**Scenario: You are setting up an Active Directory Domain for a small office network to manage user logins and share resources securely.**

**Step 1: Prepare the Environment**

1. **Hardware/Software Requirements**:
   * A computer/server with at least:
     + 2 GHz processor
     + 4 GB RAM (8 GB recommended)
     + 40 GB free disk space
   * Windows Server operating system (e.g., Windows Server 2019 or 2022).
   * A static IP address for the server.
2. **Set Up a Virtual Machine (Optional)**: If you don't have a physical server, you can set up a virtual machine (VM) using tools like VMware Workstation or Hyper-V.

**Step 2: Install Windows Server**

1. Install the Windows Server operating system on the server or virtual machine.
2. During installation:
   * Set a strong administrator password.
   * Choose appropriate time and regional settings.

**Step 3: Configure a Static IP Address**

1. Open **Control Panel > Network and Sharing Center > Change Adapter Settings**.
2. Right-click your network connection > **Properties**.
3. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
4. Enter:
   * **IP Address**: Example: 192.168.1.10
   * **Subnet Mask**: Example: 255.255.255.0
   * **Default Gateway**: Example: 192.168.1.1
   * **Preferred DNS Server**: Use the server's IP address (e.g., 192.168.1.10).

**Step 4: Install Active Directory Domain Services (AD DS) Role**

1. Open **Server Manager**.
2. Click **Manage > Add Roles and Features**.
3. Follow the wizard:
   * Select **Role-based or feature-based installation**.
   * Choose the current server.
   * Check **Active Directory Domain Services** and click **Next**.
4. Allow the wizard to install required features and click **Install**.

**Step 5: Promote the Server to a Domain Controller**

1. After the AD DS role is installed, click the notification flag in Server Manager and select **Promote this server to a domain controller**.
2. Choose:
   * **Deployment Type**: Select **Add a new forest**.
   * **Root Domain Name**: Enter your domain name (e.g., example.com).
3. Configure:
   * **Forest Functional Level**: Choose the latest compatible version (e.g., Windows Server 2016).
   * Set a Directory Services Restore Mode (DSRM) password.
4. Review settings and click **Install**.

**Step 6: Configure Active Directory**

1. After the server restarts, log in with the domain administrator account.
2. Open **Active Directory Users and Computers (ADUC)**:
   * Click **Start > Administrative Tools > Active Directory Users and Computers**.
3. Create organizational units (OUs) to organize resources:
   * Right-click your domain > **New > Organizational Unit**.
4. Create user accounts:
   * Right-click the OU > **New > User**.
   * Enter user details, set a password, and click **Next**.
5. Create groups for easier management:
   * Right-click the OU > **New > Group**.
   * Name the group (e.g., "IT Team") and set the scope/type.

**Step 7: Add Computers to the Domain**

1. On a client machine (Windows 10/11):
   * Go to **Settings > System > About > Join a domain**.
2. Enter the domain name (e.g., example.com) and click **Next**.
3. Enter the credentials of a domain administrator.
4. Restart the computer to apply changes.

**Step 8: Test Your Configuration**

1. Log into a client machine using a domain user account.
2. Verify:
   * The user can access shared resources.
   * Policies applied via Group Policy Object (GPO) are functioning.

**Next Steps for Advanced Learning**

1. Configure Group Policy for centralized management.
2. Set up DNS and DHCP services if not already done.
3. Explore other roles like File Server and Print Server.