1. Installation Options in Windows Server 2016
During the installation of Windows Server 2016, two options are typically provided:

Server Core: A minimal installation option without a graphical user interface (GUI) intended for remote management and enhanced security.
Desktop Experience: A full installation with a GUI that includes additional features and is suitable for users who prefer a more traditional Windows interface.

2. Steps to Configure Server Step by Step
Initial Setup: After installation, set the server's hostname using PowerShell or the System Properties.
Configure IP Address: Set a static IP address, subnet mask, and default gateway through the Network Connections.
Join Domain: If applicable, join the server to an Active Directory domain.
Configure Windows Firewall: Set up the firewall rules to allow necessary traffic.
Install Roles and Features: Use the Server Manager to add roles and features needed for your server's purpose (e.g., DNS, DHCP, etc.).
Update Server: Run Windows Update to ensure the server is up to date.
Configure Backup: Set up a backup solution for data protection.

3. Pre-Installation Tasks
Check Hardware Compatibility: Ensure the server hardware meets the system requirements.
Backup Existing Data: If upgrading or replacing a server, back up all important data.
Plan IP Addressing: Determine the static IP configuration for the server.
Gather Software Licenses: Ensure you have the necessary licenses for Windows Server and any additional software.
Decide Installation Type: Choose between Server Core and Desktop Experience.

4. Post-Installation Tasks
Activate Windows: Ensure Windows is activated using a valid product key.
Configure Remote Access: Set up Remote Desktop or other remote management tools.
Implement Security Policies: Configure local security policies and user permissions.
Install Updates: Check for and install the latest Windows updates.
Configure Monitoring: Set up monitoring tools to track server performance and health.
5. Standard Upgrade Path for Windows Server
The standard upgrade path generally follows:
Windows Server 2012 R2 → Windows Server 2016
Windows Server 2016 → Windows Server 2019
Windows Server 2019 → Windows Server 2022

6. Physical Structure of Active Directory
The physical structure of Active Directory (AD) consists of:
Domain Controllers (DC): Servers that host AD services and database.
Sites: Representing the physical (geographical) locations of DCs to manage replication efficiently.

7. Logical Components of Active Directory
The logical components of AD include:

Domains: The basic unit of organization in AD.
Trees: A collection of one or more domains that share a contiguous namespace.
Forests: A collection of trees that share a common schema and global catalog.
Organizational Units (OUs): Containers used to organize users, groups, and devices.
8. Full Form of LDAP
LDAP stands for Lightweight Directory Access Protocol.

9. Location of the AD Database
The Active Directory database is stored in the NTDS.dit file, typically located in the directory:

10. Child DC
A Child Domain Controller (DC) is a domain controller that exists in a child domain of a parent domain within a forest, allowing for more granular control over security and policy.

11. Forest in AD
A Forest in Active Directory is the topmost logical container that includes one or more domain trees. It defines the security boundary and encompasses all domains, their trees, and organizational units, sharing a common schema and global catalog

12. What is Active Directory? Check all that apply.
A Windows-only implementation of a directory server: ✔
Microsoft's implementation of a directory server: ✔
An LDAP-compatible directory server: ✔
Note: Active Directory is not open-source.

13. Default User Account in Active Directory Domain
The name of the default user account when you create an Active Directory domain is:

Administrator: ✔

14. Advantages of AD Domain
AD domain provides the following advantages:

Centralized Management: Allows for centralized management of users, computers, and resources.
Security Policies: Facilitates the implementation of security policies across the network.
Single Sign-On (SSO): Enables users to authenticate once and access multiple resources.
Scalability: Supports a scalable architecture for large and complex environments.
Group Policy Management: Provides tools to enforce settings and configurations across multiple devices.

15. Minimum Hardware Requirements for Installing Windows Server 2016

Processor: 1.4 GHz 64-bit processor.
RAM: Minimum of 512 MB (2 GB for Server with Desktop Experience).
Disk Space: At least 32 GB (more space may be required for certain roles).
Network Adapter: Gigabit (10/100/1000base-T) Ethernet adapter.
Firmware: UEFI firmware that supports Secure Boot.

16. Editions of Windows Server 2016 and Their Features
Windows Server 2016 Essentials:

Designed for small businesses.
Supports up to 25 users and 50 devices.
No virtualization rights.
Windows Server 2016 Standard:

For physical or minimally virtualized environments.
Supports two virtual instances (VMs) with the purchase of additional licenses.
Basic features for networking and storage.
Windows Server 2016 Datacenter:

Designed for highly virtualized data centers and cloud environments.
Unlimited virtual instances.
Advanced features like Storage Spaces Direct and Shielded Virtual Machines.

17. Steps for Installing Windows Server 2016 Using GUI Mode
Boot from Installation Media: Insert the installation DVD/USB and boot from it.
Select Language and Preferences: Choose your language, time, and keyboard input.
Click "Install Now": Start the installation process.
Enter Product Key: Enter your Windows Server 2016 product key.
Select Installation Type: Choose between “Server Core” or “Desktop Experience”.
Accept License Terms: Agree to the Microsoft license terms.
Select Installation Destination: Choose the disk/partition where you want to install.
Configure Settings: Follow the prompts to configure regional and server settings.
Complete Installation: Wait for the installation to finish and reboot.

18. Steps for Installing Windows Server 2016 in Server Core Mode
Boot from Installation Media: Use a bootable DVD/USB.
Select Language and Preferences: Choose your preferred settings.
Click "Install Now": Start the installation.
Enter Product Key: Provide your Windows Server 2016 product key.
Select Installation Type: Choose "Server Core" from the options.
Accept License Terms: Agree to the terms.
Select Installation Destination: Choose the disk for installation.
Complete Installation: Wait for the installation to finish; the server will reboot into Server Core.

19. Configuring Network Settings During Installation
During the installation process, after the OS has been installed and upon the first boot:
Use PowerShell or the Command Prompt to configure the IP address.

For example, use the command New-NetIPAddress to set a static IP or modify existing settings through the Network Connections interface.

20. Promoting a Windows Server to a Domain Controller
Open Server Manager: Launch Server Manager after the installation.
Add Roles and Features: Click on “Add roles and features”.
Select Active Directory Domain Services: Choose the AD DS role.
Install the Role: Follow the prompts to install.
Promote to Domain Controller: After installation, click on the notification flag in Server Manager and select “Promote this server to a domain controller”.
Choose Deployment Configuration: Select whether to add a domain controller to an existing domain or create a new domain.
Configure Domain Controller Options: Set the domain name, forest functional level, and Directory Services Restore Mode (DSRM) password.
Complete the Wizard: Review the settings and finish the promotion process, then reboot the server.

21. Upgrading from a Previous Version of Windows Server to Windows Server 2016
Check Compatibility: Ensure that the existing version can be upgraded (e.g., Windows Server 2012 R2).
Backup Data: Always back up critical data and system settings.
Run the Installation Media: Boot from the Windows Server 2016 installation media.
Select Upgrade: Choose the upgrade option during installation.
Follow the Prompts: Follow the on-screen instructions, ensuring that you choose to keep files and applications.
Complete Upgrade: Wait for the upgrade to complete and reboot the server.

22. Active Directory Domain Services (AD DS) and Its Key Components
AD DS is a directory service that provides a variety of network services, including:

User and Computer Accounts: Managing identities and permissions.
Group Policies: Configuring user settings and security policies.
Domain Controllers: Servers that handle authentication and directory requests.
Replication: Synchronizing data across multiple domain controllers.

23. Creating a New Active Directory User Account
Open Active Directory Users and Computers: From Server Manager or by running dsa.msc.
Navigate to the OU: Right-click on the desired Organizational Unit (OU).
Select New > User: Fill in the user details such as first name, last name, and logon name.
Set Password: Specify a password and configure options like "User must change password at next logon".
Finish Creation: Click “Finish” to create the account.

24. Creating and Managing Group Policy Objects (GPOs)
Open Group Policy Management Console: Launch gpmc.msc.
Create a New GPO: Right-click on the domain or OU, select “Create a GPO in this domain, and Link it here”.
Edit the GPO: Right-click the GPO and select “Edit” to configure settings.

Link GPO: Ensure the GPO is linked to the appropriate domain or OU.
Test and Apply: Use the “gpresult” command to verify application and functionality.

25. Organizational Units (OUs) in Active Directory
OUs are containers used to organize users, groups, and computers within a domain. They help:

Delegate Administration: Assign permissions to manage specific OUs without granting full domain access.
Apply Group Policies: Link GPOs to OUs to enforce specific policies.
Organize Resources: Structure the AD hierarchy based on business needs or department.

26. Delegating Administrative Privileges in Active Directory
Open Active Directory Users and Computers: Run dsa.msc.
Right-click on the OU: Select the OU where you want to delegate permissions.
Select “Delegate Control”: This opens the Delegation of Control Wizard.
Add User or Group: Specify the user or group to whom you want to delegate permissions.
Select Tasks: Choose specific tasks to delegate (e.g., managing user accounts, resetting passwords).
Finish the Wizard: Review and apply the delegation settings.