Windows Administration - Interview Preparation Canvas

---

1. Active Directory (AD)

Concept Explanation: - AD is Microsoft’s directory service for managing users, computers, and resources. - Users: individual accounts - Groups: collection of users for permissions - GPOs (Group Policy Objects): enforce settings across users or computers

Interview Answer: "Active Directory allows centralized management of user accounts, groups, and security policies via GPOs. Users and groups help organize access, and GPOs enforce security, software, and desktop policies across the domain."

Delivery Example: "I would say: 'Active Directory is a directory service where I manage users, groups, and computers. For example, I can create groups to control access to resources, and GPOs help me enforce security settings and software installations domain-wide.'"

---

2. DHCP, DNS, WINS

Concept Explanation: - DHCP: automatically assigns IP addresses - DNS: resolves domain names to IPs - WINS: resolves NetBIOS names (legacy)

Interview Answer: "DHCP automates IP allocation, DNS resolves domain names to IPs, and WINS resolves legacy NetBIOS names."

Delivery Example: "I would explain: 'DHCP ensures devices get IPs automatically, DNS translates website names to IP addresses, and WINS is used in older networks for NetBIOS name resolution.'"

---

3. Windows Firewall & Security Policies

Concept Explanation: - Firewall controls inbound/outbound traffic - Security policies enforce rules like password complexity, account lockout, and auditing

Interview Answer: "Windows Firewall filters traffic, while security policies control system behavior and enforce compliance across machines."

Delivery Example: "I would say: 'I use Windows Firewall to restrict network traffic and security policies to enforce standards like strong passwords, account lockout, and auditing events for compliance.'"

---

4. Event Viewer & Logging

Concept Explanation: - Event Viewer tracks system, security, and application events - Logs are crucial for troubleshooting, auditing, and monitoring

Interview Answer: "Event Viewer helps monitor and troubleshoot system, security, and application issues by analyzing logs."

Delivery Example: "I would explain: 'I use Event Viewer to check logs when users face authentication failures or system issues. For example, Security logs show failed login attempts, and System logs highlight hardware or service errors.'"

---

5. PowerShell Basics

Concept Explanation: - Task automation, system management, scripting - Cmdlets like Get-ADUser, Set-ADPassword, Get-Service, etc.

Interview Answer: "PowerShell is a command-line tool and scripting language used to automate administrative tasks in Windows."

Delivery Example: "I would say: 'PowerShell lets me automate tasks like resetting passwords, checking services, and retrieving system info. For example, Get-ADUser shows AD users, and Set-ADAccountPassword can reset a password.'"

---

6. File and Print Services

Concept Explanation: - File services: shared folders, NTFS permissions, DFS - Print services: managing network printers, queues, drivers

Interview Answer: "File and Print Services manage shared resources, access permissions, and printing across the network."

Delivery Example: "I would explain: 'I configure shared folders with NTFS permissions to control access, and manage network printers by adding them to Print Servers and managing queues efficiently.'"

---

7. Remote Desktop Services

Concept Explanation: - Provides remote access to desktops or applications - Used for administration and remote work

Interview Answer: "RDS allows users and admins to connect remotely to desktops or applications securely."

Delivery Example: "I would say: 'I use Remote Desktop Services to allow secure remote access to servers or applications for admins and users.'"

---

8. Backup & Recovery

Concept Explanation: - Windows Server Backup, System Restore, File History - Ensures data protection and recovery after failures

Interview Answer: "Backup and recovery ensure critical data and system configurations are protected and can be restored in case of failures."

Delivery Example: "I would explain: 'I schedule regular backups using Windows Server Backup, and configure recovery points so that in case of accidental deletion or system failure, data can be restored quickly.'"

Example Questions & Scenario Responses:

Q1: Reset a user password in AD? - Answer: Use ADUC GUI or PowerShell: Set-ADAccountPassword -Identity username - Delivery: 'I can reset a password via Active Directory Users and Computers or using PowerShell with Set-ADAccountPassword cmdlet, ensuring the user updates it at next login.'

Q2: Explain Group Policy Objects? - Answer: Enforce security, software, and configuration settings domain-wide - Delivery: 'GPOs help manage settings across users and computers. For example, I can enforce password policies or deploy software updates using GPOs.'

Q3: Troubleshoot DNS resolution issues? - Steps: Check IP config, ping DNS server, nslookup, check forwarders - Delivery: 'I verify the client's IP and DNS settings, ping the DNS server, use nslookup to test name resolution, and check server forwarders for proper configuration.'

Scenario 1: Users cannot log in; authentication failures - Steps: Check event logs, verify AD account status, reset password, check replication - Delivery: 'I would check Security logs in Event Viewer, confirm AD account is active, reset passwords if needed, and ensure domain controllers are replicating correctly.'

Scenario 2: Server running out of disk space - Steps: Check disk usage, delete unnecessary files, archive logs, expand volume if needed - Delivery: 'I would identify large files, clear temp and logs, move unused data to storage, and consider expanding the disk volume if required.'

Scenario 3: Deploy software update to all Windows servers - Steps: Use GPO, WSUS, or PowerShell scripting - Delivery: 'I would either deploy updates via WSUS for centralized management, use a GPO for scheduled deployment, or script the update using PowerShell for automation.'