**1. Windows Administration**

**Key Areas to Focus On**

* **Windows Server Basics**
  + Versions: Understand differences among Windows Server 2012, 2016, 2019, and 2022.
  + User Management: How to create, manage, and delete user accounts and groups.
  + Disk Management: Creating and managing partitions, understanding NTFS vs. ReFS, mounting drives.
  + File System and Permissions: NTFS permissions vs. Share permissions, inheritance, and folder security.
* **Common Administrative Tools**
  + **Event Viewer**: Monitoring logs (System, Application, Security).
  + **Task Scheduler**: Creating, managing tasks.
  + **PowerShell Basics**: Basic commands for administrative tasks, setting up scripts.
* **Remote Management**
  + RDP (Remote Desktop Protocol) basics, remote PowerShell.
  + Tools like Windows Admin Center, and an overview of SCCM (System Center Configuration Manager).

**2. Active Directory Basics**

**Topics to Cover**

* **Fundamental Concepts**
  + Understand **Domains, Trees, Forests**: Structure, purpose, and differences.
  + **Organizational Units (OUs)**: For managing users, computers, and other resources.
  + **Groups and Group Policies**: Types of groups (Security & Distribution), managing Group Policy Objects (GPOs) to control settings across users/computers.
* **Active Directory Users and Computers (ADUC)**
  + Managing users, groups, computers, resetting passwords, and enabling/disabling accounts.
* **Domain Controller (DC)**
  + What it is and its role in authentication.
  + Basics of replication between DCs, importance of Global Catalog.
* **Common Active Directory Tasks**
  + User and computer account management.
  + Basics of adding/removing Domain Controllers, FSMO roles (Flexible Single Master Operations).

**3. Troubleshooting Windows Server Issues**

**Key Troubleshooting Areas**

* **Basic Network Troubleshooting**
  + Using ipconfig, ping, tracert, netstat, and nslookup for diagnosing network issues.
  + DNS issues: Common causes and solutions, checking DNS registration, and troubleshooting name resolution issues.
* **Performance Monitoring**
  + Using **Task Manager** and **Resource Monitor** to check memory, CPU, disk usage.
  + **Event Viewer**: Looking for critical, error logs to diagnose common problems.
  + Performance Monitoring Tools: Basics of using Performance Monitor (perfmon) to analyze bottlenecks.
* **Common Windows Server Issues**
  + Disk space issues: Cleaning up, managing quotas.
  + Service failures: Checking and restarting Windows services, troubleshooting startup issues.
  + RDP Connection Issues: Checking network, firewall settings, and ensuring RDP is enabled.

**Preparation Tip**: Practice navigating Event Viewer, Services, Task Scheduler, and using PowerShell for basic commands like restarting services or checking disk usage.

**4. Intermediate AWS and Windows Security**

**AWS Security Basics**

* **IAM (Identity and Access Management)**
  + Roles, policies, and permissions: Differences between users, groups, and roles.
  + Key security best practices: MFA (Multi-Factor Authentication), least privilege access.
* **AWS Networking and Security**
  + VPC basics: Subnets, route tables, security groups, and network ACLs.
  + Key security services: Amazon GuardDuty, Inspector, and AWS WAF basics.
* **Data Protection**
  + Encryption in AWS: Basics of server-side vs. client-side encryption, using KMS (Key Management Service).
  + S3 security: Access policies, bucket policies, encryption, and logging.

**Windows Server Security Basics**

* **Windows Firewall**: Understanding firewall rules, configuring inbound/outbound rules.
* **Security Policies and Baselines**
  + Using **Local Security Policy** and **Group Policy** for enforcing security settings.
  + Password policies: Length, expiration, complexity settings.
* **Windows Defender**: Basics of Defender Antivirus, using the Security Center for regular scans, checking logs for threats.
* **Event Logging and Auditing**
  + Security logs in Event Viewer, enabling auditing for logons, file accesses, and configuration changes.
* **Patch Management**: Importance of regular updates, WSUS (Windows Server Update Services) overview for managing updates in Windows.

**Preparation Tips**

* **Practice**: Get hands-on practice with a Windows Server VM. You can set up a basic environment using AWS EC2 or Azure.
* **Mock Scenarios**: Write down common scenarios and steps to resolve them (e.g., a user can’t log in, high CPU usage).
* **Documentation**: Bookmark Windows and AWS security best practices, as they can be referenced during interviews.
* **PowerShell Commands**: Familiarize yourself with basic PowerShell commands for managing Active Directory and Windows Server.