**ASSIGNMENT**

**Assignment: Windows Server**

**Module 12: Installation, Storage, and Compute with Windows Server**

**1. What two options are provided in the type of installation window during Windows Server 2016 installation?**

**Answer:**

**During Windows Server 2016 installation, the "type of installation" window provides two main options:**

* Server Core: This is a minimal installation option without a full graphical user interface (GUI). It offers only a command-line interface (CLI) for management, focusing on reduced resource consumption and a smaller attack surface. Server Core is preferred for improved security and performance but requires administrators to use PowerShell or remote management tools.
* Desktop Experience: This option installs Windows Server 2016 with a full GUI, similar to regular Windows client systems. It includes the Start menu, taskbar, Control Panel, and Windows Explorer. Desktop Experience is suitable for scenarios needing a GUI for compatibility with certain applications, but it uses more resources and increases the server's attack surface.

You select either "Server Core" or "Desktop Experience" when prompted in the installation window, depending on your requirements for management interface and resource usage.

**2. Write the step How to configure server step by step?**

**Answer:**

**Here’s a step-by-step guide to configuring Windows Server 2016 after installation:**

1. Log in as Administrator

* Access the server console directly or via remote desktop and log in using your administrator credentials.

2. Set Static IP Address

* Go to Control Panel → Network and Sharing Center → Change adapter settings.
* Right-click your network adapter, select Properties.
* Set a static IP, subnet mask, gateway, and preferred DNS (usually your domain controller’s IP).

3. Rename the Computer

* Control Panel → System → Change Settings (next to computer name).
* Click “Change”, enter a unique server name, and restart the server to apply changes.

4. Join the Domain

* Control Panel → System → Change Settings → Member of Domain.
* Enter the domain name, supply domain administrator credentials.
* Restart the server after a successful join.

5. Update Group Policy

* Open PowerShell as administrator and run:

text

**(gpupdate /force)**

* Wait for policy update confirmation.

6. Add Server Roles and Features

* Open Server Manager from the Start menu.
* Use “Add Roles and Features” to install required roles (e.g. Web Server (IIS), Application Server) and features (.NET Framework, Active Directory module).
* Select relevant roles based on your use case and complete the feature installation. Often requires additional restarts.

7. Update Windows Server

* Use Windows Update to download and install security patches and updates.

8. Set Password Policies and Security Settings

* Configure policies for password complexity, account lockout, and auditing via Group Policy Management.

9. Configure NIC Teaming (if needed)

* If your server uses multiple network adapters, configure NIC Teaming for load balancing and failover.

10. Install Necessary Applications

* Install and configure additional applications (e.g. database services, backup tools) as needed for your environment.

11. Verify Server Activation

* Check system properties and activate Windows Server with a valid product key.

12. Backup Initial Configuration

* Set up and verify your backup solution before deployment.

These steps will set up the basic configuration for a new Windows Server 2016 deployment.

**3. What are the Pre installation tasks?**

**Answer:**

**Pre-installation tasks for Windows Server 2016 ensure a smooth and successful setup. Here are the key steps you should take before beginning the installation:**

1. Verify Hardware Requirements

* Ensure your server meets the minimum CPU, RAM, and disk space requirements for Windows Server 2016. Refer to Microsoft’s official documentation for specific requirements.

2. Collect Installation Media and Documentation

* Obtain a genuine Windows Server 2016 installation DVD/USB or ISO image.
* Gather relevant installation guides or manuals for reference.

3. Backup Important Data

* If upgrading or reinstalling on an existing system, backup all existing data to prevent loss.

4. Prepare BIOS and Firmware

* Update the server’s BIOS and firmware to the latest versions to ensure hardware compatibility with Windows Server 2016.

5. Configure Disk Array/Storage

* Check disk configurations (such as RAID setup or disk array) and confirm readiness for OS installation.

6. Gather Required Drivers and Starter Packs

* Download or collect drivers for your hardware and Starter Packs if required by your hardware vendor.

7. Plan Installation Type and Server Role

* Determine whether you will install Server Core or Desktop Experience based on your environment’s needs.
* Decide if the server will be a domain controller, file server, application host, or another role.

8. Prepare for Virtualization (if needed)

* If installing on a virtual machine, confirm compatibility with the hypervisor (e.g., VMware, Hyper-V), configure proper settings, and ensure the ISO is attached for boot.

9. Configure Network and Boot Order

* Set up network connections and peripherals.
* Adjust boot order in BIOS to prioritize booting from your installation media, either USB or DVD.

Completing these pre-installation tasks will greatly reduce the risk of interruptions or problems during Windows Server 2016 setup.

**4. What are the Post installation tasks?**

**Answer:**

After installing Windows Server 2016, there are several important post-installation tasks to configure your system for production use:

Post Installation Tasks Checklist

* Set Time Zone: Adjust the time zone to match your location for accurate logging and scheduling.
* Change Computer Name: Rename the server to a meaningful/unique hostname relevant to your environment.
* Check Network Card: Ensure the correct network adapter is enabled and functioning.
* Configure Static IP Address: Assign a static IP for reliable network connectivity and management.
* Turn On Remote Desktop: Enable Remote Desktop for remote administration if required.
* Configure Windows Firewall: Adjust firewall settings, and allow necessary traffic (e.g., ICMP/ping).
* Update Windows Server: Run Windows Update and install all critical and recommended patches.
* Join to Domain (if applicable): Add the server to your Active Directory domain if needed.
* Activate Windows Server: Enter your product key and activate the server.
* Disable Internet Explorer Enhanced Security Configuration: Optionally, turn it off to ease administration, but ensure strong security practices.
* Do Not Start Server Manager Automatically at Logon: Change this setting for performance or admin workflow preferences.
* Install and Update Device Drivers: Ensure all hardware device drivers are installed and up to date.
* Configure NIC Teaming (optional): For network redundancy and performance, configure NIC Teaming if multiple network adapters are present.
* Install Required Roles and Features: Use Server Manager or PowerShell to install roles such as Active Directory, DNS, DHCP, or IIS as required by your organization.
* Backup Initial Configuration: Set up regular backups before putting the server into production.

These steps are critical for ensuring your Windows Server 2016 is secure, functional, and ready for its designated role.

**5. What is the standard upgrade path for Windows Server?**

**Answer:**

The standard upgrade path for Windows Server follows a sequence where each version can only be upgraded directly to specific newer versions. You may sometimes need to perform multiple step upgrades if your current version is older:

| **Current Version** | **Upgrade To** | **Supported Directly?** |
| --- | --- | --- |
| Windows Server 2008 R2 | 2012, 2012 R2 | Yes |
| Windows Server 2012 | 2012 R2, 2016 | Yes |
| Windows Server 2012 R2 | 2016, 2019 | Yes |
| Windows Server 2016 | 2019, 2022, 2025 | Yes |
| Windows Server 2019 | 2022, 2025 | Yes |
| Windows Server 2022 | 2025 | Yes |

**Common Upgrade Paths**

**Example:**  
If you have Windows Server 2008 R2 and want to upgrade to 2019 or 2022, follow these steps:

* Upgrade to 2012 → 2016 → 2019 (sequentially; skipping versions is not supported).

**Key Points**

* Only 64-bit versions are supported for upgrades after 2008.
* You cannot skip major versions (e.g. 2008 R2 to 2019 directly); intermediary versions are required.
* Each upgrade step must be in place: install the next version using setup media and select the upgrade option (not a clean install).
* Always check Microsoft’s latest guidelines before upgrading as supported upgrade paths change with new releases.

This ensures compatibility and retention of roles, settings, and applications throughout the upgrade process.

**6. What is the Physical structure of AD?**

**Answer:**

The physical structure of Active Directory (AD) consists of components that represent the actual physical layout and organization of servers and network resources where AD data is stored and replicated.

The key physical components of AD are:

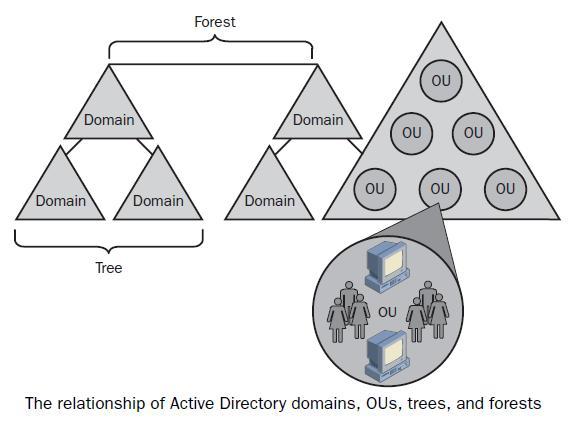
* Domain Controllers (DCs): These are servers running Windows Server with the Active Directory Domain Services (AD DS) role installed. They host the AD database and handle authentication, replication, and directory service requests. Each domain has one or more domain controllers.
* Sites: Sites are physical (not logical) groupings of IP subnets that represent the network topology. Sites help optimize replication traffic and client logon traffic by grouping physically well-connected computers. Sites are independent of domains and organizational units (OUs) and are shared across the forest.
* Global Catalog Servers: A type of domain controller containing a partial read-only copy of all objects in the forest for faster searches and logon processes across domains.
* Read-Only Domain Controllers (RODC): These are domain controllers that hold a read-only copy of the AD database, typically deployed in locations with less physical security to reduce risk.

In summary, the physical structure defines the servers (domain controllers), their role in replication and authentication, and the network infrastructure (sites) that affects replication and service efficiency.

This physical structure underpins the logical structure of AD (domains, trees, forests, OUs) which organizes and manages user and resource objects logically and administratively.

**7. What are the Logical components of Active Directory?**

**Answer:**

****

The logical components of Active Directory (AD) represent the organizational and administrative structure of the directory service. These components define how objects such as users, computers, and resources are logically grouped and managed in a hierarchical model, independent of the physical layout. Key logical components include:

* Forest: The top-level container in AD, consisting of one or more domain trees that share a common schema, configuration, and global catalog. It acts as the security boundary for all objects within it.
* Domain: A domain is a security and administrative boundary within a forest. It is a collection of objects (users, groups, computers) that share a common directory database, security policies, and trust relationships with other domains.
* Tree: A hierarchical collection of one or more domains that share a contiguous namespace. Domains in a tree are connected in a parent-child relationship.
* Organizational Units (OUs): Containers within domains used to organize objects for delegation of administrative control and application of group policies. OUs help manage and locate objects more efficiently.
* Schema: Defines the types of objects that can be created in AD and the attributes those objects can have. It is extensible, allowing additions of new object types and attributes.
* Partitions: Logical sections of the AD database for replication purposes including domain partitions, configuration partitions, and schema partitions.
* Global Catalog: An indexed, partial replica of all objects in the forest to facilitate searching across domains.
* Sites: Although primarily part of physical structure, sites can be considered logical containers grouping well-connected IP subnets to optimize replication and authentication traffic.
* Objects: The individual entities in AD, such as user accounts, computer accounts, printers, groups, etc. They are either container objects (that can contain other objects) or leaf objects (no child objects).

These logical components help organize and administer network resources, enforce security policies, delegate control, and facilitate efficient replication and querying across the directory.

**8. What is the Full form of LDAP?**

**Answer:** The full form of LDAP is Lightweight Directory Access Protocol.

**9. What is the location of the AD database?**

**Answer:**

The Active Directory (AD) database is stored by default in the following location on a domain controller:

Location:  
 **%systemroot%\NTDS folder, which is typically  
C:\Windows\NTDS**

The main database file is called ntds.dit, which contains all the AD data including domain, schema, configuration, and directory objects such as users and groups.

Alongside this database file, the folder also contains related files such as transaction logs and checkpoint files that help maintain database integrity.

It is a best practice to keep the AD database and logs on a separate disk partition from the operating system for performance and recovery reasons.

**10. What is child DC?**

**Answer:**

A child domain controller (child DC) is a domain controller that operates within a child domain, which is a subdomain under a parent domain in an Active Directory (AD) domain tree.

Key points about Child Domain Controllers:

* A child domain is a domain that exists below a parent domain in the hierarchy, with its name appended to the parent domain’s namespace (e.g., if the parent domain is company.com, a child domain might be dept.company.com).
* The child domain controller manages authentication, policies, and directory services specifically for the child domain.
* It maintains its own domain database, user accounts, security policies, and administrative boundaries, but is part of the larger forest and shares a two-way transitive trust with the parent domain.
* Child DCs replicate directory information within the child domain and also coordinate with domain controllers in the parent domain and other child domains.
* They play a crucial role in delegating administration and security control in large organizations by providing autonomy for departments, regions, or business units while maintaining a centralized directory infrastructure.

Thus, a child DC supports the management and security of a child domain as part of a hierarchical AD structure.

**11. Explain the term forest in AD**

**Answer:**

An Active Directory (AD) Forest is the highest-level logical container in an Active Directory environment. It is a collection of one or more domains that share a common schema, configuration, and global catalog. The forest acts as a security boundary and administrative framework encompassing all domains, users, computers, groups, and policies within it.

Key characteristics of an AD Forest:

* Contains multiple domains organized in trees that share a contiguous namespace or separate namespaces.
* Shares a common schema, which defines the object classes and attributes within AD.
* Shares a global catalog, which is an indexed repository of objects across all domains in the forest to facilitate searches.
* Defines security boundaries: by default, objects and users in one forest cannot access resources in another forest unless explicit trust relationships are set up.
* Supports centralized administration of policies and permissions while allowing domain-level autonomy.
* Enables an organization to manage complex networks, multiple domains, and geographic locations securely and efficiently.

In summary, the forest is the overarching container that contains all other Active Directory components, providing a unified namespace and security boundary for the entire directory service infrastructure.

**12. What is Active Directory? Check all that apply.**

**Answer:** Active Directory is:

* Microsoft's implementation of a directory server
* An LDAP-compatible directory server

It is not an open-source directory server, and it is primarily a Windows-based directory service.

So, the correct selections are:

* Microsoft's implementation of a directory server
* An LDAP-compatible directory server.

**13. When you create an Active Directory domain, what's the name of the default user account?**

**Answer:** Administrator

**14. AD domain provides which of the following advantages? Check all that apply**

**Answer:** Active Directory (AD) domain provides the following advantages:

* Centralized authentication
* Centralized management with GPOs (Group Policy Objects)

While AD may contribute to more detailed logging as part of its auditing and security features, this is not its primary advantage. Better performance is not a direct advantage of an AD domain itself; performance depends on various factors like hardware, network, and configuration.

So, the correct selections are:

* Centralized authentication
* Centralized management with GPOs.

**15. What are the minimum hardware requirements for installing Windows Server 2016?**

**Answer:** The minimum hardware requirements for installing Windows Server 2016 are:

* Processor: 1.4 GHz 64-bit processor (compatible with x64 instruction set and supporting features like DEP, NX bit)
* RAM: Minimum 512 MB; 2 GB is required for Server with Desktop Experience (GUI), with 4 GB recommended
* Disk Space: At least 32 GB of available hard disk space
* Network: Gigabit Ethernet adapter (10/100/1000baseT) recommended
* Optical Storage: DVD drive (if installing from DVD media)

Additional recommended specifications include ECC type RAM and more memory (e.g., 8 GB or higher) based on workload needs.

**16. Explain the different editions of Windows Server 2016 and their features.**

**Answer:** Windows Server 2016 is available in several editions; each designed for different types of businesses and workloads with varying features:

| Edition | Description & Features |
| --- | --- |
| Essentials | Aimed at small businesses with up to 25 users and 50 devices. It provides core server functionality with simplified management, but lacks advanced features like virtualization rights. |
| Standard | Suitable for physical or minimally virtualized environments. Includes all core Windows Server features, supports 2 Operating System Environments (OSEs) for virtualization, and basic containers support. |
| Datacenter | Designed for highly virtualized datacenter and cloud environments. Supports unlimited OSEs (virtual machines), advanced features like Storage Spaces Direct, Storage Replica, Shielded VMs, and software-defined networking. |

Key Feature Comparisons:

* Virtualization Rights:
  + Standard: Up to 2 VMs licensed per license.
  + Datacenter: Unlimited VMs per license.
* Containers: Both Standard and Datacenter support unlimited Windows Server containers.
* Shielded Virtual Machines: Only in Datacenter for improved VM security.
* Storage Replica and Spaces Direct: Available only in Datacenter edition.
* Nano Server: Supported in Standard and Datacenter with Software Assurance.

The Essentials edition is more limited and does not support some of the advanced capabilities found in Standard and Datacenter editions.

This modular approach helps organizations choose the edition that matches their scale, virtualization needs, and specific feature requirements.

**17. Walk through the steps of installing Windows Server 2016 using GUI mode.**

**Answer: Steps to Install Windows Server 2016 with GUI**

1. Boot from Installation Media  
   Insert the Windows Server 2016 DVD or USB installation media and boot your server from it.
2. Select Language and Preferences  
   In the initial setup screen, choose your language, time and currency format, and keyboard layout, then click Next.
3. Click "Install Now"  
   Begin the installation process by clicking the Install now button.
4. Enter Product Key  
   Enter your Windows Server 2016 product key to activate your copy. Click Next. You can skip activation and enter the key later if needed.
5. Select Windows Server 2016 Edition to Install  
   Choose the edition with Desktop Experience (this is the GUI mode) such as "Windows Server 2016 Standard (Desktop Experience)" or "Datacenter (Desktop Experience)". Click Next.
6. Accept License Terms  
   Read and accept the license terms, then click Next.
7. Choose Installation Type  
   Select Custom: Install Windows only (advanced) for a fresh installation.
8. Select Destination Disk  
   Pick the disk or partition where you want to install Windows Server 2016. You can create or format partitions here if required. Click Next.
9. Installation Starts  
   Windows will copy files, install features and updates, and complete the installation. This process may take some time, and the system will restart several times.
10. Configure Initial Settings  
    After reboot, you will be prompted to set an Administrator password. Enter and confirm the password, then complete the setup.
11. Log In  
    Use the Administrator account to log in to the server desktop with full GUI.
12. Post-Installation Configuration  
    Once logged in, configure network settings, activate Windows, install roles and features as per your requirements through Server Manager.

This completes the Windows Server 2016 installation in GUI mode, providing a full desktop experience for easier management.

**18. Describe the steps for installing Windows Server 2016 in Server Core mode.**

**Answer: Steps for Installing Windows Server 2016 in Server Core Mode**

1. Boot from Installation Media  
   Insert the Windows Server 2016 DVD or USB installation media and boot your server from it.
2. Select Language and Preferences  
   Choose language, time, and keyboard settings on the initial screen and click Next.
3. Click "Install Now"  
   Begin the installation by clicking the Install now button.
4. Enter Product Key  
   Enter your Windows Server 2016 product key or skip this step to activate later. Click Next.
5. Select Server Core Installation  
   Choose the edition of Windows Server 2016 labeled Server Core (e.g., "Windows Server 2016 Standard" or "Datacenter" without the "Desktop Experience" suffix). Click Next.
6. Accept License Terms  
   Agree to the license terms and click Next.
7. Choose Installation Type  
   Select Custom: Install Windows only (advanced) for a clean installation.
8. Select Disk/Partition  
   Choose the target disk or partition for installation. Format or create partitions if needed, then click Next.
9. Installation Process  
   Windows will copy the necessary files and install Server Core. Several restarts may occur during the process.
10. Initial Configuration  
    Upon first boot after installation, you'll receive a command-line interface (CLI) prompt. Use the sconfig tool to:

* Set the administrator password.
* Configure network settings (IP address, DNS).
* Join the server to a domain if needed.
* Enable Remote Desktop.
* Perform Windows Update and other configuration tasks.

1. Remote Management  
   Since there is no GUI, use PowerShell remoting, Remote Server Administration Tools (RSAT), or other management tools to administer the server remotely.

This Server Core installation reduces the server's attack surface and resource footprint, ideal for environments needing minimal overhead and higher security.

**19. How do you configure network settings during Windows Server 2016 installation?**

**Answer:** During Windows Server 2016 installation, basic network settings are usually set later after the initial install, but you can configure or change network settings through these steps after installation:

Configuring Network Settings in Windows Server 2016

1. Using GUI (Desktop Experience):
   * Open Control Panel → Network and Sharing Center → Change adapter settings.
   * Right-click the network adapter and select Properties.
   * Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.
   * Choose Use the following IP address and enter your static IP address, subnet mask, default gateway, and DNS servers.
   * Click OK to apply changes.
2. Using Server Core or Command Line:
   * Log in to the server CLI.
   * Use the sconfig utility:
     + Run sconfig and select option 8 for Network Settings.
     + Select the network adapter to configure.
     + Set the IP address, subnet mask, default gateway, and DNS servers as prompted.
   * Alternatively, use PowerShell commands:
     + View adapters:

Go to PowerShell

Type command “Get-NetAdapter”

* + - Set a static IP address:

Go to PowerShell

Type command “New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress "192.168.1.100" -PrefixLength 24 -Default Gateway "192.168.1.1"

* + - Set DNS servers:

Go to PowerShell

“Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 8.8.8.8,8.8.4.4”

1. Using PowerShell Remoting or Remote Tools:
   * From another machine, use PowerShell remoting or RSAT tools to configure network settings remotely.

These methods allow precise control over network settings essential for domain joining, communication, and management after Windows Server installation.

**20. Explain the process of promoting a Windows Server to a domain controller.**

**Answer:** Promoting a Windows Server to a Domain Controller (DC) involves installing the Active Directory Domain Services (AD DS) role and configuring the server to participate in an Active Directory domain. Here's the typical process:

Steps to Promote a Windows Server to a Domain Controller

1. Install the Active Directory Domain Services Role:
   * Open Server Manager.
   * Click on Manage → Add Roles and Features.
   * Proceed through the wizard until you reach the Server Roles page.
   * Select Active Directory Domain Services and click Next.
   * Complete the wizard and install the role. The server will prompt for a restart.
2. Promote the Server to Domain Controller:
   * After the AD DS role installation, a notification will appear in Server Manager. Click Promote this server to a domain controller.
3. Choose Deployment Operation:
   * Select one of the following:
     + Add a domain controller to an existing domain: Adds the server as an additional DC in an existing domain.
     + Add a new domain to an existing forest: Creates a new child domain.
     + Add a new forest: Creates a new root domain in a new forest.
4. Specify Domain Information:
   * For existing domains, enter the domain name.
   * For new domains or forests, provide the root domain name.
5. Set Domain Controller Options:
   * Choose Domain Controller capabilities (such as DNS server and Global Catalog).
   * Specify the forest or domain functional level.
   * Set DSRM (Directory Services Restore Mode) password.
6. Configure DNS Options:
   * If installing DNS, the wizard will configure basic DNS settings automatically.
7. Specify Additional Options:
   * Choose if this DC will be a read-only DC.
   * Specify paths for the AD database, log files, and SYSVOL folder or leave defaults.
8. Review and Confirm:
   * Review the configuration summary.
   * Click Next and then Install to start the promotion process.
   * The server will automatically reboot after promotion is complete.
9. Verify Domain Controller Status:
   * After reboot, log in with domain credentials.
   * Open Active Directory Users and Computers or run dcdiag from a command prompt to verify DC health.

This process sets up the server as a domain controller, enabling it to handle authentication, authorization, replication, and other directory services within the AD environment.

**21. Discuss the steps involved in upgrading from a previous version of Windows Server to Windows Server 2016.**

**Answer:** Steps for Upgrading to Windows Server 2016

1. Check Upgrade Compatibility and Path
   * Verify that your current Windows Server version supports in-place upgrade to 2016 (e.g., 2008 R2, 2012, or 2012 R2).
   * Consult Microsoft’s supported upgrade paths to confirm compatibility.
2. Backup Important Data and System State
   * Perform a full backup of critical data, system state, and configurations to prevent data loss in case of issues.
3. Review Installed Roles and Features
   * Check installed roles and features on the existing server. Some roles or features may not be supported or may require reconfiguration after upgrade.
4. Prepare Hardware and Software
   * Ensure hardware meets Windows Server 2016 requirements.
   * Update firmware, drivers, and BIOS to the latest versions.
5. Run Windows Server 2016 Setup
   * Launch the Windows Server 2016 installation media from the server.
   * Choose Upgrade installation type instead of a clean install.
6. Follow the Setup Wizard
   * Enter the product key and accept license terms.
   * The wizard will scan for installed applications, incompatible drivers, or roles and notify you of any upgrade blocking issues.
7. Complete Upgrade Process
   * Proceed with the upgrade, allowing the setup to copy files, install features and updates, and migrate existing data and settings.
   * The server will restart several times automatically during the upgrade.
8. Post-Upgrade Tasks
   * Verify that all roles and features are functioning correctly.
   * Install the latest cumulative updates and security patches for Windows Server 2016.
9. Check System Event Logs and Server Health
   * Review event logs for errors or warnings related to the upgrade.
   * Use tools like dcdiag and sfc /scannow to check domain controller and system health.
10. Backup the Upgraded System
    * Take a fresh backup of the upgraded server for disaster recovery.

Following these steps systematically will help ensure a successful upgrade of your Windows Server to the 2016 version with minimal downtime and risk.

**22. What is Active Directory Domain Services (AD DS), and what are its key components?**

**Answer:** Active Directory Domain Services (AD DS) is the core service within Microsoft's Active Directory technology. It provides a centralized system for managing and storing information about users, computers, services, and other resources on a network within a hierarchical structure.

AD DS stores data as objects and makes this information easy for administrators and users to find and use. It serves as the backbone for Windows domain networks by handling authentication, authorization, and directory services.

Key Components of AD DS:

* Domain Controllers (DCs): Servers that host the AD DS database, authenticate users, and enforce security policies.
* Domains: Logical groupings of objects such as users and devices that share a common database and security policies.
* Organizational Units (OUs): Containers within domains used for organizing objects and delegating administrative control.
* Trees and Forests: Hierarchical groupings of domains, where multiple domains form trees, and multiple trees form a forest sharing a common schema and configuration.
* Global Catalog: A distributed data repository containing a searchable partial replica of all objects in the forest to speed up searches and login.
* Replication: Mechanisms that synchronize AD DS data between domain controllers to ensure consistency.
* Security Principals: Objects such as users, groups, and computers that can be authenticated and authorized.
* Group Policy: Feature for centralized management and configuration of operating systems, applications, and user settings.
* DNS Integration: AD DS relies on the Domain Name System for locating domain controllers and services.

AD DS enables secure access control, centralized administration, and efficient resource management in Windows network environments.

**23. How do you create a new Active Directory user account in Windows Server?**

**Answer:** To create a new Active Directory user account in Windows Server, follow these steps:

Using Active Directory Users and Computers (ADUC) Console (GUI):

1. Open Active Directory Users and Computers:
   * Click Start, then Administrative Tools (or just search for Active Directory Users and Computers).
   * Open the Active Directory Users and Computers console.
2. Select the Target Organizational Unit (OU):
   * In the left pane, browse to the domain and choose the OU or container where you want to create the new user.
3. Create New User:
   * Right-click the chosen OU, select New → User.
4. Enter User Details:
   * In the New Object - User wizard, enter the First name, Last name, User logon name (username), then click Next.
5. Set Password:
   * Enter and confirm the user's password.
   * Choose password options such as:
     + User must change password at next logon.
     + User cannot change password.
     + Password never expires.
     + Account is disabled.
6. Finish Creation:
   * Click Next and then Finish to create the user account.

Using PowerShell:

* Open PowerShell as Administrator and use the following command syntax:

**PowerShell**

New-ADUser -Name "Mohit S Varma" -GivenName "Mohit" -Surname "Varma" -SamAccountName "msvarma" -UserPrincipalName "msvarma@domain.com" -Path "OU=Users, DC=domain, DC=com" -AccountPassword (ConvertTo-SecureString "Password123!" -AsPlainText -Force) -Enabled $true

* Set the user to change password at next logon:

**PowerShell**

Set-ADUser -Identity "msvarma" -ChangePasswordAtLogon $true

These steps let you create and configure a new user account in Active Directory on Windows Server.

**24. Explain the process of creating and managing Group Policy Objects (GPOs) in Windows Server 2016 or 2019.**

**Answer:** Creating and managing Group Policy Objects (GPOs) in Windows Server 2016 or 2019 involves using the Group Policy Management Console (GPMC) to define and enforce settings across users and computers in an Active Directory environment.

Here’s the process:

Steps to Create and Manage GPOs:

1. Open Group Policy Management Console (GPMC):
   * On a domain-joined Windows Server, open Server Manager → Tools → Group Policy Management.
2. Navigate to the Desired Scope:
   * In the GPMC console tree, expand Forest → Domains → Your domain.
   * Decide where to link the GPO: you can link it to the domain, a specific Organizational Unit (OU), or a site.
3. Create a New GPO:
   * Right-click the domain or OU where you want the GPO applied, then choose Create a GPO in this domain, and link it here.
   * Provide a descriptive name for the GPO and click OK.
4. Edit the GPO:
   * Right-click the newly created GPO and select Edit. This opens the Group Policy Management Editor.
   * Configure settings under Computer Configuration and User Configuration:
     + Policies include settings for Windows components, security settings, software installation, scripts, folder redirection, and administrative templates.
5. Scope and Filtering:
   * Use the Scope tab in the GPMC to specify which users, groups, or computers the GPO should apply to by setting security filtering or WMI filtering.
6. Enforce or Block Inheritance:
   * You can enforce a GPO to ensure it takes precedence or block inheritance on certain OUs/domains if necessary.
7. Test and Apply GPO:
   * GPOs are applied during computer startup or user logon. Use gpupdate /force command on client machines to refresh policies immediately.
   * Use tools like gpresult or RSOP (Resultant Set of Policy) to diagnose applied policies.
8. Manage Existing GPOs:
   * Modify settings, rename, backup, restore, or delete GPOs within GPMC.
   * Backup important GPOs regularly for recovery.

Summary

GPOs allow centralized and granular control over the environment, helping with security, configuration management, software deployment, and user experience across multiple devices in the network. The two options provided in the type of installation window during Windows Server 2016 installation are:

* Server Core Installation: A minimal installation without a graphical user interface (GUI); suitable for advanced users who want a lightweight, command-line-only environment.
* Server with Desktop Experience: A full installation with a GUI, also known as the Desktop Experience, suitable for users who prefer managing the server with a graphical interface.

**25. What are Organizational Units (OUs) in Active Directory, and how do you use them?**

**Answer:**

Organizational Units (OUs) are container objects within an Active Directory (AD) domain used to logically organize and manage network resources such as user accounts, groups, computers, and other AD objects. OUs help mirror the organization's functional or hierarchical structure, such as departments, locations, or roles.

Key Characteristics:

* OUs can be nested inside other OUs, creating a hierarchical structure.
* They are the smallest administrative units where Group Policy Objects (GPOs) can be applied and administrative control can be delegated.
* OUs enable delegated administration, allowing specific users or groups to manage only the objects within that OU.
* They help apply targeted group policies for centralized and efficient network management.

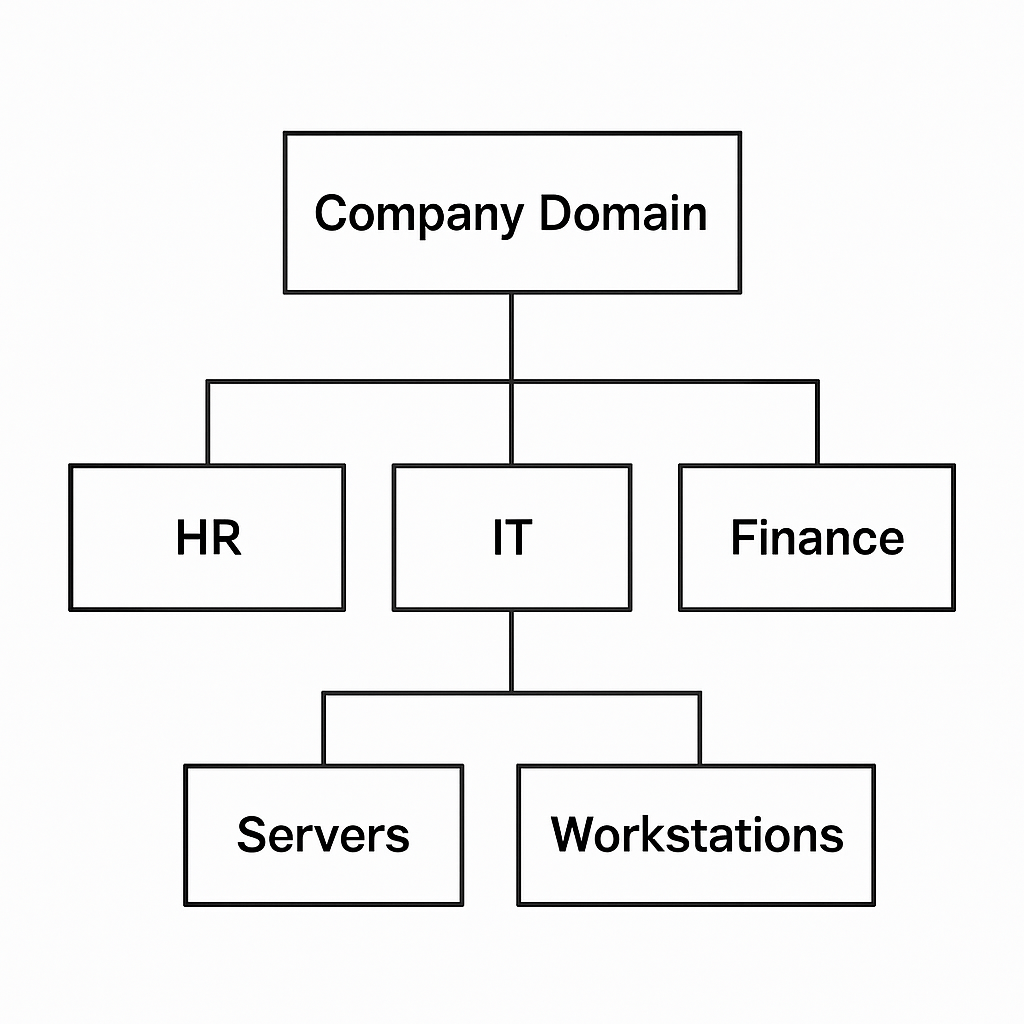
How to Use Organizational Units:

* Group related objects: Group users, computers, and other resources based on department, location, function, or security requirements.
* Delegate administrative rights: Assign administrative privileges to specific users or IT staff for managing only the resources inside their OU.
* Apply Group Policies: Link GPOs to OUs to enforce security settings, software deployment, and system configurations only on the objects within that OU.
* Simplify management: By structuring OUs logically, large networks become easier to manage and control.

Example:

An organization could have an OU structure like this:

Company Domain



Each OU can have different group policies and delegated permissions tailored for the needs of that unit.

By using OUs, administrators can efficiently organize resources, streamline management, and implement security policies across different parts of the organization.

**26. Describe the process of delegating administrative privileges in Active Directory.**

**Answer:** The process of delegating administrative privileges in Active Directory involves granting specific permissions to users or groups to manage certain aspects of AD without giving them full administrative rights.

Here’s how you can do it:

Steps to Delegate Administrative Privileges in Active Directory:

1. Open Active Directory Users and Computers (ADUC):
   * Launch the Active Directory Users and Computers console from Server Manager or search.
2. Select the Organizational Unit (OU) or Container:
   * Navigate to the OU or container where you want to delegate control (for example, an OU containing user accounts).
3. Right-click and Choose “Delegate Control”:
   * Right-click the selected OU and click Delegate Control to launch the Delegation of Control Wizard.
4. Start the Delegation of Control Wizard:
   * Click Next on the welcome page.
5. Add Users or Groups:
   * Click Add, enter the user or group name to whom you want to delegate administrative privileges, then click OK and Next.
6. Select Tasks to Delegate:
   * Choose from predefined common tasks such as:
     + Create, delete, and manage user accounts
     + Reset user passwords and force password change at next logon
     + Read user information
     + Modify group membership
     + Join computers to the domain
   * Alternatively, select Custom task to delegate for more granular permissions.
7. Complete the Wizard:
   * Review the summary of delegated permissions and click Finish.
8. Verify Delegated Permissions:
   * To check the permissions granted, right-click the OU, go to Properties → Security tab → Advanced.
   * View the Access Control Entries (ACEs) to see permissions assigned to the delegated users or groups.

Delegating control helps distribute administrative responsibilities securely and efficiently, reducing the risk of accidental or malicious changes to Active Directory.