DevOps — Linux (25 Questions)

Q1: A production server is unresponsive over SSH, but ICMP ping works.

Answer:
Check if SSH daemon is down or blocked by firewall. Use console access (cloud provider serial console) to log in and inspect systemctl status sshd. If sshd is running, check ss -tnlp | grep :22 and firewall rules (iptables -L or firewalld). Also inspect fail2ban for IP bans.

Sample Points:

- ICMP works → kernel/network up.
- SSH port/service may be blocked/stopped.
- Fail2ban or security group rules can block.

Example Code:

```
sudo systemctl status sshd
sudo ss -tnlp | grep :22
sudo iptables -L -n
```

Q2: Disk usage on `/var` hits 100% causing app crashes.

Answer:

Identifylarge files with du -sh /var/*|sort-h , check `/var/log` for oversized logs, rotate/compress logs via logrotate . Remove old journal logs (`journalctl --vacuum-time=7d`) .

Sample Points:

- Large logs are common culprit.
- Use du to locate offenders.
- Configure logrotate to prevent repeats.

Example Code:

```
sudo du -sh /var/* | sort -h
sudo journalctl --vacuum-time=7d
```

Q3: CPU usage is maxed out by a runaway process; system is sluggish.

Answer:
Find offending process with top or `ps-eopid,ppid,cmd,%cpu --sort=-%cpu` . Renice process or kill it. Investigate logs to see why it misbehaved.

Sample Points:

- Identify heavy process.
- Adjust priority with `renice`.
- Kill only if safe.

Example Code:

```
sudo renice 10 -p <PID>
```

Q4: Network latency spikes intermittently to an external service.

Answer:
Run mtr or `traceroute` to detect hop causing delay. Check `ethtool` for interface errors and `dmesg` for NIC resets.

Sample Points:

- MTR for real-time path analysis.
- Check NIC stats for errors.
- Could be external ISP hop.

Example Code:

```
mtr --report google.com
sudo ethtool -S eth0
```

Q5: Cron job didn’t execute, but works manually.

Answer:
Check cron logs (`grep CRON /var/log/syslog`), ensure script path and environment variables are absolute. Cron uses minimal `PATH`, so commands must be full path.
Sample Points:

- Cron needs absolute paths.
- Minimal environment in cron.
- Check execution permissions.
  Example Code:

```
* * * * * /usr/bin/python3 /opt/scripts/task.py
```

Q6: SSH brute-force attempts are filling logs.

Answer:
Enable fail2ban with sshd jail, set MaxAuthTries in sshd_config, and consider moving SSH to a non-standard port (security by obscurity + logging).
Sample Points:

- fail2ban blocks repeated offenders.
- Reduce max auth tries.
- Keep logs clean for real events.
  Example Code:

```
sudo apt install fail2ban
sudo systemctl enable --now fail2ban
```

Q7: A service doesn’t start on boot but runs fine manually.

Answer:
Enable with `systemctl enable servicename`, ensure `[Install]` section in unit file has

correct `WantedBy`. Check `journalctl -u servicename` for boot-time errors.

Sample Points:

- Unit must have enable target.
- Boot-time deps can delay start.
- Journal logs reveal cause.

Example Code:

```
sudo systemctl enable myservice
```

Q8: File permission changes revert after reboot.

Answer:

Likely due to immutable attribute (`lsattr`) or config management (e.g., Ansible, Puppet). Remove immutable bit (`chattr -i`) or update CM template.

Sample Points:

- Check immutable attribute.
- CM tools can reset perms.
- Edit source templates.

Example Code:

```
lsattr /path/file
sudo chattr -i /path/file
```

Q9: Web app returns 502 after Nginx restart.

Answer:

Check if upstream app service is running (`systemctl status`), correct upstream socket/port in Nginx config, test with `curllocalhost:port`.

Sample Points:

- 502 = upstream unreachable.

- Confirm backend service status.
- Port/socket config must match.
  Example Code:

```
curl -v http://127.0.0.1:5000
```

Q10: SELinux blocks app from binding to port 8080.

Answer:
Use `semanageport-a-thttp_port_t-ptcp 8080` to allow, or set SELinux boolean if service-specific. Check audit logs for denials.

Sample Points:

- SELinux enforces port context.
- Add port mapping for new services.
- Audit logs guide rules.
  Example Code:

```
sudo semanage port -a -t http_port_t -p tcp 8080
```

Q11: Slow DNS resolution on server.

Answer:
Check /etc/resolv.conf order, ensure fastest DNS servers, and test with `dig +trace`. Disable reverse DNS lookups in SSH (UseDNS no).

Sample Points:

- Optimize resolver order.
- Test with dig to isolate slowness.
- Disable unnecessary reverse lookups.
  Example Code:

```
dig example.com
```

Q12: User accidentally deleted `/etc/passwd`.

Answer:
Restore from backup or copy from a similar system, adjust UIDs/GIDs. Boot into rescue mode if needed.
Sample Points:

- System won't authenticate without it.
- Restore quickly from backup.
- Verify UIDs match actual files.
  Example Code:

```
cp /mnt/backup/etc/passwd /etc/passwd
```

Q13: Root disk filling with `/var/lib/docker`.

Answer:
Prune unused images/volumes, move Docker data root via `/etc/docker/daemon.json` and symlink or mount to larger volume.
Sample Points:

- Docker cache can bloat quickly.
- Move to dedicated disk.
- Schedule prune jobs.
  Example Code:

```
sudo mkdir /mnt/docker
{"data-root": "/mnt/docker"}
```

Q14: Process hangs in `D` state (uninterruptible sleep).

Answer:
Caused by kernel waiting on I/O. Check disk health with `smartctl`, inspect dmesg for I/O errors. Usually hardware/storage problem.

Sample Points:

- Dstate = I/O wait.
- Investigate disk/NFS mounts.
- Might require hardware fix.

Example Code:

```
sudo smartctl -a /dev/sda
```

Q15: Swap usage grows constantly, even with free RAM.

Answer:
Check vm.swappiness value (`sysctl vm.swappiness`). Lower to 10-20 to prefer RAM. Investigate memory leaks with `smem`.

Sample Points:

- Adjust swappiness for usage pattern.
- Swap use with free RAM often config issue.
- Check per-process memory.

Example Code:

```
sudo sysctl -w vm.swappiness=10
```

Q16: High load average but low CPU usage.

Answer:
Likely I/O wait or many blocked processes. Check `iostat -xz`, look for `%util` and await.

Sample Points:

- Load includes I/O wait.

- Identify bottleneck device.
- Use iostat for detailed view.
  Example Code:

```
iostat -xz15
```

Q17: After adding new disk, it's not visible in `/dev`.

Answer:
Rescan SCSI bus (`echo"- - -" > /sys/class/scsi_host/hostX/scan`) or reboot. Partition with `fdisk` and mount.
Sample Points:

- Rescan before reboot.
- Partition and format.
- Update `/etc/fstab`.
  Example Code:

```
sudo fdisk /dev/sdb
```

Q18: System time drifts in VM.

Answer:
Enable NTP (`chronyd` or `systemd-timesyncd`), check hypervisor time sync.
Sample Points:

- NTP for accuracy.
- VM tools can sync time too.
- Avoid both sources conflicting.
  Example Code:

```
sudo timedatectl set-ntp true
```

Q19: User can't write to shared directory despite group membership.

Answer:

Ensure directory has `g+w` and `setgid` bit so new files inherit group.

Sample Points:

- setgid preserves group ownership.
- Check umask settings.
- Group perms must be correct.

Example Code:

```
chmod 2775 /shared
```

Q20: Network service fails to bind after reboot because interface name changed.

Answer:

Disable predictable interface names or update systemd service to use new name. Use networkctl to see current mapping.

Sample Points:

- Predictable names can change after NIC add/remove.
- Use persistent naming via udev rule.
- Update configs accordingly.

Example Code:

```
sudo ln -s /dev/null /etc/udev/rules.d/80-net-setup-link.rules
```

Q21: Script fails in cron but works manually due to environment vars.

Answer:
Export needed vars in script or source profile file at start. Cron has minimal env.

Sample Points:

- Cron env minimal.
- Source ~/.profile if needed.
- Explicitly set PATH.
  Example Code:

```
#!/bin/bash
. /home/user/.profile
```

Q22: `top` shows zombie processes.

Answer:
Zombies are dead processes not reaped by parent. Identify parent PID, restart it if safe.

Sample Points:

- Zombies don't consume CPU.
- Restart parent to clear.
- Orphan adoption by init reaps.
  Example Code:

```
ps -el | grepZ
```

Q23: Ulimit prevents app from opening more than 1024 files.

Answer:
Increase `nofile` in `/etc/security/limits.conf` and ensure PAM configs load it.

Sample Points:

- Raise limits in limits.conf.

- Check PAM session files.
- Apply at systemd service level.
  Example Code:

```
LimitNOFILE=65535
```

Q24: Package install fails due to broken apt/yum repo.

Answer:
Check repo URL in sources, refresh cache, disable failing repo temporarily.

Sample Points:

- Validate repo URL.
- Refresh metadata.
- Disable if not needed.
  Example Code:

```
sudo apt update
sudo yum --disablerepo=badrepo install pkg
```

Q25: Need to audit recent sudo commands run by a user.

Answer:
Check `/var/log/auth.log` or journal with `journalctl _COMM=sudo`.

Sample Points:

- Auth log records sudo usage.
- Use journalctl for query.
- Track time + command run.
  Example Code:

```
sudo journalctl _COMM=sudo
```