Systems Administrator interview questions

careertips.com.au: common questions and what they're really testing

What to expect

Systems Administrator interviews tend to mix technical depth with judgement calls, since the job involves both keeping infrastructure running day to day and making decisions under pressure when something breaks. Expect a panel that includes at least one senior technical person who will push on detail.

- **Technical:** Direct questions about server, network and cloud tools you've used, testing depth of knowledge rather than just familiarity with names.
- **Scenario/troubleshooting:** A described outage or security event where you're asked to talk through your diagnostic and decision-making process in real time.
- **Behavioural:** Past-experience questions about handling incidents, competing priorities or working with non-technical staff.
- **Security and compliance:** Questions checking your understanding of patch management, access control and audit requirements relevant to the organisation's regulatory obligations.

Most interviews open with a short walkthrough of your background and current role, move into technical and scenario questions that make up the bulk of the conversation, then close with behavioural questions and a chance for you to ask about the team's tooling, on-call arrangements and current infrastructure projects.

1. Walk me through how you'd patch a fleet of production servers with minimal disruption.

Why they ask

Patch management is a core, recurring task in this role and interviewers want to see a repeatable process rather than a one-off answer.

How to structure your answer

Walk through it as a sequence: assessment, testing, scheduling, rollback plan, verification. Name the tools or environments you'd use at each step.

Example answer

“I'd start by reviewing the patch notes against our environment to flag anything with known compatibility issues, then test on a non-production server first. I'd schedule the rollout in batches outside business hours, starting with lower-priority servers, and keep a rollback snapshot ready in VMware before touching anything critical. After each batch I'd check system logs and run a quick functional test before moving to the next group, and document what was applied and when for the compliance record.”

2. Tell me about a time you diagnosed and fixed an outage under pressure.

Why they ask

Outages are inevitable in this role, and the interviewer wants evidence you can stay methodical rather than reactive when things go wrong.

How to structure your answer

Use STAR: situation, task, action, result, with enough technical detail to show real hands-on involvement.

Example answer

“A file server became unreachable during business hours, affecting several departments. I checked the network path first and ruled out connectivity, then found the disk array was near capacity and had

triggered a failover that hadn't completed cleanly. I manually restarted the failover process, freed up space by archiving old logs, and had the server back within the hour. Afterwards I set up a Zabbix alert threshold so we'd get a warning well before capacity became critical again."

3. A user reports they can access a shared drive they shouldn't have permission to see. How do you handle it?

Why they ask

This tests your judgement on access control and compliance, an area regularly audited in this kind of role.

How to structure your answer

Frame it as immediate action versus follow-up: what you'd do in the moment, then what you'd investigate afterwards.

Example answer

"First I'd confirm the report and remove the excess access straight away rather than waiting to investigate, since the exposure risk matters more than root cause in that moment. Then I'd check Active Directory group memberships to see how the permission was inherited, most likely through a nested group rather than a direct grant. I'd review whether other users are affected by the same misconfiguration and report the incident through our internal process, since it's the kind of thing an auditor would want documented."

4. How do you decide what to prioritise when you've got a security patch, a user access request and a performance issue all flagged at once?

Why they ask

Systems administrators constantly juggle competing demands, and this checks whether you can reason about risk rather than just working through a queue.

How to structure your answer

Explain your prioritisation logic explicitly: what factors you weigh and why, rather than just stating an order.

Example answer

"I'd weigh risk and impact first. A security patch addressing a known exploit usually takes priority over routine access requests, unless the performance issue is affecting a large number of users right now, in which case that comes first because it's actively disrupting work. The access request would typically wait unless it's blocking someone from doing their job, in which case I'd handle it quickly since it's usually a small task."

5. What experience do you have with cloud infrastructure, and how does it differ from managing on-premises servers?

Why they ask

With growing use of Azure and AWS in this role, interviewers want to know whether your skills extend beyond traditional on-prem administration.

How to structure your answer

Answer directly with specific tools and platforms, then contrast the operational differences you've actually encountered.

Example answer

"I've worked mainly in Azure, managing virtual machines, storage accounts and network security groups, and migrated several workloads from on-premises VMware environments. The main difference is that scaling and provisioning happen much faster, but cost management becomes an ongoing responsibility rather than a one-off hardware purchase. I also had to get comfortable with role-based access control in Azure, which works differently to traditional Active Directory group

permissions."

6. How do you stay current with new threats and vulnerabilities relevant to the systems you manage?

Why they ask

Security is embedded in this role, and the interviewer wants to know you take initiative on this rather than relying solely on vendor alerts.

How to structure your answer

Give a concrete, specific answer about your actual habits and sources, avoiding vague claims.

Example answer

"I subscribe to vendor security bulletins for the platforms we run, and I check the Australian Cyber Security Centre's alerts regularly since they're directly relevant to compliance obligations here. When a significant vulnerability is disclosed, I assess our exposure against our asset list before deciding on urgency, rather than treating every alert as equally critical."