Linux Scenario Based Questions for Interview

User Management: A user complains they cannot log in. How will you troubleshoot?

Answer:

- Check if the account is locked: passwd -S username or chage -l username
- Verify account expiry: chage -l username
- Check /etc/passwd and /etc/shadow for account details
- Review authentication logs: /var/log/auth.log or /var/log/secure
- Test password reset: passwd username
- Check home directory permissions and existence
- Verify SSH configuration if remote login
- Check disk space on /home and /tmp
- Test with su - username from root

2. File Permissions: A script is executable by one user but not another. How do you resolve this?

Answer:

- Check current permissions: ls -l scriptname
- Check file ownership: ls -l scriptname
- Add execute permission: chmod +x scriptname or chmod 755 scriptname
- Change ownership if needed: chown user:group scriptname
- Check parent directory permissions
- Verify user is in correct group: groups username
- Check if file system is mounted with noexec option
- Use sudo -u username ./script to test execution

3. Process Management: A service is consuming 100% CPU. How will you find and fix it?

Answer:

- Identify the process: top, htop, or ps aux --sort=-%cpu
- Get detailed process info: ps -ef | grep processname
- Check process tree: pstree -p PID
- Analyze with: strace -p PID (system calls)
- Lower priority: nice -n 19 command or renice 19 PID

- Kill if necessary: kill PID or kill -9 PID
- Restart the service: systemctl restart servicename
- Check service logs: journalctl -u servicename
- Monitor resource usage: iotop, iftop

4. SSH Issues: You cannot SSH into a remote machine. How do you debug?

Answer:

- Test basic connectivity: ping hostname
- Check if SSH port is open: telnet hostname 22 or nmap -p 22 hostname
- Try verbose SSH: ssh -v username@hostname
- Check SSH client config: ~/.ssh/config
- Verify SSH keys: ssh-keygen -l -f ~/.ssh/id_rsa.pub
- Check server SSH logs: /var/log/auth.log
- Verify SSH daemon is running: systemctl status sshd
- Check SSH configuration: /etc/ssh/sshd_config
- Test with password if key fails: ssh -o PreferredAuthentications=password

5. Disk Space Full: / partition is full. How do you find and delete large files safely?

Answer:

- Check disk usage: df -h
- Find largest directories: du -sh /* | sort -hr
- Find large files: find / -type f -size +100M -exec ls -lh {} \;
- Clean temporary files: rm -rf /tmp/* and /var/tmp/*
- Clean logs: journalctl --vacuum-time=7d
- Clear package cache: yum clean all or apt clean
- Check for deleted but open files: lsof +L1
- Remove old kernels: package-cleanup --oldkernels --count=2
- Clean user trash and browser cache

6. File Corruption: A log file is showing junk characters. How will you check and recover it?

Answer:

- Check file encoding: file filename
- Try different character sets: iconv -f ISO-8859-1 -t UTF-8 filename
- Check for binary data: hexdump -C filename | head

- Verify file integrity: md5sum filename (if original checksum available)
- Check file system: fsck /dev/device
- Restore from backup if available
- Check if file is actively being written: lsof filename
- Try to salvage readable parts: strings filename > recovered.log
- Stop the service writing to it: systemctl stop servicename

7. Crontab Not Running: A scheduled job is not executing. How do you debug?

Answer:

- Check if cron daemon is running: systemctl status crond
- View user's crontab: crontab -l
- Check cron logs: /var/log/cron or journalctl -u cron
- Verify cron syntax: Use online cron validators
- Test the command manually in shell
- Check script permissions and paths
- Ensure full paths in cron commands
- Check environment variables: env in cron vs shell
- Verify user has cron access: /etc/cron.allow and /etc/cron.deny

8. Package Installation Failing: yum or apt is failing. How will you resolve it?

Answer:

- Check repository configuration: /etc/yum.repos.d/ or /etc/apt/sources.list
- Update package database: yum update or apt update
- Check network connectivity to repositories
- Clear package cache: yum clean all or apt clean
- Check disk space: df -h
- Resolve dependency conflicts: yum deplist package or apt-cache depends
- Try force reinstall: yum reinstall or apt --reinstall install
- Check for held packages: apt-mark showhold
- Use alternative package managers: dnf instead of yum

9. User Cannot Sudo: A user was added to sudoers, but sudo still doesn't work. What could be wrong?

Answer:

- Check sudoers file syntax: visudo -c
- Verify user is in sudo group: groups username
- Check sudoers file: cat /etc/sudoers
- Look for user-specific rules: /etc/sudoers.d/
- Test sudo access: sudo -l -U username
- Check for typos in username or permissions
- Verify user session: logout and login again
- Check if sudoers file is corrupted
- Use pkexec visudo if sudo is completely broken

10. Kernel Panic: How do you troubleshoot and recover from a kernel panic?

Answer:

- Boot from rescue/recovery media
- Check kernel panic message from console or /var/log/messages
- Boot with previous working kernel from GRUB menu
- Check hardware: memory test, disk check
- Verify recent kernel updates: rpm -qa kernel or dpkg -l linux-image*
- Check for hardware compatibility issues
- Boot in single-user mode: add single to kernel parameters
- Rollback recent changes or updates
- Check disk space and file system integrity
- Update initramfs: dracut -f or update-initramfs -u

11. Zombie Processes: How do you identify and remove zombie processes?

Answer:

- Identify zombies: ps aux | grep '<defunct>' or ps -eo stat,pid,ppid,comm | grep '^Z'
- Check parent process: ps -ef | grep PPID
- Kill parent process: kill PPID (zombies will be inherited by init)
- Use signal to parent: kill -CHLD PPID
- Restart parent service if possible
- Check system load: uptime
- Monitor with: top (look for 'Z' state)
- Prevent by fixing parent process to properly handle SIGCHLD

- Reboot as last resort if system becomes unstable

12. Too Many Open Files Error: How do you fix "Too many open files" in Linux?

Answer:

- Check current limits: ulimit -n and ulimit -Hn
- Check system-wide limits: /proc/sys/fs/file-max
- Increase user limits in /etc/security/limits.conf:

text

```
username soft nofile 4096

username hard nofile 8192
```

- Check current open files: lsof | wc -l
- Find processes with most open files: lsof | awk '{print $2}' | sort | uniq -c | sort -nr
- Restart services after changing limits
- Check application configuration for connection pools
- Modify systemd service limits if needed

13. Finding and Killing Processes: A process is causing high memory usage. How do you locate and stop it?

Answer:

- Find memory-heavy processes: ps aux --sort=-%mem | head
- Use top/htop: top then press 'M' to sort by memory
- Get detailed memory info: cat /proc/PID/status
- Check memory maps: pmap PID
- Kill gracefully: kill PID
- Force kill if needed: kill -9 PID
- Kill by name: pkill processname
- Kill all user processes: pkill -u username
- Monitor system memory: free -h and vmstat

14. Home Directory Missing: A user's home directory is missing. How will you restore it?

Answer:

- Check if user exists: id username
- Create home directory: mkdir /home/username
- Copy skeleton files: cp -r /etc/skel/. /home/username/

- Set ownership: chown -R username:username /home/username
- Set permissions: chmod 755 /home/username
- Update user's home in passwd: usermod -d /home/username username
- Restore from backup if available
- Check if home is on different partition: mount | grep home
- Verify user can login and access files

15. Time Sync Issues: The server time is incorrect. How do you fix NTP sync?

Answer:

- Check current time: date and timedatectl
- Check NTP service: systemctl status ntp or systemctl status chronyd
- Check NTP servers: ntpq -p or chrony sources
- Manual time sync: ntpdate pool.ntp.org
- Configure NTP: /etc/ntp.conf or /etc/chrony.conf
- Set timezone: timedatectl set-timezone America/New_York
- Enable NTP: timedatectl set-ntp true
- Restart NTP service: systemctl restart ntp
- Check hardware clock: hwclock --show

16. Finding Recently Changed Files: How do you find all files modified in the last 10 minutes?

Answer:

- Use find command: find /path -type f -mmin -10
- For specific directory: find /var/log -mmin -10
- Include access time: find /path -type f -amin -10
- Show detailed info: find /path -type f -mmin -10 -ls
- Exclude certain directories: find /path -type f -mmin -10 -not -path "*/proc/*"
- Sort by modification time: find /path -type f -mmin -10 -exec ls -lt {} +
- Monitor real-time changes: inotifywatch /path

17. Deleting Large Files But Space Not Freeing Up: What could be the reason?

Answer:

- Check for open file handles: lsof +L1 (deleted but still open files)
- Find processes holding deleted files: lsof | grep deleted
- Restart services holding the files: systemctl restart servicename

- Check if files are hard-linked: ls -li filename
- Verify you deleted from correct partition: df -h
- Check for hidden files: ls -la
- Empty trash/recycle bin
- Check if deletion was successful: ls -l filename
- Kill processes holding the file handles: kill PID

18. Checking System Load: How do you analyze high system load issues?

Answer:

- Check load average: uptime and w
- Monitor with top/htop: top or htop
- Check I/O wait: iostat -x 1
- Monitor disk activity: iotop
- Check memory usage: free -h and vmstat
- Network monitoring: iftop or nethogs
- Check for CPU-bound processes: ps aux --sort=-%cpu
- System activity: sar -u 1 10
- Check for swap usage: swapon -s

19. NFS Mount Issues: How do you troubleshoot an NFS mount not working?

Answer:

- Check NFS services: systemctl status nfs-server rpcbind
- Test NFS server connectivity: showmount -e nfs-server
- Check exports: cat /etc/exports
- Verify mount command: mount -t nfs server:/path /mnt/point
- Check network connectivity: ping nfs-server
- Test RPC services: rpcinfo -p nfs-server
- Check firewall rules: iptables -L or firewall-cmd --list-all
- Check NFS logs: /var/log/messages
- Verify permissions on export directory
- Try different NFS versions: mount -t nfs -o vers=3

20. Hostname Resolution Issues: ping is working, but ssh is failing by hostname. Why?

Answer:

- Check DNS resolution: nslookup hostname or dig hostname
- Check /etc/hosts file for hostname entries
- Check /etc/nsswitch.conf for name resolution order
- Test reverse DNS: dig -x IP_ADDRESS
- Check SSH configuration: /etc/ssh/sshd_config (UseDNS setting)
- Try SSH with IP instead: ssh user@IP_ADDRESS
- Check if IPv6 is causing issues: ssh -4 user@hostname
- Verify hostname matches certificate if using SSH keys
- Check SSH client configuration: ~/.ssh/config

21. How do you extend a partition without unmounting it?

Answer:

- For LVM volumes:

bash

```
lvextend -L +10G /dev/vg/lv
resize2fs /dev/vg/lv  # for ext2/3/4
xfs_growfs /mount/point  # for XFS
```

- Check current size: df -h and lsblk
- Extend physical volume first if needed: pvextend /dev/sda1
- For non-LVM: Use growpart utility
- Verify file system type: mount | grep partition
- Online resize for ext4: resize2fs /dev/device
- For XFS: xfs_growfs /mount/point
- Check after extension: df -h

22. What steps are needed to add a new disk to a Linux server?

Answer:

- Physical connection and detection: lsblk or fdisk -l
- Partition the disk: fdisk /dev/sdX or parted /dev/sdX
- Create file system: mkfs.ext4 /dev/sdX1
- Create mount point: mkdir /mnt/newdisk
- Mount temporarily: mount /dev/sdX1 /mnt/newdisk
- Add to fstab: echo "/dev/sdX1 /mnt/newdisk ext4 defaults 0 2" >> /etc/fstab

- Test fstab: mount -a
- Set permissions: chmod 755 /mnt/newdisk
- Verify: df -h and lsblk

23. How to check which processes are writing to a file in real time?

Answer:

- Use lsof: lsof filename
- Monitor file access: lsof +f -- filename
- Use inotify: inotifywait -m filename
- Check with fuser: fuser -v filename
- Monitor directory: inotifywait -m -r /path/to/directory
- Use strace on process: strace -e write -p PID
- System-wide monitoring: iotop -o
- Check file locks: lslocks
- Monitor with auditd: auditctl -w /path/to/file -p wa

24. How to recover a deleted file in Linux?

Answer:

- Stop writing to the disk immediately
- Check if file is in trash: ~/.local/share/Trash/
- Use file recovery tools:
  - testdisk and photorec
  - extundelete for ext3/4
  - debugfs for ext2/3/4
- Check for recent backups
- Look for temporary copies: /tmp, /var/tmp
- Check application-specific recovery:
  - Database logs
  - Editor backup files
- Use grep to search for file content in raw disk
- Restore from system snapshots if available

25. How to check disk I/O performance in Linux?

Answer:

- Use iostat: iostat -x 1 5
- Monitor with iotop: iotop -o
- Check with sar: sar -d 1 10
- Use dd for testing: dd if=/dev/zero of=testfile bs=1M count=1000
- hdparm for disk tests: hdparm -t /dev/sdX
- Use fio for comprehensive testing:

bash

```
fio --name=randwrite --ioengine=libaio --bs=4k --rw=randwrite --size=1G
```

- Check disk usage: df -h and du -sh
- Monitor system load: uptime
- Use atop for detailed monitoring

26. A directory is taking too much space. How do you analyze it?

Answer:

- Check directory size: du -sh /path/to/directory
- Find largest subdirectories: du -sh /path/* | sort -hr
- Recursive analysis: du -ah /path | sort -hr | head -20
- Use ncdu for interactive analysis: ncdu /path
- Find large files: find /path -type f -size +100M -exec ls -lh {} \;
- Check hidden files: du -ah /path/.[^.]* | sort -hr
- Use tree command: tree -h /path
- Find old files: find /path -type f -mtime +30 -ls
- Check for duplicate files: fdupes -r /path

27. How do you remount a filesystem in read-write mode without rebooting?

Answer:

- Remount as read-write: mount -o remount,rw /mountpoint
- Check current mount options: mount | grep mountpoint
- For root filesystem: mount -o remount,rw /
- Check file system errors first: fsck /dev/device (if safe)
- Verify no processes are using it: lsof +f -- /mountpoint
- Check fstab entry: grep mountpoint /etc/fstab
- Force remount if needed: mount -o remount,rw,force /mountpoint

- Verify successful remount: mount | grep mountpoint
- Check write permissions: touch /mountpoint/testfile

28. What happens when a file is deleted but is still in use by a process?

Answer:

- File descriptor remains open in process
- Disk space is not freed until process closes file or terminates
- File becomes "deleted" but still accessible to the process
- Check with: lsof +L1 (shows deleted files still open)
- File appears as "(deleted)" in lsof output
- Process can continue reading/writing to the file
- To free space: kill the process or restart it
- Check which process: lsof | grep deleted
- File will be completely removed when last reference is closed
- This is common with log files and temporary files

29. How do you create and mount a swap file?

Answer:

- Create swap file: dd if=/dev/zero of=/swapfile bs=1M count=2048
- Set permissions: chmod 600 /swapfile
- Format as swap: mkswap /swapfile
- Enable swap: swapon /swapfile
- Add to fstab: echo "/swapfile none swap sw 0 0" >> /etc/fstab
- Verify swap is active: swapon -s or free -h
- Check swap usage: cat /proc/swaps
- Set swappiness: echo 'vm.swappiness=10' >> /etc/sysctl.conf
- Apply sysctl changes: sysctl -p

30. How do you find large unused files across multiple partitions?

Answer:

- Find large files: find / -type f -size +100M -atime +30 2>/dev/null
- Check all partitions: df -h then search each mount point
- Find by size and access time: find / -type f -size +1G -atime +60 -ls
- Exclude system directories:

bash

```
find / -type f -size +100M -atime +30 -not -path "/proc/*" -not -path "/sys/*"
```

- Use locate database: locate -S then locate -r '.*' | xargs ls -lah | grep '^-.*[0-9]G'
- Find temporary files: find /tmp /var/tmp -type f -size +100M -atime +7
- Check log files: find /var/log -type f -size +100M -mtime +30

31. How do you fix a corrupted file system using fsck?

Answer:

- Unmount the filesystem first: umount /dev/sdX1
- Run fsck in check-only mode: fsck -n /dev/sdX1
- Run interactive repair: fsck /dev/sdX1
- Force check: fsck -f /dev/sdX1
- Auto-repair: fsck -y /dev/sdX1 (answer yes to all)
- For specific file systems:
    - ext2/3/4: e2fsck -f /dev/sdX1
    - XFS: xfs_repair /dev/sdX1
- Check bad blocks: fsck -c /dev/sdX1
- Boot from rescue media for root filesystem
- Always backup important data first if possible

32. What is inode exhaustion, and how do you resolve it?

Answer:

- Check inode usage: df -i
- Find directories with many files: find / -xdev -type f | cut -d/ -f2 | sort | uniq -c | sort -n
- Find directories with most files: find /path -type d -exec sh -c 'echo "$(ls -1A "$1" | wc -l) $1"' _ {} \; | sort -n
- Delete unnecessary files, especially:
    - Temporary files in /tmp
    - Old log files
    - Cache files
- Clean package manager cache
- Remove old kernels and headers
- Check for directories with many small files

- Increase inode count (requires filesystem recreation):

bash

```
mkfs.ext4 -N 2000000 /dev/sdX1
```

33. You need to copy a huge file across servers. What's the fastest way?

Answer:

- Use rsync with compression: rsync -avz --progress file user@server:/path/
- Use scp with compression: scp -C largefile user@server:/path/
- Use netcat for direct transfer:
  - Receiver: nc -l 9999 > file
  - Sender: nc server 9999 < file
- Use tar with ssh: tar -czf - file | ssh user@server 'tar -xzf - -C /path/'
- Parallel transfer with aria2: aria2c --file-allocation=none file
- Use bbcp for high-speed transfers: bbcp file user@server:/path/
- Consider splitting large files: split -b 1G file prefix
- Use compression if network is slow: gzip file before transfer

34. Your df -h and du -sh show different disk usage. Why?

Answer:

- Deleted files still held open by processes (check with lsof +L1)
- Hard links counted multiple times by du
- Sparse files (du shows actual disk usage, df shows allocated space)
- Different block size calculations
- Files in mount points hidden by mounted filesystems
- Metadata overhead (inodes, journal) counted by df
- Snapshot or backup files taking space
- Check for files in directories that are mount points
- Reserved space for root user (usually 5% on ext filesystems)
- Different units or rounding differences

35. How do you find out which directory is consuming the most space in /var?

Answer:

- Use du command: du -sh /var/* | sort -hr
- Drill down into largest directory: du -sh /var/log/* | sort -hr

- Interactive exploration: ncdu /var
- Show all subdirectories: du -ah /var | sort -hr | head -20
- Find large files specifically: find /var -type f -size +100M -exec ls -lh {} \;
- Use tree with sizes: tree -h -L 2 /var
- Check specific common directories:

bash

```
du -sh /var/log /var/cache /var/lib /var/spool /var/tmp
```

- Real-time monitoring: watch "du -sh /var/* | sort -hr"