Active Directory: Objects and Containers

1. What is Active Directory Domain Services (AD DS)?

Active Directory Domain Services (AD DS) is a core component of Windows Server that enables centralized management of network resources. It provides:

- **Authentication** – Verifies user identity.
- **Authorization** – Grants access to resources.
- **Directory Services** – A structured database to store information about users, computers, and other resources on the network.

AD DS allows administrators to manage users, computers, groups, and security policies across a network from a single point.

2. Active Directory Objects

Objects are the core items stored within Active Directory. Each object represents a real-world resource, and AD manages their attributes and permissions.

Common Object Types:

- **Users** – Represent people who need access to the network. Each user has a unique username and password.
- **Computers** – Devices joined to the domain. Each has a computer account managed by AD.
- **Groups** – Collections of users, computers, or other groups. Used to assign permissions collectively.
- **Shared Folders** – Folders accessible over the network, often with defined permissions.
- **Printers** – Network printers made available to domain users.

Objects can be managed individually or grouped using containers for ease of administration.

3. Active Directory Containers

Containers are logical structures used to group and organize AD objects. They help in managing policies and delegating administrative control.

Types of Containers:

- **Domain** – The highest-level container in Active Directory. A domain is a logical boundary for security and administrative control.
- **Sites** – Represent physical locations in the network. They help optimize traffic and replication between domain controllers.
- **Organizational Units (OUs)** – Custom containers used to organize users, groups, and computers. OUs make it easy to apply Group Policies and delegate control to specific administrators.

4. Domain Environment Structure

- A **Windows Server (e.g., Server 2016)** typically acts as the **Domain Controller (DC)**. It holds a copy of the AD database and provides login/authentication services.
- Multiple **Client PCs** (computers) are joined to the domain. They rely on the Domain Controller for access to resources and policies.
- A central network switch or logical connection point enables communication between the server and clients.

In this structure:

- The domain controller manages all the domain objects.
- Client PCs authenticate against the domain controller to access resources.
- Administrators can manage users and apply policies across all machines centrally.

✅ How to Implement Active Directory (AD DS)

🔧 Step 1: Prepare Your Environment

1. **Choose a Windows Server version** (e.g., Windows Server 2016, 2019, or 2022).
2. **Hardware Requirements**:

- At least 2 CPU cores
- 4 GB RAM minimum (8+ GB recommended)
- 40+ GB disk space

3. **Static IP Address**:
    - Assign a **static IP** to the server (e.g., `192.168.1.10`).

🛠️ Step 2: Install Active Directory Domain Services (AD DS)

1. **Open Server Manager**.
2. Click on **"Add roles and features"**.
3. Select:
    - **Role-based or feature-based installation**
    - Choose the local server
4. In the **Roles** section:
    - Check **Active Directory Domain Services**
5. Complete the wizard and click **Install**.

🚀 Step 3: Promote the Server to a Domain Controller

1. After AD DS installs, click the **"Promote this server to a domain controller"** option.
2. Choose:
    - **Add a new forest** (if this is the first domain)
    - Enter your root domain name (e.g., `class.com`)
3. Set a **Directory Services Restore Mode (DSRM)** password.
4. Proceed through the wizard and click **Install**.
    - The server will reboot.

🏗️ Step 4: AD DS is Ready – Configure Basic Settings

After reboot:

1. Log in with **domain credentials** (e.g., `class\Administrator`).
2. Open **Active Directory Users and Computers** (ADUC).
3. Create:
    - **Users**
    - **Organizational Units (OUs)**
    - **Groups**
    - **Computer accounts** (optional—will be created automatically when joining PCs)

🖥️ Step 5: Join Client PCs to the Domain

On each Windows client PC:

1. Go to **System > About > Rename this PC (Advanced)**.
2. Click **Change** > select **Domain**, and enter `class.com`.
3. Enter domain admin credentials when prompted.
4. Reboot the PC.

After reboot, users can:

- Log in using **domain credentials**
- Access network resources

🛡️ Step 6: Apply Group Policies (Optional but Recommended)

1. Open **Group Policy Management** on the server.
2. Create or edit policies to:
    - Enforce password rules

    - Map network drives
    - Block/control apps
    - Deploy software
3. Link policies to specific **OUs** (like `Students`, `Staff`, `IT`, etc.).

📊 Step 7: Monitor and Maintain

- Use tools like:
    - **Event Viewer** – for logging
    - **AD Administrative Center** – for enhanced management
    - **PowerShell** – for scripting and automation
- Perform **regular backups** of the AD database.
- Keep your domain controller updated and patched.

🔁 (Optional) Add Additional Domain Controllers

For redundancy and load balancing:

- Set up another Windows Server
- Join it to the domain
- Promote it as a **secondary Domain Controller**

🧪 Bonus: Test Setup in a Virtual Lab

You can practice all the above steps in a virtual lab using:

- **VirtualBox** or **VMware**
- One virtual machine for the server (DC)
- One or more virtual machines as clients