Linux Administration – Scenario Based Questions and Solutions

1) List out 5 files in your system which are consuming the most disk space

Objective: Identify the largest files/directories on the system to understand disk usage.

Command: sudo du -ah / | sort -rh | head -n 5

Explanation: The du command checks disk usage. The -a option includes files, -h makes sizes human-readable. The output is sorted in reverse order by size, and the top 5 largest entries are displayed. Starting from the root directory ensures system-wide coverage.

2) Create a common folder where anyone can create files but cannot delete other users' files

Objective: Allow shared usage while preventing accidental or malicious deletion.

Commands: sudo mkdir /common sudo chmod 1777 /common

Explanation: The permission 1777 enables read, write, and execute access for everyone and sets the sticky bit. The sticky bit ensures that only the owner of a file (or root) can delete it. This is the same permission model used by /tmp.

Verification: ls -ld /common

3) Create user "shubham" and add him to group "adm"

Commands: sudo useradd shubham sudo usermod -aG adm shubham

a) Create /data directory and set ownership to root:adm

Commands: sudo mkdir /data sudo chown root:adm /data

b) Allow users to write and ensure files inherit group ownership

Command: sudo chmod 2775 /data

Explanation: The setgid bit (2) ensures that files created inside /data inherit the group ownership (adm). Users in the adm group can write to the directory, and all files maintain consistent ownership.

Expected output example: -rw-rw-r-- root adm test.txt

4) Create user "nikhil" with specific account policies

Create user with home directory and shell: sudo useradd -m -d /home/nikhil -s /bin/sh nikhil

Set password and expiry policies: sudo passwd nikhil sudo chage -M 9 -W 2 -E $(date -d "+30 days" +%F) nikhil

Explanation: The password expires every 9 days, a warning is shown 2 days before expiry, and the account itself expires after one month.

c) Allow user nikhil to start and stop cron daemon only

Command: sudo visudo

Entry to add: nikhil ALL=(root) /bin/systemctl start cron, /bin/systemctl stop cron

Explanation: This grants limited root privileges for controlling only the cron service, following the principle of least privilege.

4.1) Set /nikhil as home directory for user nikhil

Commands: sudo mkdir /nikhil sudo chown nikhil:nikhil /nikhil sudo usermod -d /nikhil nikhil

Verification: getent passwd nikhil

List the highest priority process in the system

Command: ps -eo pid,comm,ni --sort=ni | head

Explanation: Processes with lower nice values have higher priority. A nice value of -20 is the highest priority.

5) Pause and resume vmstat using signals

Terminal 1: vmstat 1

Terminal 2: ps aux | grep vmstat

Pause vmstat: kill -STOP <PID>

Resume vmstat: kill -CONT <PID>

Explanation: SIGSTOP pauses the process, and SIGCONT resumes it without terminating execution.

6) Find process in waiting (sleep) state

Command: ps -eo pid,comm,state | grep D

Explanation: Processes in state D are in uninterruptible sleep, typically waiting for I/O operations to complete.

7) Add additional swap space permanently

Commands: sudo dd if=/dev/zero of=/swapfile bs=1M count=1024 sudo chmod 600 /swapfile sudo mkswap /swapfile sudo swapon /swapfile

echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab

Verification: swapon --show free -h

Explanation: This creates a 1GB swap file and ensures it remains active after reboot by updating /etc/fstab.

8) Find number of processes in run queue and blocking queue

Command: vmstat 1

Explanation: The r column shows processes waiting for CPU (run queue), and the b column shows processes blocked due to I/O wait.

End of Document