System Administration Troubleshooting - Interview Preparation Canvas

---

Objective: Provide a complete guide to troubleshooting common system admin issues with a structured approach, real-world examples, and practical steps for any IT environment.

---

1. Structured Troubleshooting Approach

Step 1: Identify the Problem - Collect information from user and system logs. - Ask questions: When did it start? Any recent changes? Who is affected?

Step 2: Establish a Theory of Probable Cause - Consider hardware, software, network, configuration, and human error. - Prioritize likely causes based on symptoms.

Step 3: Test the Theory - Perform diagnostics, ping, traceroute, system checks. - Check logs for errors (Event Viewer in Windows, /var/log in Linux).

Step 4: Plan and Implement a Solution - Decide safest resolution method. - Backup data if needed. - Apply fix carefully.

Step 5: Verify Full System Functionality - Ensure system works as expected. - Test affected users, services, or network connectivity.

Step 6: Document Findings and Actions - Record problem, solution, and preventive measures. - Helps in recurring issues and knowledge sharing.

---

2. Common Troubleshooting Issues & Real-World Examples

A. Network Issues

Problem: Users cannot connect to the internet.

Steps: 1. Check physical connections (cables, Wi-Fi) 2. Verify IP configuration (ipconfig/ifconfig) 3. Ping gateway and DNS servers 4. Check router/firewall rules 5. Trace route to confirm network path 6. Reset network adapter if needed

Example: A user complains internet is down. On investigation: - IP shows APIPA (169.254.x.x), meaning DHCP failed. - Restarted DHCP service on server, released and renewed IP on client. - Internet restored.

B. Server/Service Issues

Problem: Web server is not responding.

Steps: 1. Check if service is running (systemctl status apache2 / netstat -tuln) 2. Check logs (/var/log/apache2/error.log) 3. Test port connectivity (telnet/port check) 4. Check firewall rules 5. Verify disk space and resource usage 6. Restart service if safe

Example: Apache fails to start due to full /var/log directory. - Cleared old logs, restarted service, web server functional.

C. Windows System Issues

Problem: Blank screen on startup.

Steps: 1. Check power and monitor connections 2. Boot in Safe Mode 3. Check event logs for recent updates/drivers 4. Perform system restore if needed 5. Update display drivers 6. Test with alternate monitor

Example: User reports blank screen after Windows update. - Safe Mode booted successfully. - Uninstalled latest graphics driver. - Rebooted system, normal display restored.

D. Authentication & Access Issues

Problem: Users cannot log in; account locked or password expired.

Steps: 1. Check Active Directory for account status 2. Verify password policies and account lockouts 3. Check replication between domain controllers 4. Reset password if needed 5. Review login logs for failed attempts

Example: Multiple users report login failure. - Event logs show account lockouts from a rogue device. - Identified device, disconnected it, reset passwords, users regain access.

E. Storage & Disk Space Issues

Problem: Server running out of space.

Steps: 1. Check disk usage (du -sh, df -h) 2. Identify large files/folders 3. Delete temp/log files, archive old data 4. Expand volume if necessary

Example: /var filled on Linux server. - du -sh /var/* identified logs consuming space. - Rotated logs, removed old backups, disk space freed.

F. Backup & Recovery Issues

Problem: Backup fails.

Steps: 1. Check backup logs 2. Verify destination storage and permissions 3. Test backup manually 4. Restart backup service/scheduler 5. Review network/storage connectivity

Example: Nightly backup failed. - Logs indicated network share not accessible. - Network path fixed, backup resumed successfully.

G. Common Client Issues

- Wi-Fi not connecting: Check SSID, password, adapter, DHCP
- Slow system: Check CPU/RAM usage, running processes, malware scan
- Application crashes: Check logs, reinstall software, verify dependencies
- Printer not working: Check network, drivers, queue status

---

3. Troubleshooting Framework / Mindset

1. Stay calm and gather all facts.
2. Avoid making random changes.
3. Prioritize business-critical systems.
4. Use logs and monitoring tools effectively.
5. Isolate the problem (user, system, network).
6. Implement changes methodically.
7. Document every step for accountability.

---

4. Example Scenario Questions & Model Responses

Scenario 1: Users cannot access shared folder. - Steps: Check network, check server, verify permissions, check AD group membership, test access - Interview Delivery: 'I first verify network connectivity, then check the server hosting the share, confirm permissions for the user/group, and test access. Finally, I document the findings and fix.'

Scenario 2: VPN not connecting. - Steps: Verify client config, check VPN server, check firewall/ports, test from different client, review logs - Interview Delivery: 'I ensure the client configuration is correct, verify server health, check firewall rules and ports, test connectivity from another client, and review VPN logs for errors.'

Scenario 3: High CPU usage on server. - Steps: Identify processes consuming CPU (Task Manager/top), check scheduled tasks, check for malware, optimize services - Interview Delivery: 'I check which processes are consuming resources, review scheduled jobs, verify no malware is running, and optimize or restart services if required.'

Scenario 4: Ransomware detected. - Steps: Isolate machine, stop spread, backup critical data, restore from clean backups, perform malware analysis - Interview Delivery: 'I immediately isolate the infected system, prevent further spread, backup critical data, restore systems from backups, and analyze how the ransomware entered to prevent future incidents.'

---

5. Real-World Practical Example

Problem: Corporate Wi-Fi outage.

Steps: 1. Gather reports: Are all users affected? 2. Check access points: Power, connectivity, SSID broadcasting 3. Check DHCP server: IP assignment functioning? 4. Test connectivity from multiple devices 5. Check firewall/router: Any recent changes? 6. Restart network equipment if needed

Outcome: - Discovered AP controller service crashed. - Restarted service, Wi-Fi restored for all users. - Documented incident and implemented monitoring for AP controller service.

---

6. Key Tools to Aid Troubleshooting

- Ping, Traceroute, nslookup/dig
- netstat, ss, ipconfig/ifconfig
- Event Viewer, /var/log/
- Task Manager, top, htop, Resource Monitor
- Powershell / Bash scripting for automation
- Remote access tools: RDP, SSH
- Backup & monitoring dashboards (Splunk, CloudWatch, Nagios)

Summary: This canvas provides a structured methodology for troubleshooting, covers common system, network, and client issues, illustrates real-world examples, and delivers interview-friendly responses. Following this framework ensures a methodical, reliable, and documented approach for any system administrator.