**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.

### 1. Fundamental Concepts

#### Domains, Trees, and Forests

* **Domain**: A domain is a logical grouping of objects (like users, computers, and resources) that share a common directory database. Each domain has its own security policies and trust relationships.
* **Tree**: A tree is a collection of one or more domains that are connected in a hierarchical structure. The root domain of a tree can have child domains. For example, in a tree named example.com, you could have child domains like sales.example.com or hr.example.com.
* **Forest**: A forest is a collection of one or more trees that share a common schema and global catalog. Forests are used when you want to manage multiple domains with a common directory structure. Each tree in a forest can be independently managed but can also share information.

**Purpose and Differences**:

* **Structure**: Domains are the core unit, trees create a hierarchy, and forests allow for multiple trees to coexist.
* **Purpose**: Domains manage security and resource access; trees provide an organizational structure; forests allow for administrative boundaries and schema sharing.

#### Organizational Units (OUs)

* **Definition**: OUs are containers within a domain that can hold users, groups, computers, and other OUs. They allow for a more granular delegation of authority and policy application.
* **Purpose**: OUs help in organizing users and resources logically, making it easier to manage permissions and apply Group Policy settings.

**Example**: You could have OUs for each department (HR, Sales, IT) to apply specific policies relevant to each department.

#### Groups and Group Policies

* **Groups**:
  + **Security Groups**: Used to grant permissions to shared resources. They can contain users, computers, and other groups. They are used for access control.
  + **Distribution Groups**: Primarily used for email distribution lists and cannot be used for security permissions.
* **Group Policy Objects (GPOs)**: GPOs are used to manage settings across users and computers in an Active Directory environment. They can control various settings, including security policies, software installations, and user environment configurations.

**Example**: You might create a GPO that enforces a password policy across all users in the domain.

### 2. Active Directory Users and Computers (ADUC)

#### Managing Users and Groups

* **ADUC**: This is a Microsoft Management Console (MMC) snap-in that allows administrators to manage users, computers, and groups in Active Directory.
* **Key Tasks**:
  + **Creating Users**: You can create user accounts with specific attributes.
  + **Managing Groups**: Create, delete, and modify groups.
  + **Resetting Passwords**: Administrators can reset user passwords.
  + **Enabling/Disabling Accounts**: Control user access by enabling or disabling their accounts.

### 3. Domain Controller (DC)

#### Role of a Domain Controller

* **Definition**: A Domain Controller is a server that responds to security authentication requests within a Windows Server domain. It stores the Active Directory database and is responsible for allowing access to network resources.
* **Role in Authentication**: DCs authenticate users and computers in the domain, allowing access to resources based on permissions.

#### Basics of Replication

* **Replication**: DCs replicate directory information among themselves to ensure all DCs have the same data. This helps in load balancing and fault tolerance.
* **Global Catalog**: A Global Catalog server holds a partial replica of every object in the forest, allowing users to search for objects across all domains in the forest. It helps in locating users and resources efficiently.

### 4. Common Active Directory Tasks

#### User and Computer Account Management

* **Creating and Managing Accounts**: Administrators can create and manage user and computer accounts through ADUC.
* **Bulk Operations**: You can use PowerShell or CSV files to perform bulk import/export of user accounts.

#### Adding/Removing Domain Controllers

* **Adding DCs**: This involves installing the Active Directory Domain Services (AD DS) role and promoting the server to a Domain Controller.
* **Removing DCs**: If a DC is to be decommissioned, it should first be demoted to ensure that directory information is replicated properly and that no lingering objects remain.

#### FSMO Roles (Flexible Single Master Operations)

* **Definition**: FSMO roles are special roles assigned to one or more domain controllers to prevent conflicts and ensure data integrity.
* **Types of FSMO Roles**:
  1. **Schema Master**: Manages updates to the schema.
  2. **Domain Naming Master**: Manages the addition and removal of domains in the forest.
  3. **Relative ID (RID) Master**: Allocates RIDs to DCs for creating security principals (like users and groups).
  4. **PDC Emulator**: Acts as a primary domain controller for backward compatibility with Windows NT and handles password changes.
  5. **Infrastructure Master**: Updates references to objects in other domains.

**# Sound knowledge in security and ensuring AWS and it’s workloads are secured to best practices**

In securing AWS workloads, I prioritize implementing best practices that encompass the shared responsibility model, which divides security responsibilities between AWS and the customer. Here are some of the key practices I follow:

1. **Identity and Access Management (IAM)**:
   * **Principle of Least Privilege**: I ensure that users and services have the minimum permissions necessary to perform their tasks. This involves creating IAM roles and policies tailored to specific needs.
   * **Multi-Factor Authentication (MFA)**: I enable MFA for all users, especially those with administrative privileges, to add an extra layer of security.
2. **Network Security**:
   * **VPC Configuration**: I design Virtual Private Clouds (VPCs) with subnets that segment resources based on their security needs. I use public and private subnets appropriately to isolate sensitive workloads.
   * **Security Groups and NACLs**: I configure security groups and Network Access Control Lists (NACLs) to restrict inbound and outbound traffic to only what's necessary, reducing the attack surface.
3. **Data Protection**:
   * **Encryption**: I ensure that data at rest and in transit is encrypted using AWS services like AWS Key Management Service (KMS) for managing encryption keys. Services such as Amazon S3, RDS, and EBS support encryption natively.
   * **Backup and Recovery**: I implement automated backup solutions using AWS Backup and ensure that data can be quickly restored in case of an incident.
4. **Monitoring and Logging**:
   * **AWS CloudTrail**: I enable CloudTrail to log all API calls, providing an audit trail for monitoring and investigation purposes.
   * **Amazon CloudWatch**: I use CloudWatch for real-time monitoring of resources and setting up alerts for unusual activities or performance metrics.
5. **Compliance and Governance**:
   * **AWS Config**: I utilize AWS Config to assess, audit, and evaluate the configurations of AWS resources to ensure compliance with policies.
   * **Security Assessments**: Regularly conducting security assessments and audits to identify and mitigate vulnerabilities using tools like AWS Inspector and third-party security solutions.
6. **Incident Response**:
   * **Incident Response Plan**: I develop and maintain an incident response plan that outlines the steps to take during a security breach, ensuring that all stakeholders know their roles and responsibilities.
7. **Training and Awareness**:
   * **Regular Training**: I promote a culture of security awareness by providing regular training to team members about AWS security best practices and emerging threats.