Linux Admin Interview Simulation Test

🧠 Section A – Theory & Conceptual (8 Questions)

1. Explain the Linux file system hierarchy. What is stored under `/etc`, `/var`, and `/usr`?
    - /etc – it stores the files related to users authentication and passwords and logs related to the users logins
    - /var – it stores program files and the log files related to the program
    - /usr – they store the files related to the program libraries, data files and the user related programs
2. What is the difference between a soft link and a hard link? When would you use each?
    - Softlinks are those which are not linked with the inode and they create an links between the files when the main files are deleted the links are also deleted [ln -s filename]
    - Hardlinks are those which are linked to the inode and they are created the links between the files and the when the file are deleted the links stays on because they are related to thee inode [ln filename]
3. How do Linux file permissions work? Explain rwx with numeric and symbolic examples.
    - Chmod , chown , chgrp are the permissions used to allocate the permissons to the files present in the user machine
    - Rwx – read , write , execute
    - Chmod 755 filename
    - Chmod a+x filename – allocate executable to all files present
4. What is the difference between `cron` and `at`? When would you use each?
    - Cron is used to schedule task automation on an daily basis and also on an repeated way
        - Crontab -e
        - 00 5 16 7 * echo "command for cron ">> cron_output
    - At command is used to allocate task at an single time
        - at [time]
        - now give the command shutdown -r now
        - ctrl + D to save and exit
5. What is the role of `/etc/passwd`, `/etc/shadow`, and `/etc/group`?
    - /etc/passwd – its is used to store the users' passwords and authentications, its stores the users ID, group ID
    - /etc/shadow – same as /etc/passwd but at a highest enhanced level
    - /etc/group – they are used to store the information about the user groups

6. Compare yum vs rpm. Which one would you prefer for automated updates and why?
    - Yum and rpm both are an package manager used to download and check for libraries that are present in the machine
    - Rpm or also known as the redhat package manager where they are an low tier package manager where installing, updating and deleting are possible but handling dependencies are not possible for automation purpose this is not possible
    - Rather than rpm we can use yum where all the dependencies handling are also done so for automation purpose, we can use yum instead of rpm
7. What are wildcards in Linux? Provide 3 examples of file selection using them.
    - Wildcards are mostly used for the purpose of finding removing files easily in a file of in a directory using strings or patterns
    - For example :
    - rm -rf *abc – deleting the files that are ending with the words abc in the path
    - and take this , an path containing different types of file structure like txt, sh and etc and you want to filter out only the txt files then we can use the command - [ls *.txt]
8. Explain the difference between SSH and Telnet. Why is SSH preferred in production?
    - Ssh and telnet are both used for remote access and machine access
    - But for production we don’t use telnet because they don’t give secured hosting and also don’t help is managing data breaches
    - But ssh overlay with many secured ways of hosting the machine by using password , IP address , user name , key pairs and etc and they help in managing data breaches using ACL

🧪 Section B – CLI Practical Tasks (7 Questions)

1. List all files larger than 100MB in /home, compress them, and move to /tmp/archive.
2.
3. Find and display the total number of .log files inside /var/log, and their combined size.

    - Find /var/log -type f -name “.log” -exec du -ch {} + | grep total

4. Create a group devops, add user testuser to it, and verify group membership.

    - groupadd <devops>
    - useradd <testuser>
    - usermod -aG <devops> <testuser>

5. Using netstat, show all ports listening on the system. Save output to /tmp/ports.txt.

    - Touch /tmp/ports.txt
    - netstat > /tmp/ports.txt
    - next time you want to save the output then you can just append the output to the file - >>

6. Extract all failed login attempts from the past 24 hours using journalctl or /var/log/secure.

    - journalctl –since “24 hours ago” -COMM=sshd | grep “Failed Password” | wc -l

7. Use vi to create a file named report.txt, write a 3-line summary, and save the file.

    vi report.txt

    click I to insert and then – hello my name is omega

    I am here to learn linux

    I will succeed in it

    Now click esc and then :wq! To write and quit from the file

---

💼 Section C – Real-Time Interview Scenarios (5 Questions)

1. A developer cannot SSH into the test server but the system is up. How would you troubleshoot?

    - First check whether the sshd service is running or not – systemctl command
    - Then check for the error message – ssh developer@hostname or ip add
    - In the machine just check whether the port number is listening using ths command netstat -tulnp | grep :22
    - Check the firewall permissions – firewall -cmd --list-all and check they have allowed for the port number 22 to be listened in the firewall
    - Check the logs for the error - tail -f /var/log/secure
    - Check whether the userID is there or exist in the /etc/passwd

2. Your root disk is full. How would you find and clean up large files safely?

    - Use the du -h | head -n 5 to list the top 5 big files
    - Now we can analyse and delete the unwated files
    - We can clear or all the libraries cache files
    - We can check these paths for the cache files var/cache , /tmp , /var/tmp files to clear of unwanted cache file s
    - To find the files that are larger than 100 mb in these paths we can use the find command
        - find /var/cache /tmp /var/tmp -type f -size +100M -exec ls -lh {} \; | awk '{print $9 " : " $5)
    - clean the package managers - yum clean all
    - find the biggest directory in the root
        - du -h –max-depth=1 /var | sort -hr | head -n 10

3. A user accidentally deleted a file. There was a hard link to it in another location. What do you do?

    - First the method to create an hard link for an file is :
        - Ln hardlinknew filename
        - So this is the name of the hard link created
    - So when you delete the original file then the hard link will still remain
    - So we can just copy the file from the hardlink
    - cp hardlinknew filename

4. After rebooting the system, Apache doesn't start automatically. How do you fix it?

    - First the check the status of the service that is present apache
    - systemctl enable apache – this enables the service across the machine
    - just if you want to start the service immediately the systemctl start service_name

5. An update failed and now yum is broken. What are your steps to restore or roll back?

    - Yum install service
    - Now check the yum history and not the id that you want to rollback
    - Yum history undo <ID>

⚙️ Section D – Shell Scripting Challenges (5 Questions)

1. Write a script that checks if the sshd service is running. If not, restart and log to /var/log/sshd_watch.log.

```
#!/bin/bash

    clear

    LOGFILE="var/log/servicelogcheck.log"

    TIMESTAMP=$(date %y-%m-%d %H-%M-%S)

    if systemctl is-active --quite sshd; then

        echo "[TIMESTAMP] the service is active" >> $LOGFILE

    else

        echo "[TIMESTAMP] the service is not active" >> $LOGFILE

        systemctl restart sshd

        if --is-active --quiet sshd; then

            echo " [TIMESTAMP] the system restarted " >> $LOGFILE

        else

            echo "[TIMESTAMP] the system is not restarted " ?? $LOGFILE

        fi

    fi
```

2. Write a script to accept a directory path and return the number of .conf files in it.

```
#!/bin/bash

        clear

        TIMESTAMP=$(date %y-%m-%d %H-%M-%S)
```

```
CONFFILECOUNT="/var/tmp/countconf.txt"

read -p "enter the directory path " DIRECTORYPATH

COUNTCONF=$(find $DIRECTORYPATH -type f -name "*.conf" | wc -l)

echo "[TIMESTAMP] the number of conf files in $DIRECTORYPATH is $COUNTCONF" >> $CONFFILECOUNT
```

3. Schedule a script using cron to monitor disk usage every hour. If usage exceeds 85%, log a warning.

DISKUSAGE.SH

```
#!/bin/bash

clear

TIMESTAMP=$(date %y-%m-%d %H-%M-%S)

DISKEXCEEDSTORAGE="/var/tmp/diskusagealeart.log

DISKCOMMAND=$(df-h| awk '$5 >=85)

if[ ! -z '$DISKCOMMAND' ]; then

        echo " [TIMESTAMP] the disk exceed the limit" >> $DISKEXCEEDSTORAGE

        echo "$DISKCOMMAND" >> $DISKEXCEEDSTORAGE

fi
```

```
chmod a+x /path/to/ssh/diskusage.sh
```

now create a cron command

```
crontab -e

0 * * * * /path/to/ssh/diskusage.sh
```

4. Write a script that lists top 5 largest files in /var/log and stores the output in /tmp/largest_logs.txt.

```
#!/bin/bash

clear

TIMESTAMP=$(date %y-%m-%d %H-%M-%S)

OUTPUT="/tmp/largest_logs.txt"

echo "[TIMESTAMP] The top 5 largest files to be listed " >> $OUTPUT

find /var/log -type f -exec du -h {} + 2/dev/null | sort | head -n 5 >> $OUTPUT

echo "[TIMESTAMP] thee report is saved at this time " >> $OUTPUT
```