Windows Sysadmin Interview Questions And Answers

MASTERING THE WINDOWS SYSADMIN INTERVIEW: KEY QUESTIONS AND EXPERT ANSWERS

Landing a role as a Windows Systems Administrator demands more than just familiarity with a server operating system. It requires a deep understanding of Active Directory, networking, security, scripting, and troubleshooting. Hiring managers use targeted **Windows Sysadmin Interview Questions and Answers** to gauge your practical knowledge and problem-solving abilities. Whether you are a seasoned professional or preparing for your first senior role, this guide covers the core topics you need to master. We've organized the most common questions by domain, providing detailed, real-world answers that demonstrate competence and confidence.

ACTIVE DIRECTORY AND IDENTITY MANAGEMENT

Active Directory (AD) remains the backbone of most Windows enterprise environments. Interviewers will often start here to assess your foundational knowledge.

What is Active Directory and how does it work?

Active Directory is a directory service developed by Microsoft for Windows domain networks. It stores information about objects on the network (users, computers, groups, printers) and makes this information easily accessible to administrators and users. AD uses a hierarchical structure composed of domains, trees, and forests. The **Domain Controller** authenticates and authorizes all users and computers, enforcing security policies. A solid answer should also mention the role of **LDAP**, **Kerberos**, and **DNS** in the AD ecosystem.

Explain the difference between a Domain Local, Global, and Universal group.

- **Domain Local groups** are used to assign permissions to resources (e.g., a shared folder) and can contain users and groups from any domain in the forest.
- **Global groups** are used to organize users who share a common role (e.g., all sales staff) and can be placed into other groups across domains.
- **Universal groups** are used for cross-domain access and contain global groups or users from any domain; they are stored in the Global Catalog.

For an interview, explain the **AGDLP** (Accounts, Global groups, Domain Local groups, Permissions) best practice strategy.

How do you troubleshoot a user who cannot log in to the domain?

Start by verifying the user account is not locked or disabled. Check the **Event Viewer** on the Domain Controller for Kerberos errors. Ensure the client can resolve the domain name (nslookup). Common causes include time synchronization issues, bad password caching, or blocked ports. If the issue is isolated to one workstation, try rejoining the domain after resetting the computer account.

GROUP POLICY MANAGEMENT

Group Policy is a powerful tool for centralized configuration management. Expect questions that test both theory and hands-on experience.

What is Group Policy inheritance and how do you enforce it?

Group Policy Objects (GPOs) are applied in a specific order: Local, Site, Domain, and then Organizational Unit (OU). By default, child OUs inherit settings from parent OUs. An admin can use **Enforce** (formerly "No Override") to force a GPO to apply regardless of inheritance blocking. Conversely, you can **Block Inheritance** at an OU level. The interviewer may ask you to describe a scenario where you would use each setting. Be prepared to explain the result of combining Enforce and Block Inheritance—Enforce always wins.

How can you apply a GPO only to specific users or computers?

Use **Security Filtering**. By default, a GPO applies to all authenticated users. Remove "Authenticated Users" from the security filtering and add the specific users or groups that need the GPO. You can also use **WMI Filters** to target computers based on operating system version, hardware configuration, or other attributes. For example, apply a setting only to Windows 10 workstations via a WMI filter.

POWERSHELL AND AUTOMATION

Modern Windows Sysadmins are expected to be proficient in PowerShell. Automation and scripting skills separate good candidates from great ones.

Write a PowerShell command to get all disabled users in Active Directory.

```
Get-ADUser -Filter {Enabled -eq $false} -Properties Name, SamAccountName
```

Explain that `Get-ADUser` requires the Active Directory module, and the `-Filter` parameter allows efficient server-side filtering. For large environments, always avoid client-side filtering by using proper filter syntax.

How do you handle errors in a PowerShell script?

Use `try / catch` blocks to capture terminating errors, and `$ErrorActionPreference` to control behavior for non-terminating errors. For example, setting `$ErrorActionPreference = "Stop"` can make all errors terminating. Another good practice is to use `-ErrorAction` on individual cmdlets. Mention checking `$?` or `$LASTEXITCODE` for external commands.

How can you remotely execute a script on multiple servers?

Using **PowerShell Remoting** (WinRM), you can use `Invoke-Command` with a list of computer names. For example:

```
Invoke-Command -ComputerName Server01, Server02 -ScriptBlock { Get-Service }
```

Ensure WinRM is enabled and configured correctly. For larger environments, consider **PowerShell workflows** or using `Invoke-Parallel` from the PS Parallel module.

NETWORKING AND CORE SERVICES

A sysadmin must understand the network services that Windows relies on: DNS, DHCP, and basic TCP/IP troubleshooting.

Explain the role of DNS in a Windows domain environment.

DNS is critical for Active Directory. Domain Controllers register SRV records that clients use to locate services like LDAP, Kerberos, and Global Catalog. Without proper DNS, domain functionality breaks. Interviewers often ask about **forward lookup zones**, **reverse lookup zones**, and **conditional forwarders**. Be ready to describe how to verify DNS health using `dcdiag /test:dns` or `nslookup`.

What troubleshooting steps do you take when a client cannot receive an IP address via DHCP?

First, check that the DHCP server is authorized and active. Verify the client's network adapter is enabled and connected. Use `ipconfig /release` and `ipconfig /renew`. If the client gets a 169.254.x.x address, it indicates an APIPA address, meaning no DHCP server was reachable. Check the DHCP scope for exhaustion, ensure the relay agent (if needed) is configured, and verify firewall rules for UDP ports 67 and 68.

SECURITY, PERMISSIONS, AND HARDENING

Security is a top priority. Questions will cover file permissions, user rights, and best practices for securing Windows servers.

What is the difference between NTFS permissions and Share permissions?

NTFS permissions are applied at the file system level and control access whether the user is local or remote. **Share permissions** only apply when accessing the folder over the network. The effective permission for a network user is the more restrictive of the two—NTFS and Share permissions are both evaluated. Best practice: set Share permissions to "Full Control" for everyone, and then lock down access using NTFS permissions.

How do you prevent unauthorized USB devices on company workstations?

Use **Group Policy** to disable USB removability. Deploy the policy setting "Removable Storage: Deny write access to all removable storage classes". Additionally, configure the **Device Installation Restrictions** to prevent installation of USB mass storage devices. For more granular control, consider third-party endpoint protection or Windows Defender Application Control.

BACKUP, RECOVERY, AND DISASTER PLANNING

No sysadmin interview is complete without backup and recovery questions. Show that you understand both traditional and modern approaches.

Explain a typical backup strategy for a Windows Server environment.

A common framework is the **3-2-1 rule**: at least three copies of data, on two different media types, with one offsite copy. For Windows Server, you might use **Windows Server Backup**, **System Center Data Protection Manager**, or third-party tools. Schedule full backups weekly, with incremental or differential backups daily. Always test restores periodically. Be prepared to discuss **bare-metal recovery** and **Active Directory restores** using authoritative or non-authoritative methods.

How do you recover a deleted user account in Active Directory?

In Windows Server 2016 and later, you can use the **Active Directory Recycle Bin**. Enable it via PowerShell or ADAC (Active Directory Administrative Center). Once enabled, go to the "Deleted Objects" container, right-click the user, and choose "Restore". For earlier versions, you would need to perform an authoritative restore using `ntdsutil` or restore the entire domain controller from backup. Mention the benefit of the Recycle Bin to reduce downtime.

PERFORMANCE MONITORING AND TROUBLESHOOTING

You will likely face a scenario question about a slow server or an application crash.

What tools do you use to diagnose high CPU usage on a Windows server?

Use **Task Manager** for a quick look, then **Resource Monitor** to drill down into specific processes. For more granular analysis, **Performance Monitor** allows logging counters like `% Processor Time` and `Process\% Processor Time\_Total`. For historical data, **Reliability and Performance Monitor** can create data collector sets. In modern environments, **Process Explorer** (Sysinternals) can show threads and handles. Always correlate high CPU with other metrics like memory and disk I/O.

How would you troubleshoot a server that randomly loses network connectivity?

Start by checking the event logs for network-related errors. Update or roll back network drivers. Test with a known good cable and switch port. Monitor for IP address conflicts (use `arp -a`). Check for duplex mismatch—autonegotiation can sometimes cause issues. Also consider hardware faults, power-saving features on the NIC, or driver conflicts. Persistent issues may require capturing a network trace (WireShark or netsh trace).

VIRTUALIZATION AND CLOUD INTEGRATION

Many Windows environments now involve Hyper-V, Azure, or hybrid setups. Be ready to discuss basic virtualization concepts.

What are the advantages of using Hyper-V over VMware for Windows workloads?

Hyper-V is deeply integrated with Windows Server, offering lower licensing costs for Windows VMs (additional licenses may not be required for all instances). It supports nested virtualization, live migration, and replication. However, the answer should be balanced—acknowledge that VMware often has stronger management tools and third-party support. Many enterprises run both, so show awareness of hybrid management.

How do you migrate an on-premises Windows file server to Azure?

Use **Azure Migrate** for assessment and migration. Alternatively, you can perform a lift-and-shift by replicating the server to Azure using **Azure Site Recovery**. Another approach: migrate data to **Azure Files** and decommission the on-prem file