Linux System Administration Scenario-Based Question& Answer

Scenario 1: High CPU Usage
Question: You receive an alert that a production server is experiencing consistently high CPU usage (e.g., 90-95%). What steps would you take to diagnose and resolve this issue?
Answer:
 * Initial Assessment: I'd immediately log into the server via SSH and use top or htop to identify the processes consuming the most CPU.
 * Process Identification: If a specific process is hogging the CPU, I'd analyze its details:
 * ps aux --sort=-%cpu | head -n 5: To see the top 5 CPU-consuming processes with full details.
 * lsof -p <PID>: To see files opened by the process, which might indicate what it's doing.
 * Check application logs related to the process for errors or unusual activity.
 * Root Cause Analysis:
 * Application Issue: Is it a runaway script, an inefficient query, or an application bug? I'd consult with the development team if it's an application.
 * Resource Contention: Is the application simply under heavy load? I'd check active connections, request rates, etc.
 * Malicious Activity: While less common, I'd consider if there's any unauthorized process or attack.
 * Mitigation & Resolution:
 * Temporary: If critical, I might kill or renice (lower priority with renice +10 <PID>) the problematic process.
 * Permanent:
 * Application Optimization: Work with developers to optimize code, queries, or increase application resources.
 * Scaling: If due to legitimate load, propose scaling up (more CPU/RAM) or scaling out (adding more servers).
 * Debugging: Use tools like strace for system calls or perf for performance analysis if deep debugging is required.
 * Configuration Tuning: Adjust system or application configurations (e.g., web server concurrency).
 * Monitoring: Implement continuous monitoring to track CPU usage and prevent recurrence.

Scenario 2: Disk Space Running Out
Question: A critical log partition on a Linux server is at 95% capacity. How would you

quickly free up space and then implement a long-term solution?

Answer:

* Immediate Action (Freeing Space):
* df -h: Verify the exact partition and its usage.
* du -sh /*: Start from the root and recursively find large directories (e.g., /var/log).
* find /var/log -type f -name "*.log" -mtime +7 -delete: Delete old log files (e.g., older than 7 days).
* truncate -s 0 /path/to/large/log_file: Truncate specific large log files that are actively being written to (use with caution, as it will clear the file).
* Check for core dumps (find / -name core -delete).
* Clear package manager caches (sudo apt clean on Debian/Ubuntu, sudo yum clean all on RHEL/CentOS).