Active Directory

Introduction to Active Directory (AD)

Active Directory (AD) is Microsoft's directory service for **managing users, computers, and resources** in a network.

Purpose:

- **Centralized authentication** – One username/password works across the network.
- **Centralized management** – Admins can control computers, users, and policies from one place.
- **Resource organization** – Easier to find and manage printers, shared folders, applications.

Key Components:

1. **Domain** – Logical boundary for the network
2. **Domain Controller (DC)** – Server that runs AD and stores user/computer information.
3. **Organizational Units (OUs)** – Containers for organizing objects (users, groups, computers).

4. **Group Policy Objects (GPOs)** – Rules/settings applied to users or computers.

Real-World Use:

- Used in **corporate environments**, schools, and government networks to manage thousands of devices securely.
- Works with **DNS** for locating resources.
- Domain Controllers always have **static IPs** for reliability.

IP Allocation in an AD Environment

1. Static IPs for Critical Infrastructure

- **Domain Controllers (DCs)** – Always given static IPs so clients can always find them.
- **DNS Servers** – Often hosted on the DC; must be static for reliability.
- **DHCP Servers** – Must have static IPs so clients can always request addresses.
- **File/Print Servers** – Static to avoid changing network paths.

2. DHCP for Workstations

- User computers generally get **dynamic IPs via DHCP** for flexibility.
- DHCP leases are renewed automatically; no manual configuration required.

3. DHCP Reservations for Certain Devices

- Some devices (e.g., network printers, VoIP phones) get **reserved IPs** in DHCP so they always get the same address but still use DHCP.
- Every static IP is **documented in an IP address management (IPAM)** system or spreadsheet.
- Prevents duplication and helps troubleshooting.

Setting a Static IP on the AD Server (Windows Server VM)

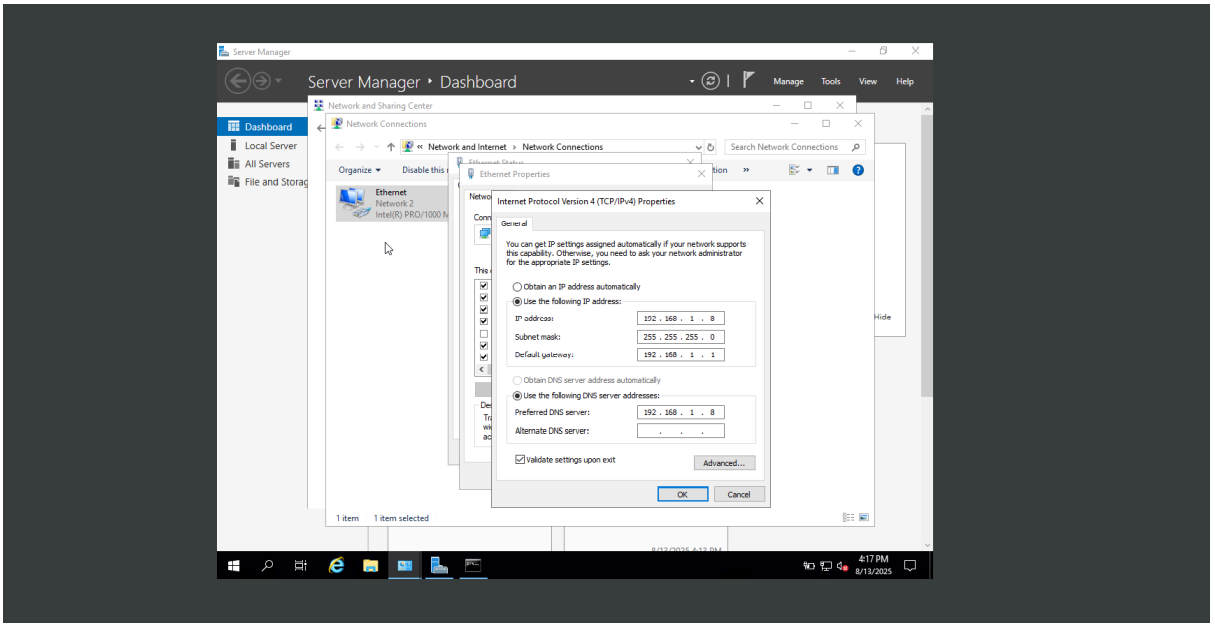
A. Open Network Settings

1. Login to your Windows Server.

2. Open **Control Panel → Network and Internet → Network and Sharing Center**.
3. Click **Change adapter settings** (left side).
4. Right-click your active network adapter → **Properties**.

B. Configure IPv4

1. Select **Internet Protocol Version 4 (TCP/IPv4)** → Click **Properties**.
2. Select **Use the following IP address** and enter:
   - **IP address:** `192.168.56.10`
   - **Subnet mask:** `255.255.255.0`
   - **Default gateway:** `192.168.56.1`
3. Under **Preferred DNS server**, enter:
   - `192.168.56.10` *(point to itself, since the DC will be DNS)*



Installing the Active Directory Domain Services (AD DS) Role

1. What we're doing

We are adding the **Active Directory Domain Services (AD DS)** role to our Windows Server.

This role turns a normal Windows Server into a machine that *can* become a **Domain Controller (DC)**.

---

2. Why we're doing it

- In a corporate network, a **Domain Controller** is the heart of authentication and security.
- Without the AD DS role, the server is just a regular file/print server — it cannot manage users, computers, or policies centrally.
- Installing AD DS is the **first step** before actually configuring the domain

Real-world example:

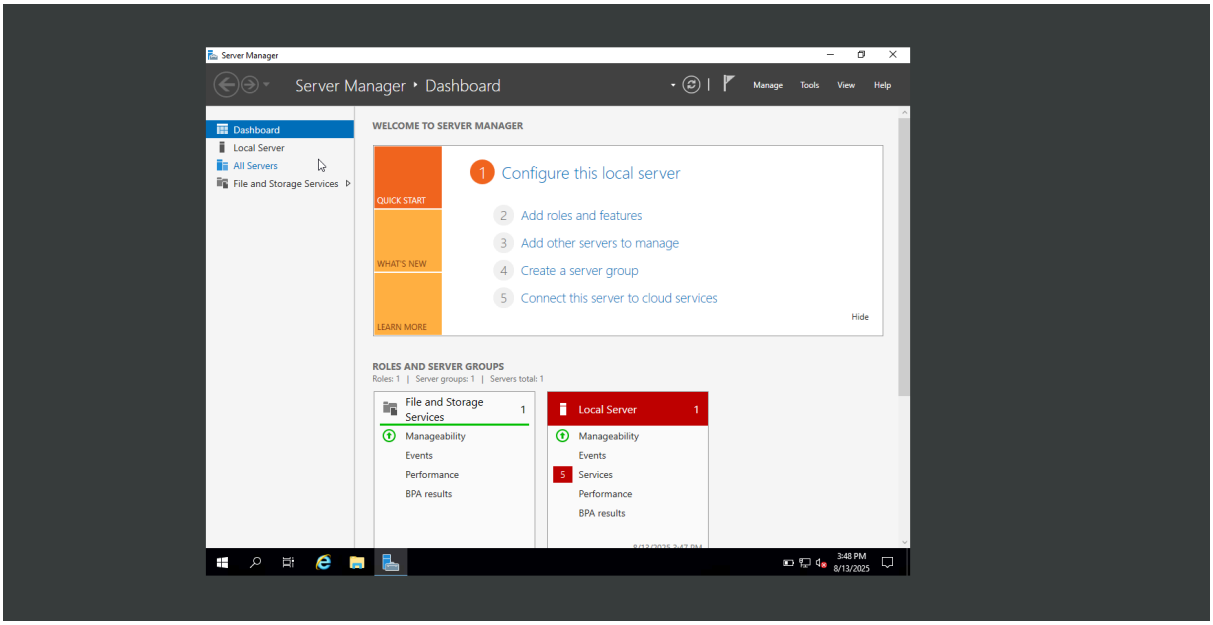
If you join a company and log in to your laptop with your work email & password, that authentication likely comes from a Domain Controller running AD DS.

---

3. How it works in the background

- AD DS provides a **directory database** (NTDS.dit file) that stores user accounts, passwords (hashed), group memberships, and computer objects.
- It also integrates with **DNS** so devices can find each other in the domain.
- When installed, it adds special background services (like `NTDS` service) to handle authentication requests from clients.

Detailed Steps to Install AD DS (Active Directory Domain Services)

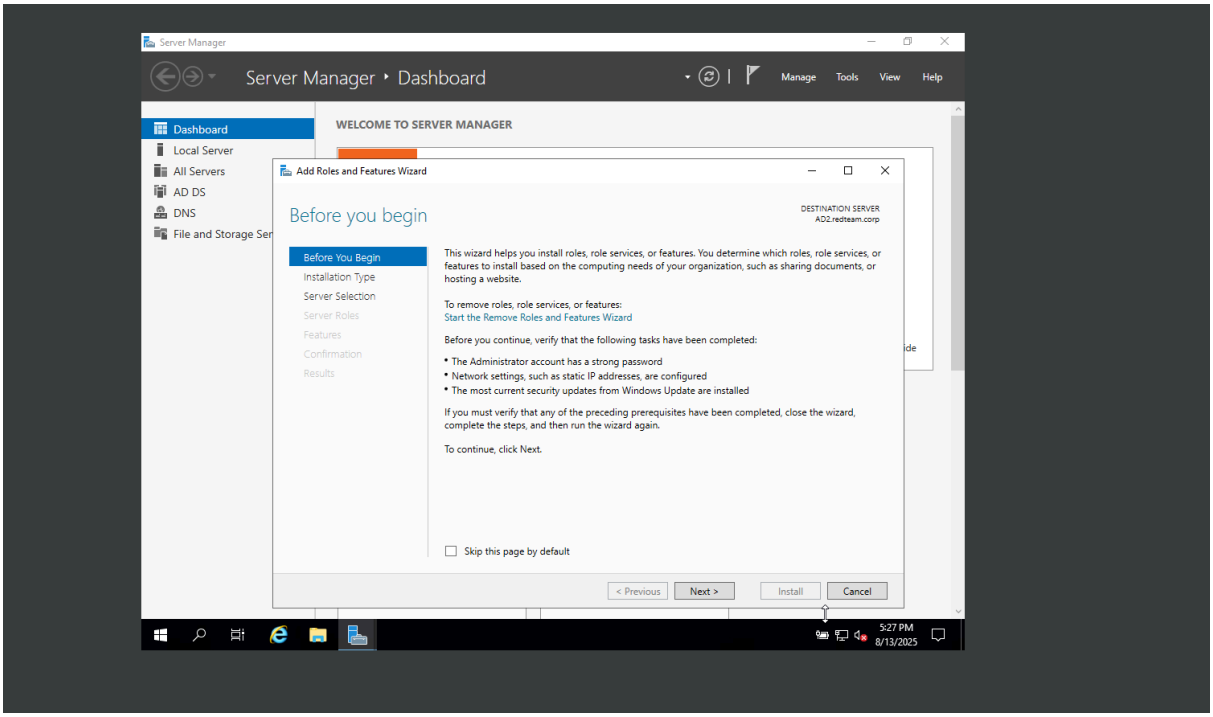


Step 1 — Open the Add Roles Wizard

- After logging in, **Server Manager** opens automatically.
- Click **Manage** (top right) → **Add Roles and Features**.
- This launches the **Add Roles and Features Wizard**, which is used to install server roles like AD DS, DNS, DHCP.

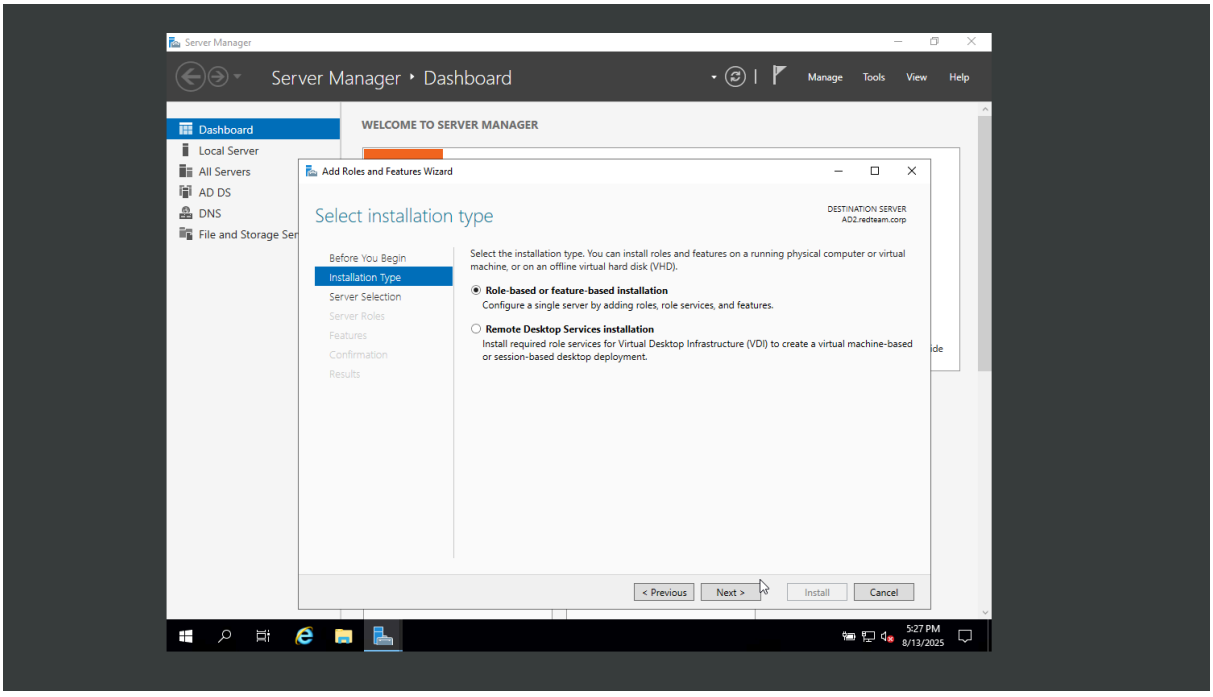
Step 2 — "Before You Begin" Page

- This page is just an introduction, reminding you to:
  - Have a strong admin password set.
  - Have a static IP configured.
  - Have the latest updates installed.
- Click **Next**.



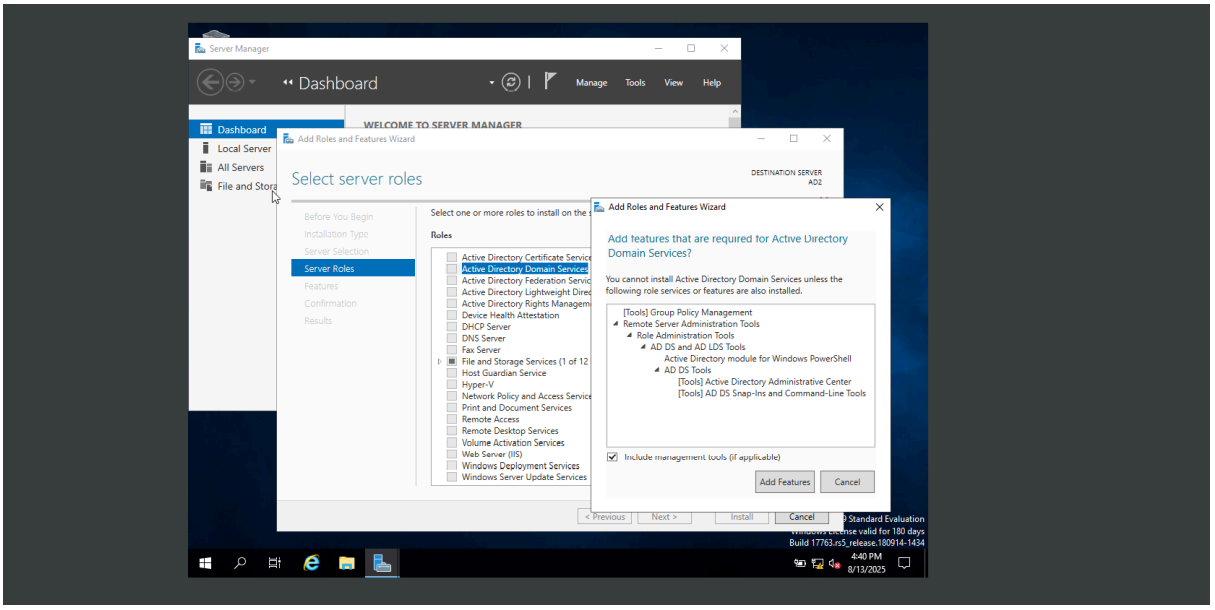
Step 3 — Installation Type

- Choose **Role-based installation**.
- This means we're adding a functional "role" to this server
- Click **Next**.



Step 4 — Server Selection

- Select the server you're working on (it should be highlighted by default).
- This is important in large organizations where multiple servers are listed.
- Click **Next**.



Step 5 — Server Roles

- Scroll down and tick **Active Directory Domain Services**.
- A popup will appear saying **"Add features that are required for Active Directory Domain Services?"**

  → Click **Add Features**.
- Click **Next**.

Step 6 — Features

- Leave the default features selected — AD DS already added what it needs.
- Click **Next**.

Step 7 — AD DS Information

- This screen explains what AD DS does:
  - Stores directory data.

- Handles authentication & authorization.
- Requires DNS for name resolution.

- Click **Next**.

Step 8 — Confirmation

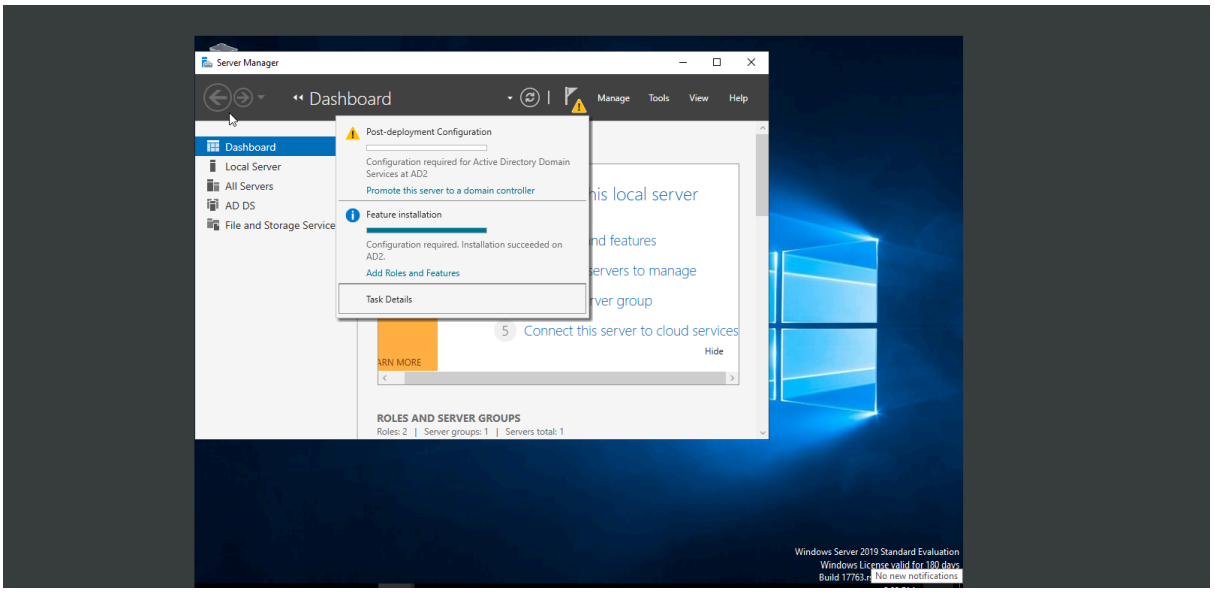
- Review your choices.
- Optionally tick **Restart the destination server automatically if required** (not needed here).
- Click **Install**.

Step 3 – Promote Server to a Domain Controller

1️⃣ Open Server Manager → Notifications Flag → Promote this server to a domain controller

What: This action launches the **Active Directory Domain Services Configuration Wizard**.

Why: We already installed the AD DS role in Step 2, but the server is still just a regular Windows Server — this step actually **creates the domain** and **enables the DC functions**.

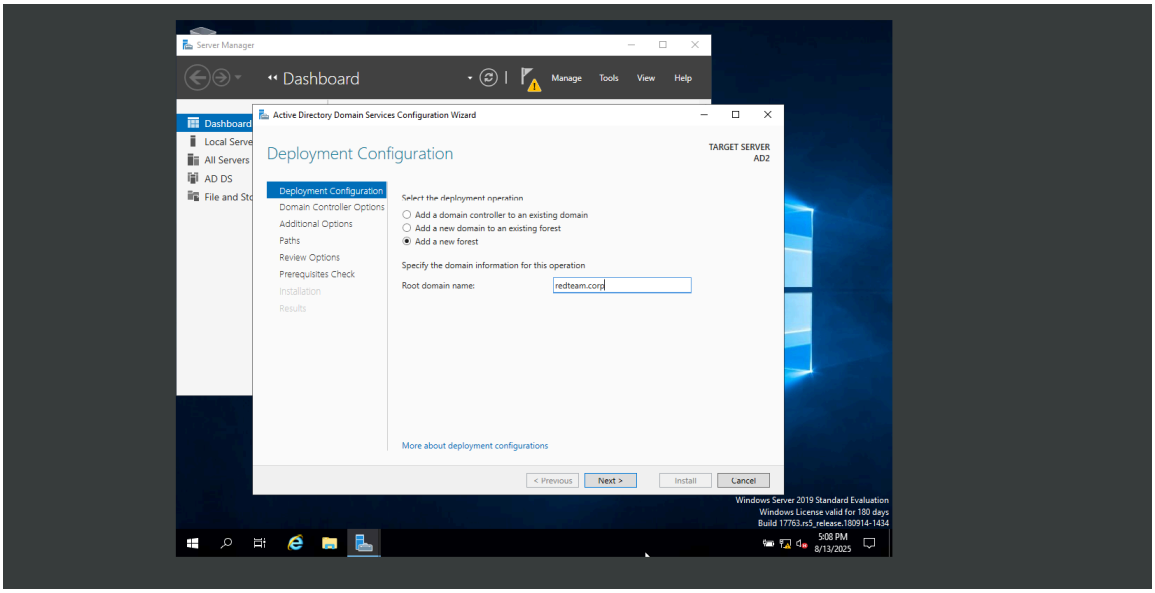


2️⃣ Deployment Configuration

- Select **Add a new forest**.
- **Root domain name:** `redteam.corp`

  Why:

  - A *forest* is the highest-level AD container.
  - `redteam.corp` will be the top authority for authentication and naming in your network.

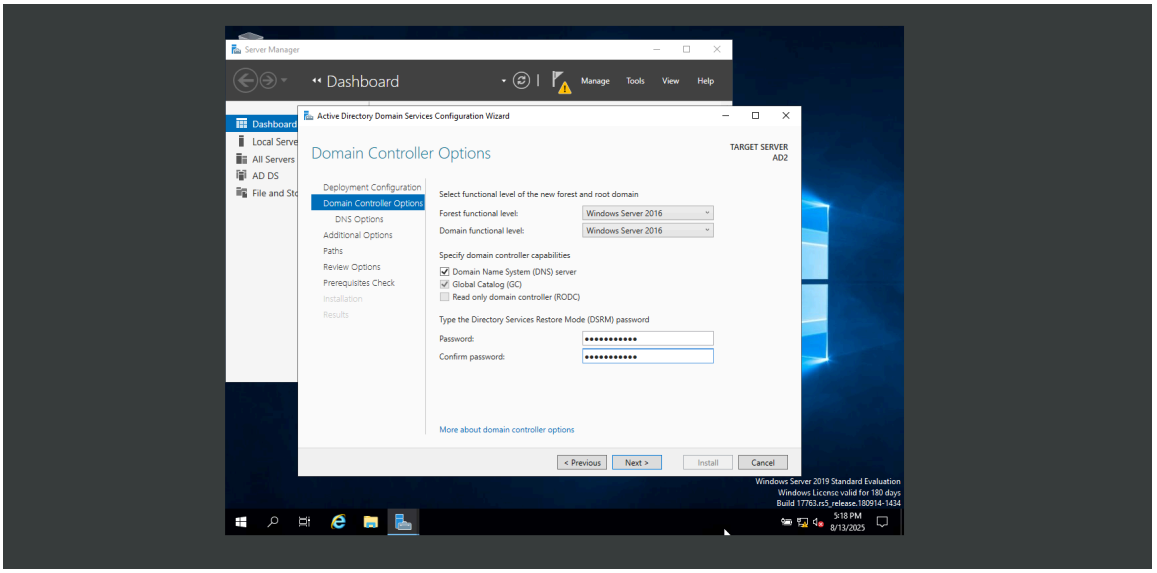


3️⃣ Domain Controller Options

- **Forest functional level:** Windows Server 2022
- **Domain functional level:** Windows Server 2022
- **Check DNS Server** (recommended in a lab).
- Set **Directory Services Restore Mode (DSRM) password**.

  Why:

  - Functional levels define which AD features are available.
  - DNS is needed for AD to locate domain resources.
  - DSRM password is for repairing AD in disaster recovery.



4 DNS Options

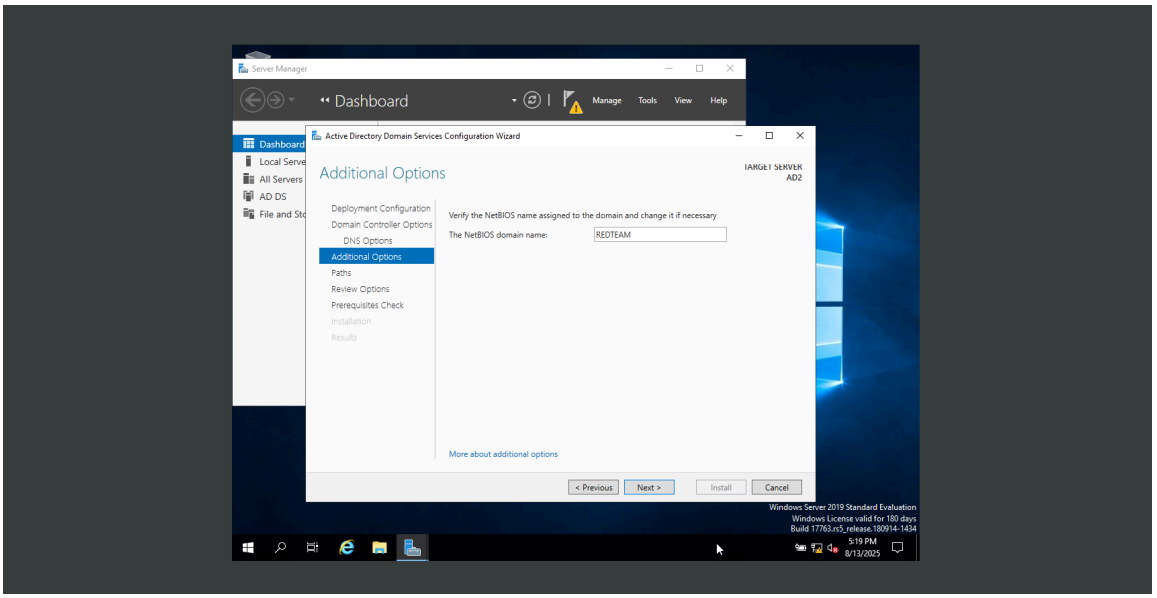
- Ignore warning about DNS delegation (normal for lab).

  Why: No external DNS zone yet, so delegation isn't possible in a lab environment.

5 Additional Options

- **NetBIOS name:** Will auto-fill as `REDTEAM`.

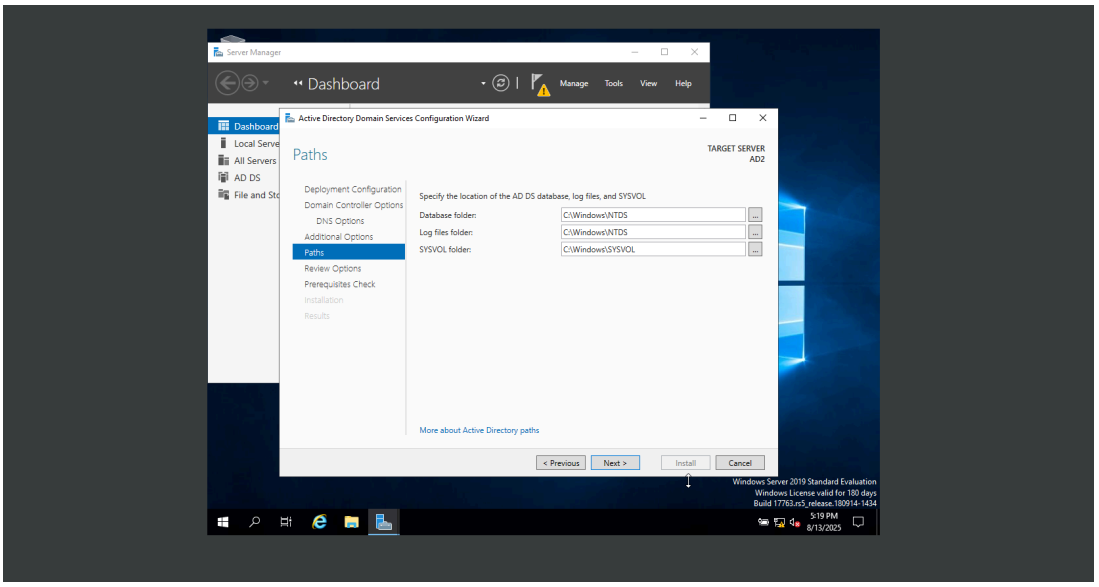
  Why: Legacy Windows systems still use NetBIOS for compatibility.



6️⃣ Paths

- Keep default locations for:
  - **Database folder** (`NTDS`)
  - **Log files folder** (`NTDS`)
  - **SYSVOL folder**

    Why: These store AD database, logs, and shared scripts/GPOs.



7️⃣ Review and Install

- Review summary → Click **Install**.
- Server will reboot automatically.

  Why: Reboot finalizes AD DS setup and activates the DC role.

Step 4 – Creating Organizational Units (OUs) & Users in AD

Why OUs?

- Organize users by **department** or **function**.
- Apply **specific Group Policies** per department.
- Easier **management & scalability**.

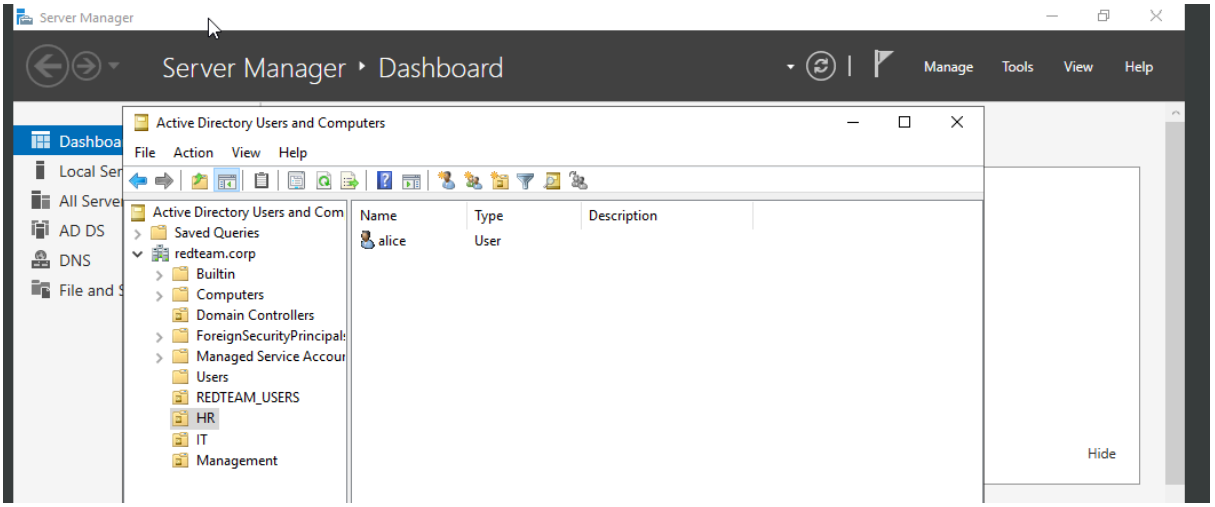
"In a real organization, users are separated into Organizational Units based on their department. This makes management easier and allows targeted policies, like restricting software installation for HR but allowing it for IT."

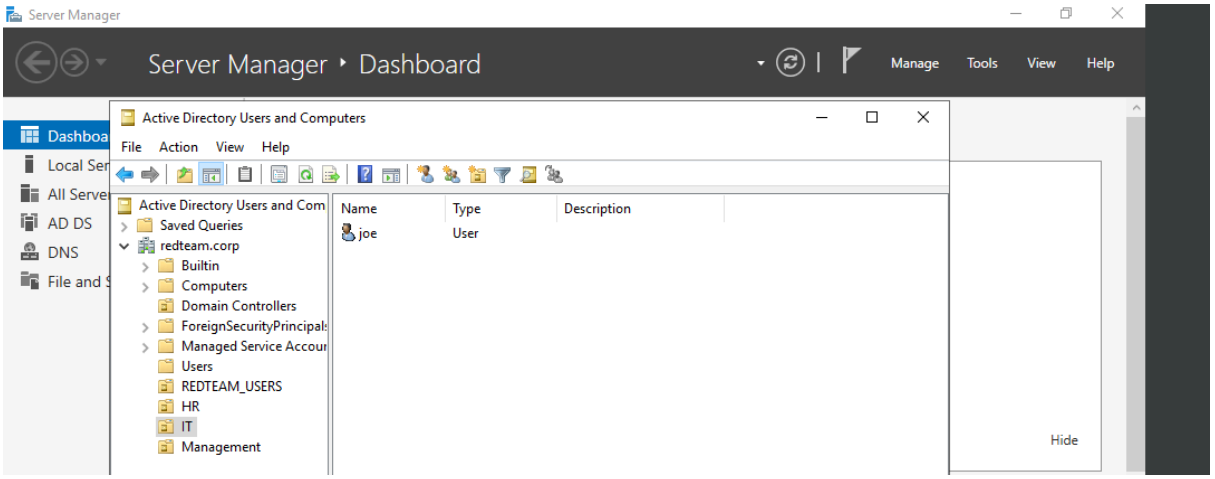
Structure

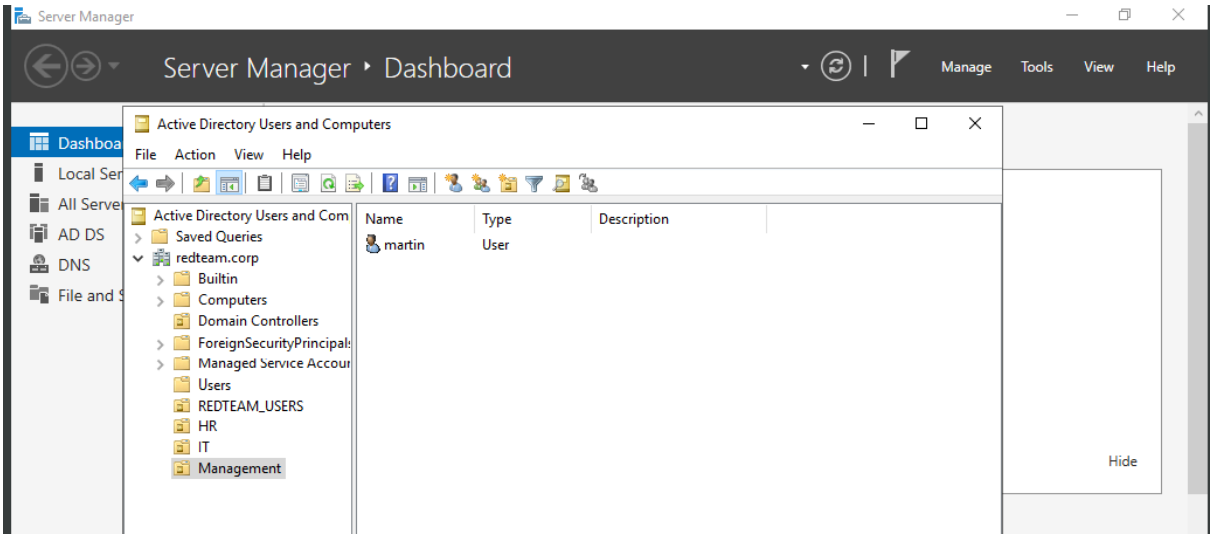
```
redteam.corp
 ├── HR
 │    └── Alice (HR Officer)
 ├── IT
 │    └── joe(IT Support)
 └── Management
      └── martin (Manager)
```

Steps to Create in AD

1. **Open ADUC**
   - Server Manager → Tools → **Active Directory Users and Computers**.
2. **Create OUs**
   - Right-click `redteam.corp` → New → **Organizational Unit**.
   - Add: `HR`, `IT`, `Management`.
3. **Add Users to Each OU**
   - **HR → Alice**
   - **IT → joe**
   - **Management → martin**







Step 5 – Joining Client PC to the Domain

1️⃣ Why this step is important

- In an organization, all computers are part of a **domain** so users can:
  - Log in with their **AD credentials** instead of local accounts.
  - Get **Group Policies** applied (security settings, software installs).
  - Be managed centrally from the AD server.

Without this step, your client PC is "standalone" and won't benefit from centralized management.

2️⃣ Pre-requisites

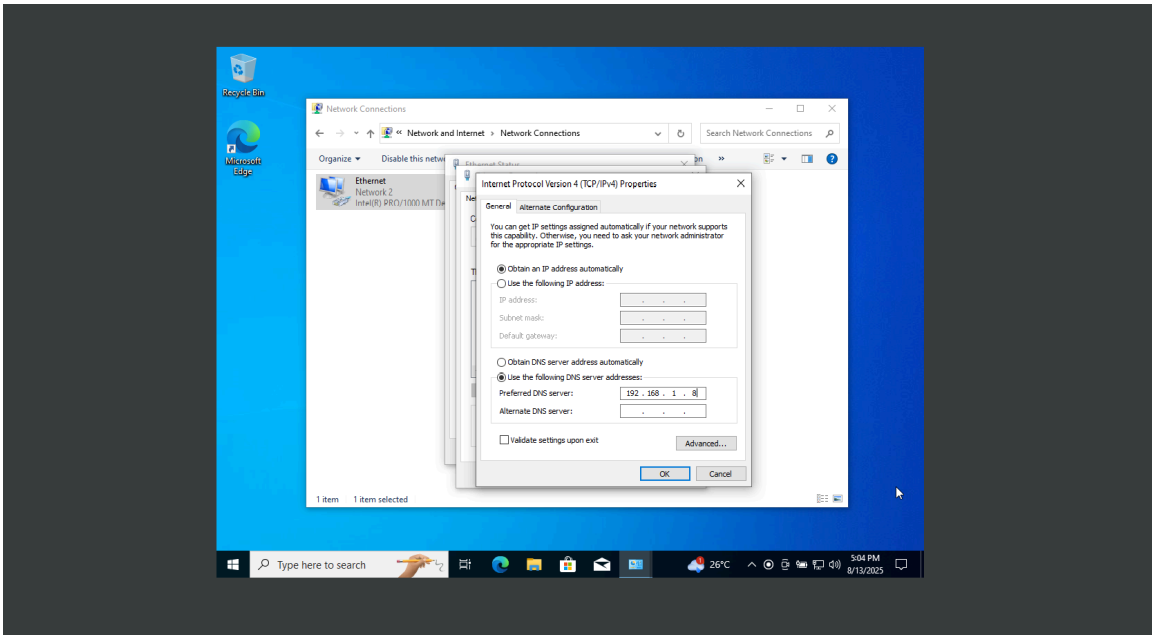
Before joining:

1. **AD server must have a static IP** (done in Step 1).
2. **Windows 10 client must use AD server as its DNS server** (because AD login & discovery depends on DNS).
3. Both machines should be able to **ping each other**.

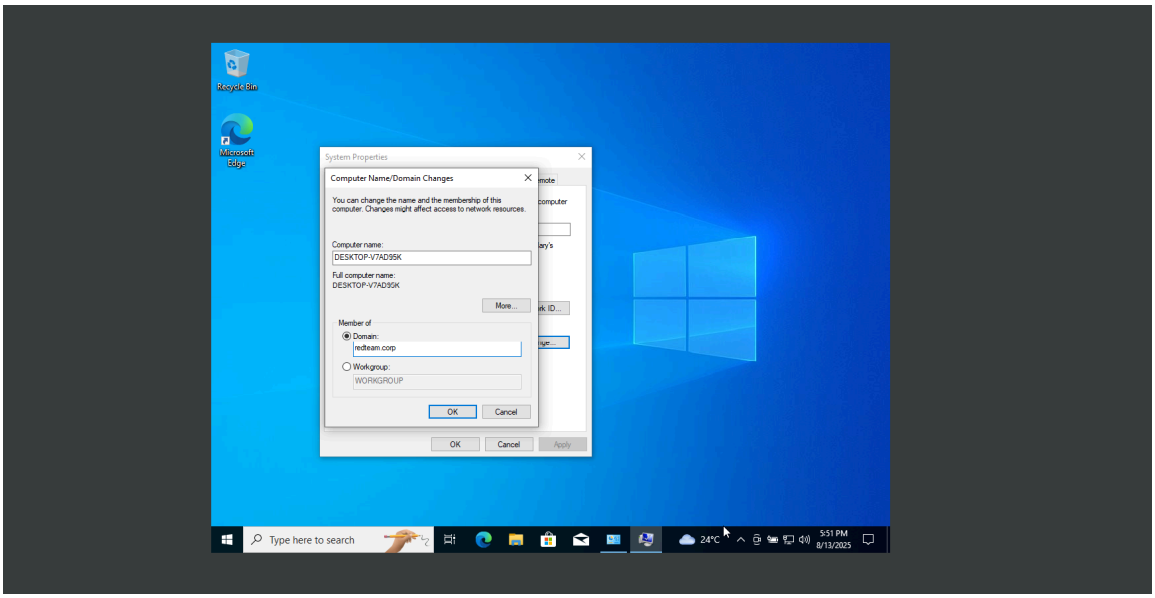
3️⃣ Steps to join the domain

On the Windows 10 Pro client:

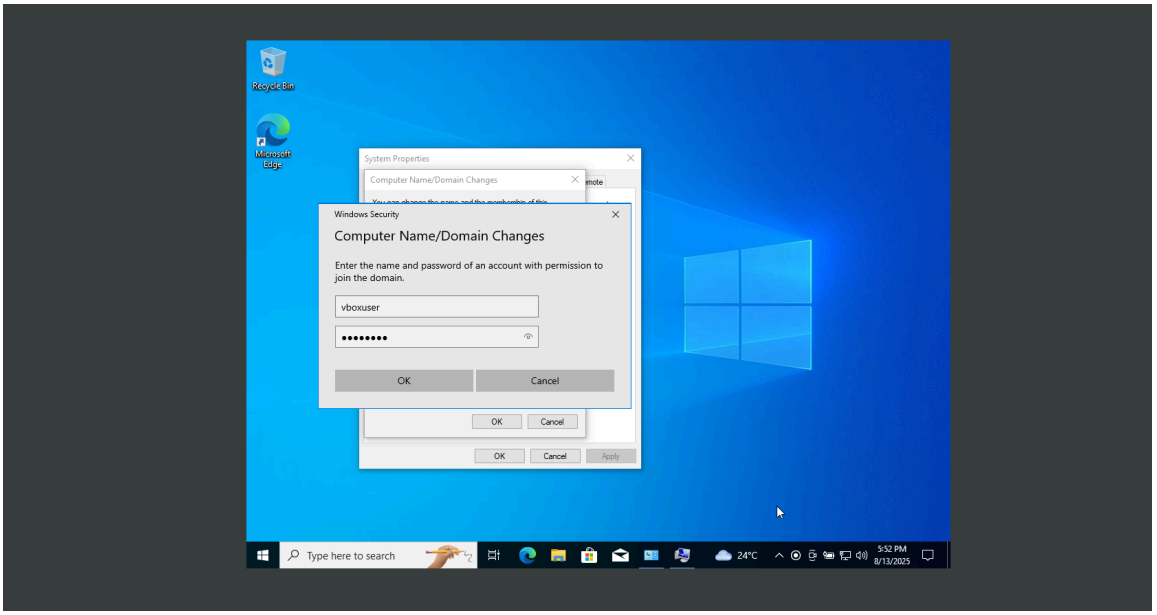
1. **Set DNS to AD server IP**
   - Go to **Control Panel → Network and Sharing Center → Adapter Settings**.
   - Right-click your network adapter → **Properties** → IPv4 settings.
   - Set **Preferred DNS server** to the **IP of your AD server**.
   - Reason: So the client can find `redteam.corp` through AD-integrated DNS.



2. **Join the domain**
   - Right-click **This PC → Properties → Advanced system settings**.
   - Under **Computer Name** → Click **Change**.
   - Select **Domain** and enter: `redteam.corp`.
   - Click **OK**.



   - Enter AD **administrator username & password** when prompted.



3. **Restart the client**

Step 6: Creating and Applying Group Policies

What This Is

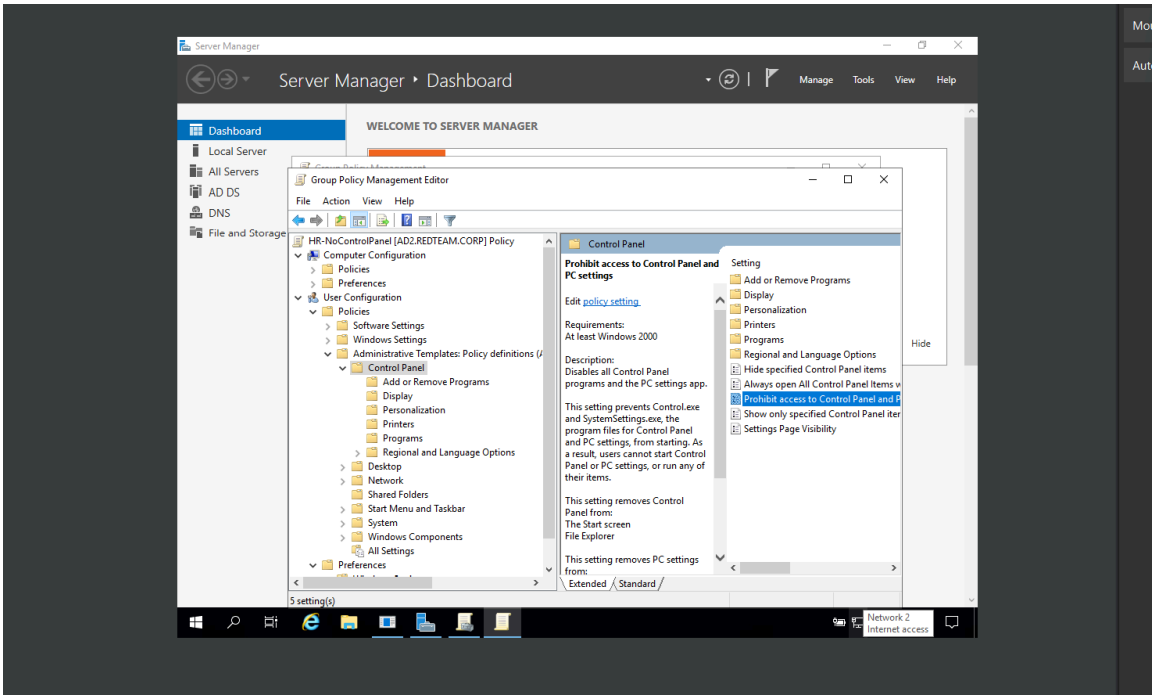
Group Policy in Active Directory lets you centrally configure settings for **users** and **computers** in the domain — without touching each device manually.

Group Policy example

1. Disable Control Panel for HR Users

1. Open **Group Policy Management** → right-click the **HR OU** → Create a new GPO called `HR-NoControlPanel`.
2. Right-click `HR-NoControlPanel` → **Edit**.
3. Go to:

   `User Configuration → Administrative Templates → Control Panel → Prohibit access to Control Panel and PC settings`.



4. Set to **Enabled**.
5. Link this GPO to **HR OU**.

When Alice (HR user) logs in, trying to open Control Panel will show:

> "This operation has been cancelled due to restrictions in effect on this computer."