use tcpdump to capture network packages and analyze the number received, dropped and so on.

- tcpdump -i enp0s3 -w /tmp/capture. Tcpdump -r to read the content of the capture.

76. QUESTION: How to capture traffic between src and destination IP? 

-tcpdump scr 192.162.0.2 and dst 192.178.2.9

77. QUESTION: How to capture network traffic from destination port? Tcpdump dst port 443.

78. QUESTION: How to diagnose performance issues related to storage devices?

A close up of text

Description automatically generated

Iostat -d: to display I/0 statistic of disks.

Iostat -c: to display cpu utilization average. If you have multiple apps running, the idle time will drop.

79. QUESTION: If a program is not starting due to dependencies not available, what do you do? I will run the ldd command to find out the shared libraries it is looking for.

Ldd – prints shared libraries dependencies.

80. QUESTION: How to show statistics of all protocols? Netstat (Network Statistics) is a popular command to print network connections, interface statistics and to troubleshoot various network related issues.

# netstat -s | grep error. To get potential error messages.

A screenshot of a computer

Description automatically generated

81. QUESTION: HOW to see kernel routing table? Netstat -r

1. What is the difference between hard links and soft links?  
Answer: Hard links point directly to the inode of a file, while soft links (or symbolic links) are separate files that contain the path to the target file.  
  
2. Explain the significance of the 'root' user in Linux.  
Answer: The 'root' user is the superuser with administrative privileges. It has the highest level of access and can perform any operation on the system.  
  
3. How do you find all files modified in the last 10 minutes in a directory and its subdirectories?  
Answer: Use the find command: find /path/to/directory -mmin -10.  
  
4. What is a kernel in Linux?  
Answer: The kernel is the core of the operating system that manages hardware resources and provides essential services for other parts of the system.  
  
5. Explain the purpose of the 'chmod' command.  
Answer: 'chmod' changes the permissions of a file or directory. It can add or remove read, write, and execute permissions for the owner, group, and others.  
  
6. How can you find out the current runlevel of a Linux system?  
Answer: Use the runlevel command: runlevel.  
  
7. Explain the role of the 'grep' command in Linux.  
Answer: 'grep' is used for searching text patterns in files. It can search for patterns using regular expressions and display matching lines.  
  
8. What is the purpose of the 'df' command?  
Answer: 'df' displays information about disk space usage on the filesystem.  
  
9. Explain the 'ps' command and how it is used to view processes.  
Answer: 'ps' shows information about currently running processes. Common options include ps aux to display detailed information about all processes.  
  
10. How do you change the priority of a process in Linux?  
Answer: Use the nice command to run a process with a specified priority. For example, nice -n 10 command sets a lower priority.  
  
11. What is the purpose of the 'awk' command?  
Answer: 'awk' is a versatile text processing tool that performs pattern scanning and text extraction. It is often used for data manipulation and reporting.  
  
12. Explain the role of the 'tar' command in Linux.  
Answer: 'tar' is used for creating and extracting archive files. It bundles multiple files into a single archive file and can compress the archive using various algorithms.  
  
13. How can you check the connectivity between two hosts using the 'ping' command?  
Answer: Use the ping command followed by the target IP or hostname: ping <target>.  
  
14. What is a cron job, and how do you create one?  
Answer: A cron job is a scheduled task in Linux. To create one, use the crontab -e command and add an entry specifying the schedule and the command to be executed.  
  
15. Explain the purpose of the 'iptables' command.  
Answer: 'iptables' is used for configuring the Linux kernel's netfilter firewall. It can filter, modify, or redirect network packets.