Active Directory Intial Setup

WE Innovate X Zero$ploit

Supervised By : Zeyad Mazen

Prepared By : Omar Hassan

Active Directory Setup

In this scenario, we are tasked with setting up and configuring Active Directory (AD) in a Windows Server environment using Packet Tracer or a virtualized lab. Active Directory will allow centralized management of users, computers, and security policies, while enabling authentication and access control within the domain.

Topology Requirements

- 1 Windows Server (acting as Domain Controller)
- 1 Switch
- 10 Client PCs (Windows 10/11)
- 1 Router (optional, if connecting to external networks)
- All devices should be on the same subnet for domain communication

Server Preparation

Before configuring Active Directory, ensure the Windows Server machine is properly set up:

- Assign a static IP address to the server.
- Configure the hostname (e.g., DC1).
- Verify network connectivity between the server and client PCs.

Step 1: Install Active Directory Domain Services (AD DS)

1. Open **Server Manager**.
2. Click **Manage > Add Roles and Features**.
3. In the wizard, select **Active Directory Domain Services (AD DS)** and complete the installation.
4. Once installed, a notification will appear to promote the server to a domain controller.

Step 2: Promote Server to Domain Controller

1. In **Server Manager**, click the notification flag and choose **Promote this server to a domain controller**.
2. Select **Add a new forest** and specify a root domain name (e.g., company.local).
3. Set a **Directory Services Restore Mode (DSRM)** password.
4. Complete the wizard and restart the server.

Step 3: DNS Configuration

During domain controller promotion, DNS services are installed automatically. Verify DNS by ensuring:

- The domain controller has a loopback DNS entry (127.0.0.1).
- Client PCs are configured to use the domain controller’s IP address as their primary DNS.

Step 4: Create Users and Organizational Units (OUs)

1. Open **Active Directory Users and Computers** from Administrative Tools.
2. Create Organizational Units (e.g., HR, Sales, IT).
3. Add users inside each OU and assign them to security groups as needed.
4. Apply Group Policies (via Group Policy Management) for centralized control.

Step 5: Join Client PCs to the Domain

On each Windows 10/11 PC:

1. Open **System Properties** (Win+Pause > Change Settings).
2. Click **Change**, select **Domain**, and enter the domain name (e.g., company.local).
3. Provide domain administrator credentials when prompted.
4. Restart the PC to apply changes.
5. Verify login using a domain account.

Verification & Testing

Once setup is complete:

- Ping the domain controller from client PCs to verify connectivity.
- Log in with a domain user account on client PCs.
- Test Group Policy application (e.g., password policies, desktop restrictions).
- Verify DNS resolution within the domain.