🔍 What is AD DS (Active Directory Domain Services)?

AD DS is a directory service that stores information about users, computers, groups, and other resources on a network and makes this information easy to find and manage.

🧱 Core Functions of AD DS:

1. **Authentication and Authorization:**
    - **Validates users and computers when they log in.**
    - **Ensures users have the appropriate permissions to access resources.**
2. **Centralized Resource Management:**
    - **Admins can manage all users, devices, and permissions from a central location.**
3. **Group Policy:**
    - **Used to enforce settings on computers and users (like password policies, desktop settings, etc.)**
4. **Scalability and Hierarchy:**
    - **Organized into domains, trees, and forests to allow scalable network structures.**

🗃️ Key Components of AD DS:

Component	Description
Domain	Logical grouping of users and devices.
Tree	A collection of one or more domains in a hierarchical structure.
Forest	The top-level container that holds one or more trees.
Organizational Units (OUs)	Containers used to organize users, groups, and computers within a domain.
Domain Controllers (DCs)	Servers that run AD DS and respond to authentication requests.

🔐 Why Use AD DS?

- **Simplifies user and permission management across a large organization.**
- **Enables Single Sign-On (SSO).**
- **Provides security and compliance through centralized policy enforcement.**
- **Supports integration with other Microsoft services (like Exchange, SharePoint, etc.)**

✅ Top Reasons We Need AD DS

1. Centralized Authentication and Authorization

- **Users can log in to any domain-joined computer using a single username and password.**
- **AD DS authenticates users and controls access to resources (files, printers, applications) based on their permissions.**

> **🔐 Example: A user logs in once and can access emails, shared drives, and printers without logging in again—Single Sign-On (SSO).**

2. Centralized Management

- **Admins can manage all users, groups, computers, and security policies from one place.**
- **Changes (like password policies) can be applied across all machines instantly.**

> **🎯 Example: An admin can disable a user's account across the entire company with one click.**

3. Group Policy Control

- **AD DS uses Group Policy Objects (GPOs) to enforce security and configuration settings on all domain-joined computers.**

> **🧰 Example: Automatically lock user screens after 10 minutes of inactivity across the entire organization.**

4. Security and Compliance

- **Helps enforce security standards (password complexity, account lockout, etc.).**
- **Keeps auditing and logging for compliance (e.g., HIPAA, GDPR).**

5. Scalability and Organization

- **Supports complex, hierarchical structures (domains, trees, forests) to scale across large and distributed organizations.**

- Uses Organizational Units (OUs) to logically group users and computers for easier management.

6. Integration with Other Microsoft Services

- Works seamlessly with Microsoft Exchange, SharePoint, Azure, and Office 365.
- AD DS is the backbone of Microsoft's identity and access management infrastructure.

7. User Experience and Productivity

- Users can log in on any computer in the domain.
- User profiles and settings can follow them from one computer to another (roaming profiles, folder redirection).

🚫 Without AD DS (in a Workgroup):

- User accounts must be created on each computer.
- Policies must be configured manually on each system.
- No centralized control or management.

🎯 Summary

Without AD DS	With AD DS
Decentralized user management	Centralized control
Manual configuration	Automated via Group Policy
Weak security	Strong access control
Poor scalability	Scales to thousands of devices

The process step by step ADDS setup

✅ Pre-Requisites

Before starting:

- A clean Windows Server installed (e.g., Windows Server 2016, 2019, or 2022).
- A static IP address set on the server.
- A proper computer name (change it before promotion if needed).

- Know your desired domain name (e.g., `company.local`).
- Local admin privileges.

🛠️ Step-by-Step AD DS Setup

1. Set a Static IP Address

- Go to Control Panel > Network and Sharing Center > Change adapter settings.
- Right-click your network adapter > Properties.
- Select Internet Protocol Version 4 (TCP/IPv4) > Properties.
- Set a static IP, subnet, and default gateway.
- Set Preferred DNS Server as the same static IP (this server will become the DNS server).

2. Rename the Server (Optional but recommended)

- Go to System Properties.
- Click Change Settings next to the computer name.
- Enter a meaningful name (e.g., `DC01`).
- Restart the server.

3. Install AD DS Role

- Open Server Manager.
- Click Manage > Add Roles and Features.
- Click Next until you reach Server Roles.
- Check Active Directory Domain Services.
- Click Add Features when prompted.
- Click Next > Install.
- Wait for installation to complete (do not restart yet).

4. Promote Server to Domain Controller

- **After AD DS is installed, in Server Manager, click the notification flag and select Promote this server to a domain controller.**

You have three options:

- **Add a new forest (for first domain controller).**
- **Add a domain controller to an existing domain.**
- **Add a new domain to an existing forest.**

Assume you're creating a new forest.

➢ If creating a new forest:

- **Select Add a new forest and enter your domain name (e.g., `company.local`).**
- **Click Next.**

5. Set Domain Controller Options

- **Choose:**
  - **Domain functional level (default is fine for most cases).**
  - **Forest functional level.**
  - **Check:**
    - **DNS Server (recommended).**
    - **Global Catalog (GC) (auto-selected).**
  - **Enter a Directory Services Restore Mode (DSRM) password.**

Click Next.

6. DNS Options

- **Ignore the delegation warning (if applicable).**
- **Click Next.**

7. Additional Options

- NetBIOS name will be set automatically (you can change it).
- Click Next.

8. Paths

- You can leave the defaults:
  - Database folder
  - Log files folder
  - SYSVOL folder

Click Next.

9. Review and Install

- Review all settings.
- Click View script if you want to export PowerShell for automation.
- Click Install.

The server will automatically reboot after installation.

10. Verify Domain Controller

- After reboot, log in using domain credentials (e.g., `company\Administrator`).
- Open Server Manager > Tools > Active Directory Users and Computers.
- You should see your domain and be able to manage users, computers, and OUs.

🧪 Optional: Post-Setup Configuration

- Create Organizational Units (OUs).
- Create user accounts and groups.
- Set up Group Policies using Group Policy Management Console (GPMC).
- Join client machines to the domain.

Let me know if you want:

- A PowerShell version of this setup.

- **Help setting up additional domain controllers or RODCs.**
- **A diagram of AD DS structure.**