**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 analyse bottlenecks.
* **Common Windows Server Issues**
  + Disk space issues: Cleaning up, managing quotas.
  + Service failures: Checking and restarting Windows services, troubleshooting start up 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 Centre 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 on AD.

#### 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.

* Suppose an organization has departments like **HR**, **Sales**, and **IT**.
* Each department can have its own OU, so you might create:
  + An "HR" OU for HR users and resources.
  + A "Sales" OU for the Sales team’s users and resources.
  + An "IT" OU for users, computers, and groups specific to the IT department.
* **Benefits**:
  + If there’s a policy for password complexity that HR and Sales need but IT does not, you can link a Group Policy to only the HR and Sales OUs. This applies the policy only to users within those OUs.
  + Additionally, you could delegate management of the HR OU to an HR administrator, allowing them to manage their users without needing domain-wide permissions.

### Summary

OUs help streamline **administrative control** and **policy management** by organizing resources within a domain logically. They allow you to apply targeted settings and delegate specific tasks, enhancing **security** and **efficiency** in managing the AD environment.

#### 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.

**Groups**

Groups are collections of **users, computers, or other groups**. They allow administrators to manage access permissions more efficiently by applying permissions at the group level instead of individually.

1. **Types of Groups**:
   * **Security Groups**:
     + **Purpose**: Used to control access to resources like files, folders, printers, and shared network drives.
     + **Example**: You might have a security group called "HR Access" that includes only HR users. You can then grant this group access to sensitive HR documents on the network, rather than assigning access to each user individually.
   * **Distribution Groups**:
     + **Purpose**: Primarily used for **email distribution lists**.
     + **Limitations**: Distribution groups cannot be used to assign security permissions to resources.
     + **Example**: A distribution group for "Sales Team" might be set up so that all members receive announcements by email.

**Group Policy Objects (GPOs)**

**GPOs** are used to apply specific configurations or policies to groups of users and computers within an AD environment.

1. **Purpose of GPOs**:
   * They allow administrators to **standardize settings** across the organization by applying policies to users or computers based on where they are located in the AD structure (such as at the domain, OU, or site level).
   * **Example Settings Managed by GPOs**:
     + **Security Policies**: Enforcing password complexity requirements, lockout settings, or restrictions on software installation.
     + **Software Installations**: Automatically install or update software on all computers in an OU.
     + **User Environment**: Setting desktop backgrounds, screen saver policies, or drive mappings.
2. **Example**:
   * Let’s say your organization requires a **strong password policy** for all employees. You could create a GPO that enforces this rule and link it to the **domain level** so it applies to every user account within the domain.
   * For a specific department, like IT, you might want to enforce different settings, like enabling remote management tools. You could create another GPO and link it specifically to the IT OU.

**Summary**

* **Groups** help organize users and computers for **easy management** of permissions.
* **GPOs** apply settings and enforce policies across users and computers in AD, allowing an administrator to control security, software, and environment settings efficiently.

|  |
| --- |
| **Policies** |

|  |
| --- |
| Group Policies can be applied to OUs |

|  |
| --- |
| Group Policies cannot be applied to groups |

### 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.

### 1. ****AD DS (Active Directory Domain Services)****

* **What it is**: AD DS is the **service or role** within Windows Server that provides the core directory services for managing identities (like users, computers, groups) and resources (like printers and shared folders) in a network.
* **Purpose**: AD DS helps manage permissions, authentication, and access to resources within an organization's network. It enables centralized management of user and computer accounts, enforces security policies, and provides a directory of information about network resources.
* **Components**: AD DS includes multiple components, such as domains, trees, forests, organizational units, and Group Policy Objects (GPOs).

### 2. ****AD DC (Active Directory Domain Controller)****

* **What it is**: An AD DC is the **physical or virtual server** where the AD DS service is installed and running. The domain controller hosts the AD DS database and is responsible for authenticating and authorizing users and computers within a domain.
* **Purpose**: The domain controller is essential for AD DS to function because it handles the actual processing of authentication and access requests within the domain. It stores a copy of the Active Directory database and replicates it with other domain controllers for high availability and fault tolerance.
* **Key Roles**: Domain controllers also hold **Flexible Single Master Operations (FSMO)** roles, which are specialized tasks that help maintain the integrity of the AD environment, such as the Schema Master or RID Master roles.

### Key Differences

* **AD DS (Domain Service)** is the **service** or **role** responsible for the directory and identity management structure.
* **AD DC (Domain Controller)** is the **server** that hosts this service and performs the core functions like authentication, replication, and directory updates.

In summary, **AD DS** provides the framework for directory services, while the **AD DC** is the actual server that delivers these services and handles requests within the Active Directory environment.

### 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.

The term "domain" can indeed refer to different concepts based on context. Here’s a breakdown of the difference:

**1. Domain from Hostinger (like learntechnology.cloud)**

* This is a **website domain** or **Internet domain**.
* It's the address people type into their browsers to access a specific website.
* Purchasing a domain from a provider like Hostinger essentially gives you ownership of that unique Internet address, making it easier for people to find your site (instead of typing in an IP address).
* Example: learntechnology.cloud is a unique name associated with a specific website on the Internet.

**2. Domain in IT or Directory Services (like in Active Directory)**

* This is a **network domain** often used in corporate or organizational IT environments, especially in systems like Active Directory.
* Here, a domain is a logical grouping of users, computers, and resources within a secure network.
* It’s used to manage resources and apply security policies across multiple devices and users under a single directory service.
* Each domain can have unique security policies and can establish trust relationships with other domains, allowing access to shared resources across different network segments.

So, in short:

* The **Hostinger domain** is a **public web address** used to access websites on the Internet.
* The **IT/network domain** is a **private, organizational structure** used within a network environment to manage and secure resources.

**Visualizing the Concept**

Think of a forest as a large university with multiple faculties:

* **Forest:** University
  + **Tree 1:** Faculty of Science
    - **Subdomains:** Department of Biology, Department of Chemistry
  + **Tree 2:** Faculty of Arts
    - **Subdomains:** Department of History, Department of Literature

This structure allows different faculties to operate independently while still being part of the same university.

**Forest:**  
**TechInnovationsCorp.com**  
(Think of this as the entire organization that encompasses all divisions and departments.)

**Tree 1:**  
**Engineering.TechInnovationsCorp.com**  
(This tree represents the engineering department within the organization.)

* **Root Domain:**  
  **Engineering.TechInnovationsCorp.com**
* **Subdomains:**
  + **Development.Engineering.TechInnovationsCorp.com**  
    (Handles software development projects.)
  + **QA.Engineering.TechInnovationsCorp.com**  
    (Responsible for quality assurance and testing.)
  + **DevOps.Engineering.TechInnovationsCorp.com**  
    (Manages infrastructure and deployment.)

**Tree 2:**  
**Sales.TechInnovationsCorp.com**  
(This tree represents the sales department within the organization.)

* **Root Domain:**  
  **Sales.TechInnovationsCorp.com**
* **Subdomains:**
  + **Domestic.Sales.TechInnovationsCorp.com**  
    (Handles domestic sales operations.)
  + **International.Sales.TechInnovationsCorp.com**  
    (Manages international sales strategies.)
  + **CustomerSupport.Sales.TechInnovationsCorp.com**  
    (Provides support for sales-related inquiries.)

In this example, each **root domain** (such as **Engineering.TechInnovationsCorp.com**, **Sales.TechInnovationsCorp.com**, and **HR.TechInnovationsCorp.com**) represents an **Active Directory (AD) domain** within the overall AD **forest** (TechInnovationsCorp.com).

**# 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.