Real-World Linux Server Troubleshooting Scenarios

DevOps & Cloud Engineers

1. Kernel Panic on Production Server

Q: How do you diagnose and recover from a kernel panic on a cloud VM?
A: Review VM console output and `/var/log/kern.log`. Boot from a rescue image if inaccessible, mount the disk, and check for hardware, driver, or recent kernel update issues. Roll back with package manager or replace corrupted files.

---

2. Unresponsive Application After Deploy

Q: A containerized app isn't responding post-deployment. Steps?
A: Use `docker logs`/`kubectl logs` and `kubectl describe pod`. Check for resource limits, networking (Service/Ingress), image tags, and failed health checks. Roll back or redeploy as needed.

---

3. High Disk I/O Latency

Q: Identify and resolve excessive disk latency in a cloud-hosted Linux server.
A: Use `iostat`, `iotop`, and `df -h`. Check for noisy neighbor effects on the cloud, misconfigured swap, or apps causing high write ops. Consider moving workloads or resizing volumes.

---

4. Service Downtime After Security Patch

Q: Web service crashes after a security patch; what next?
A: Review `systemctl status` and service logs. Investigate changed files/binaries with `rpm -V`/`dpkg -V`. Roll back patch if critical; schedule staged testing for future updates.

---

5. Slow Database Performance

Q: Live DB running slow during peak hours, how do you proceed?
A: Use `top`, `htop`, and database monitoring tools. Pinpoint long queries, full disk, or insufficient RAM. Scale vertically/horizontally or optimize queries and disk layout.

---

6. SSH Brute Force Attack Detected

Q: What's your response strategy?
A: Analyze logs (`/var/log/auth.log`), block offending IPs via `iptables` or security groups. Enable key-based authentication, change default port, and deploy fail2ban.

---

7. Cloud Storage Mount Failure

Q: NFS/EFS mount breaks in production; troubleshooting steps?
A: Confirm network path (`ping`, `traceroute`), NFS client/service status, security group/firewall permission, and export options. Remount and review for kernel upgrades or IP whitelisting.

8. Periodic Application Crashes

Q: How do you identify the root cause of intermittent process crashes?
A: Enable core dumps/`ulimit` and analyze with `gdb`. Review `/var/log/messages`, memory/cpu metrics, and recent release notes or bug trackers.

---

9. Misconfigured Load Balancer

Q: After DNS cutover, app is unreachable; best troubleshooting approach?
A: Check DNS propagation, load balancer health checks, and backend registration. Use `curl` and LB logs; rollback DNS if needed. Validate SSL and target group configs.

---

10. Increasing Memory Usage

Q: Mitigate and analyze rising memory on a Linux service.
A: Track process with `ps aux --sort=-%mem`, `top`, and heap profilers. Check for leaks, misconfigured cache, or unbounded queues. Restart service and plan patching.

---

11. Delayed Cron Jobs

Q: Why might cloud-hosted cron jobs run late or not at all?
A: Review `cron.log`, timezone settings, service status, and permission issues. For cloud VMs, check instance hibernation or scaling events that could interrupt schedules.

---

12. Network Throughput Bottleneck

Q: Degraded throughput between app and DB; where do you start?
A: Run `iperf` tests, inspect MTU, security group rules, and check cloud vendor metrics for throttling. Optimize routes, leverage VPC peering, check for packet loss.

---

13. Linux Server Won't Boot on Cloud

Q: Steps for a non-booting cloud VM.
A: Review cloud console (serial output), use rescue/recovery mode to inspect `/boot`, `/etc/fstab`, and disk health with `fsck`. Detach/attach disk to another VM if necessary.

---

14. Remote Logging Not Working

Q: Syslog/ELK forwarding stops; how do you fix it?
A: Check service status (`systemctl`), firewall rules, TCP port 514 accessibility. Review log agent configs and test with `logger`, check for certificate validity in cloud logging setups.

---

15. Hung Process on Critical Service

Q: Diagnosing a frozen but non-crashing daemon.
A: Use `ps`, `strace -p [PID]`, and `lsof`. Identify blocking syscalls. Restart or SIGTERM/SIGKILL if necessary; capture before/after logs for RCA.

16. High Load Average with Low CPU Usage

Q: What causes high load average but idle CPUs?
A: Check for I/O waits using `vmstat` and `iostat`, zombie or blocked processes, or network bottlenecks. Address disk, NFS, and process locking issues.

---

17. DNS Resolution Failure

Q: Apps report name resolution errors. Steps?
A: Validate `/etc/resolv.conf`, test with `nslookup` and `dig`, check upstream DNS, firewall rules, and host file overrides.

---

18. Mount Point Becomes Read-Only

Q: Fixing unexpected filesystem remounts to read-only.
A: Check `dmesg` for disk errors, run `fsck`, review cloud disk health. Restore from snapshot if corruption persists; monitor for hardware faults.

---

19. Application Timeouts

Q: Linux web app times out; debugging steps?
A: Trace with `curl`/`wget`, review service and network latency, inspect cloud load balancer logs, and check for thread pool exhaustion.

---

20. Scheduled Backup Failures

Q: Automated backup scripts fail; troubleshooting sequence?
A: Inspect log/filesystem errors, permission/space issues, remote endpoint availability, and cron scheduling. Manually run script for error output.

---

21. OS Upgrade Regression

Q: Kernel/OS upgrade breaks a mission-critical service.
A: Identify incompatible drivers, use previous kernel from GRUB, rollback with package manager, and create upgrade playbooks for future safe deployment.

---

22. Cloud Autoscaling Fails

Q: Newly provisioned VMs fail health checks; what's your approach?
A: Analyze cloud instance logs, validation scripts, configuration drift, and image/AMI validity. Validate startup/boot hooks and network access for config management tools.

---

23. SELinux/AppArmor Denials

Q: How to diagnose sudden service access denials?
A: Review `/var/log/audit/audit.log`, run `ausearch`, and look for "denied" context. Adjust policy or create overrides as needed; test in staging.

24. Data Corruption After Storage Migration

Q: File corruption post-migration. How do you resolve and prevent?
A: Use `md5sum` or `sha256sum` for validation, fsck, restore recent snapshot, and review migration documentation for protocol mismatches.

---

25. Infrastructure as Code Drift Detected

Q: Deployed resources don't match IaC definitions—next steps?
A: Run `terraform plan`/`apply` with state refresh, investigate manual changes, enforce policy-as-code with CI/CD checks, and plan remediation.

---

26. Persistent High Server Load from CI/CD Jobs

Q: Jenkins server load spikes during build windows; mitigation strategy?
A: Monitor builds using `htop`/`ps`, tune executor/worker count, check pipeline for inefficient jobs, and consider workload offloading to cloud-native runners.

---

27. Networking Issues With Kubernetes Pods

Q: Pods can't reach services in another namespace—debug plan?
A: Use `kubectl get svc,pods`, review NetworkPolicies, check CNI plugin logs, and ensure DNS resolution between namespaces.

---

28. Security Group Misconfiguration

Q: Service down after security group change—quick checks?
A: Validate inbound/outbound rules, port/protocol specs, instance association, and recent changes in version control/cloud audit logs.

---

29. Log File Rotation Gaps

Q: Intermittent log rotations delete or skip files. How to fix?
A: Review `logrotate` config, permissions, and recent updates. Test rotation manually and integrate log archiving into the central logging pipeline.

---

30. Cloud Billing Unexpected Spike

Q: Unusual cost surge traced to one Linux instance—troubleshooting flow?
A: Check instance type/hours, burstable CPU/network traffic, premium disk usage, or idle resources (orphaned volumes). Audit with cloud cost explorer/monitoring tools.

By_Kranthi Putti