VINAY.T

LINUX Interview Style Q&A with Practical Context DAY 14

System Monitoring

151. Q: You suspect a process is consuming too much CPU. How do you identify and monitor it in real time?
A: Use the **top** or **htop** command.

- **top** shows real-time CPU usage by processes.
- **htop** offers a more user-friendly interface with sortable columns and color-coded metrics.
  Ideal for spotting CPU bottlenecks and high-load processes.

152. Q: How do you quickly check if the server is under load or operating normally?
A: Use the **uptime** command.
It shows how long the system has been running and provides load averages over the last 1, 5, and 15 minutes.
Helps assess if the server is overloaded, especially in multi-core environments.

153. Q: A production service stopped, and you suspect the disk might be full. What command do you use to verify this?
A: Run **df -h.**
This shows disk usage for all mounted filesystems in a human-readable format.
Look for any partitions at 100% usage that could be causing failures.

154. Q: How do you check the current memory usage of the system?
A: Use **free -h.**
It provides total, used, and available memory, along with buffer/cache details.
The -h flag makes it easier to interpret values in MB/GB.

155. Q: How can you check if swap space is being utilized and how much is in use?
A: Use **swapon --show** or **free -h.**

- **swapon --show** lists active swap devices and their usage.
- **free -h** gives a quick overview of both RAM and swap in one shot.
  Useful for identifying memory pressure issues.

156. Q: Network latency is increasing. You want to check current network usage per interface. What do you use?
A: Use **ifstat.**
It provides real-time statistics on bandwidth usage (in/out) for each network interface.
Helps spot sudden traffic spikes or saturation.

157. Q: You want detailed stats on the number of packets sent/received, including errors. What command helps with this?
A: Run **ip -s link.**
This displays traffic statistics, errors, dropped packets, and collisions for all network interfaces.
Very useful for diagnosing low-level network issues.

158. Q: An application is misbehaving, and you want to monitor its logs in real time. What do you do?
A: Use **tail -f /var/log/syslog** (or any relevant log file).
The **-f** option allows live tracking of new log entries.
Great for monitoring logs during service restarts or issue reproduction.

159. Q: A manager asks how long a server has been up. What's the quickest way to check this?
A: Use the **uptime** command.
It provides the exact duration since the last reboot along with load averages.
Quick and reliable for uptime verification.

160. Q: How do you get a snapshot of overall system resource utilization like CPU, memory, and I/O?
A: Use the **vmstat** command.
It reports stats on processes, memory, paging, block I/O, and CPU.
Ideal for performance trend analysis and identifying resource bottlenecks.

Advanced File Handling

161. Q: You need to copy an entire directory and its contents, including subdirectories. What command do you use?
A: Use:
cp -r source_directory destination_directory

- The -r (recursive) flag ensures all nested files and directories are copied.
- If the destination directory doesn't exist, it will be created.

This is useful for backups, duplicating configurations, or staging environments.

162. Q: How do you rename a file or move it to another directory?
A: Use the mv command:
mv old_name new_name

- If new_name is a file, this renames the file.
- If new_name is a directory, the file will be moved into it.

Commonly used for organizing files, renaming configs, or promoting builds (e.g., from staging.conf to production.conf).

163. Q: You want to delete a file from the filesystem. What's the command?
A: Run:
rm filename

- Permanently deletes the file.
- No confirmation is asked unless -i is used.

Use with caution, especially when running scripts with elevated permissions.

164. Q: How do you delete a directory and all its contents in one go?
A: Use:
rm -r directory_name

- The -r option recursively removes all files and subdirectories.
- Add -f to force deletion without prompts (rm -rf).

This is powerful but dangerous — always double-check the path before execution.

165. Q: How do you locate a file by its name starting from the root directory?
A: Use the find command:
find / -name "filename"
- This recursively searches all directories starting from /.
- For a case-insensitive search, use -iname.

Helpful when dealing with misplaced configs or binary files.

166. Q: How do you search for a specific string inside a file?
A: Use:
grep "text" file_name
- This prints lines from the file that match the given text pattern.
- Add -i for case-insensitive search and -r to search recursively in directories.

Useful for scanning logs, config files, or codebases.

167. Q: You need to find and replace text in a file. What's the easiest way from the CLI?
A: Use sed (stream editor):
sed -i 's/old_text/new_text/g' file_name
- The -i flag edits the file in place.
- The s command means substitute, and g applies the change globally on each line.

Frequently used in automation scripts for templating configs or updating variables.

168. Q: How do you combine the contents of two files into a new one?
A: Use the cat command:
cat file1 file2 > new_file
- This merges the contents of file1 and file2 into new_file.
- Use >> instead of > to append to an existing file.

Common for log aggregation or building combined config files.

169. Q: You want to compress a directory into a .tar.gz archive. How do you do it?
A: Use:
tar -czf archive_name.tar.gz directory_name
- -c creates the archive, -z compresses it with gzip, and -f specifies the filename.
- Preserves directory structure.

Widely used for backups, packaging applications, and deployments.

170. Q: You received a .tar.gz archive and need to extract its contents. What's the command?
A: Use:
tar -xzf archive_name.tar.gz
- -x extracts, -z handles gzip compression, and -f specifies the archive.
- Add -C /path/to/dir to extract to a specific location.

Standard practice when handling source code, binaries, or artifacts in CI/CD pipelines.

Backup and Recovery

171. Q: You need to back up a directory for safekeeping. What's the go-to command?
A: Use the tar command:
tar -cvf backup_name.tar.gz directory_name

- -c creates a new archive, -v shows progress (verbose), -f names the output file.
- Although the filename ends in .gz, actual compression requires the -z flag (tar -czvf).

This is commonly used for simple, quick backups of config directories or application data.

172. Q: You have a .tar.gz backup file. How do you restore its contents?
A: Use:
tar -xvf backup_name.tar.gz

- -x extracts files, -v is for verbose output, and -f specifies the archive to extract.
- Add -C /target/path if you want to extract to a specific location.

A standard method to restore archived data or configs.

173. Q: You want to sync files from one server to another for incremental backups. What do you use?
A: Use rsync:
rsync -avz source/ destination/

- -a enables archive mode (preserves permissions, timestamps),
- -v for verbose, and -z compresses data during transfer.

Great for efficient backups over SSH or local incremental copies.

174. Q: How do you automate backup scripts to run daily?
A: Use cron by editing the crontab:
crontab -e

Then add a line like:
0 2 * * * /path/to/backup_script.sh
This runs the script every day at 2 AM.

Cron is a widely used scheduling tool in Linux for backup automation and routine tasks.

175. Q: Where do you check backup job logs for success or failure?
A: Use:
cat /var/log/backup.log

- This assumes your backup script logs output to that file.
- For real-time monitoring, use tail -f /var/log/backup.log.

Important for validating backup jobs and troubleshooting failures.

176. Q: How do you take a full disk image of a system using dd?
A: Use:
dd if=/dev/sda of=backup.img bs=4M status=progress

- if is input file (disk), of is output file (image), bs=4M speeds up the copy, and status=progress shows live status.

Useful for full-system cloning or low-level backups before major changes.

177. Q: How do you restore a system from a dd disk image?
A: Use:
dd if=backup.img of=/dev/sda bs=4M status=progress

- This performs a block-level restore to the original disk.

Warning: This will overwrite the entire destination drive. Make sure /dev/sda is correct before executing.

178. Q: How do you configure incremental, snapshot-style backups using rsnapshot?
A:
1. Edit the configuration file:
   /etc/rsnapshot.conf

2. Run scheduled tasks using:
   rsnapshot daily

- rsnapshot uses rsync under the hood and manages multiple timestamped backups efficiently.

It's ideal for versioned backups without consuming large amounts of storage.

179. Q: How do you manually mount a backup disk?
A: Run:
mount /dev/sdX /mount_point
- Replace /dev/sdX with your actual disk device, and ensure the mount point exists.
- Use lsblk or fdisk -l to identify the correct disk.

Necessary for accessing or restoring data from external or attached backup drives.

180. Q: How do you safely unmount a backup disk after use?
A: Use:
umount /mount_point

- Make sure no processes are using the disk (check with lsof or fuser if needed).

Unmounting prevents data corruption and safely removes external drives.

Security and Permissions

181. Q: You need to change the access permissions of a file. How do you do it in Linux?
A: Use the chmod command:
chmod 755 script.sh
- Numeric mode (e.g., 755) sets permissions for user, group, and others.
- Symbolic mode (chmod u+x file) can also be used for finer control.

Essential for managing file-level security, especially in production scripts and executables

182. Q: A file needs to be reassigned to another user and group. What's the proper way?
A: Use the chown command:
chown alice:developers report.txt
- Changes ownership of report.txt to user alice and group developers.

Helps enforce proper file access in multi-user or team environments.

183. Q: How do you create a new user on a Linux system?
A: Run:
useradd john

- This adds a new user but does not set a password.
- Use -m to create a home directory: useradd -m john.

Crucial step in system provisioning and user management.

184. Q: You've created a user. Now how do you set or change their password?
A: Use:
passwd john

- Prompts for a new password and applies it to the user account.

This is necessary for enabling login access.

185. Q: A user account is no longer needed. How do you delete it?
A: Use:
userdel john
- Add -r to delete the user's home directory as well:
userdel -r john

Used during de-provisioning to cleanly remove access.

186. Q: You want to give a user access to additional group privileges. How do you do that?
A: Use:
usermod -aG docker john
- -aG appends the user to a group without removing existing group memberships.

This is commonly used to grant access to tools like Docker or sudo.

187. Q: How can you see all the groups defined on your system?
A: View the contents of:
cat /etc/group
- Each line represents a group and its members.

Useful for validating group assignments and permissions.

188. Q: How do you harden SSH by disabling root login?
A: Edit the SSH configuration file:
sudo vi /etc/ssh/sshd_config

Set:
PermitRootLogin no

Then restart SSH:
systemctl restart sshd

This prevents direct root login over SSH — a key security best practice.

189. Q: You want to enable SSH key-based login instead of passwords. How do you do that?
A: Copy your public key to the server:
ssh-copy-id user@remote_host

Or manually:
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys

- Make sure .ssh directory and file permissions are correct.

Enhances security and is essential for automation and secure remote access.

190. Q: Where do you view general system logs in Linux for troubleshooting?
A: Use:
journalctl

- For traditional logs, use:
  cat /var/log/syslog

- Use tail -f for live updates.

Log monitoring is vital for incident response, audits, and security reviews.