◆ What is Active Directory (AD)?

Active Directory (AD) is Microsoft's directory service introduced in **Windows 2000 Server**. It provides a **centralized and standardized system** for **network resource management**, including users, computers, printers, and policies.

The most commonly used role of AD is **Active Directory Domain Services (AD DS)**, which allows for **domain-based identity and access control**, **user and group management**, and **centralized authentication** using protocols like **Kerberos**.

🧠 Why Use Active Directory?

Benefit	Description
Centralized Management	Manage users, computers, and resources from a central location.
Authentication & Authorization	Secure login and access control using domain credentials.
Policy Enforcement	Apply consistent security and operational policies using Group Policy.
Scalability	Supports millions of objects across multiple locations.
Security	Integration with Kerberos, NTLM, and certificate-based security.

🏛️ Core Components of AD DS

1. Domain

- The fundamental unit of AD.
- Logical grouping of objects (users, computers, etc.).
- Each domain has its own **security boundary** and **policies**.

2. Forest

- A collection of one or more **domains** that share a **global catalog**, **schema**, and **trust relationships**.
- First domain created = **forest root domain**.

3. Tree

- A hierarchical structure of domains that share a **contiguous namespace** (e.g., `corp.com`, `hr.corp.com`).

4. **Organizational Units (OUs)**

- Containers used to **organize** users, groups, and computers.
- **Delegation of control** is possible at the OU level.

5. **Objects**

- Every entity in AD is an object: **User, Group, Computer, Printer, GPO, etc.**
- Each object has a **Globally Unique Identifier (GUID)**.

🔧 Key Roles in AD DS

Role	Description
Domain Controller (DC)	A server that holds a copy of the AD database and handles logins and directory requests.
Global Catalog (GC)	Indexes data from all domains for faster searching.
FSMO Roles (Flexible Single Master Operations)	Special roles assigned to DCs for specific operations (explained below).

🧩 FSMO (Flexible Single Master Operations) Roles

AD uses **5 FSMO roles**:

FSMO Role	Scope	Purpose
Schema Master	Forest	Controls schema changes.
Domain Naming Master	Forest	Adds/removes domains.
RID Master	Domain	Allocates relative IDs to DCs.
PDC Emulator	Domain	Syncs time, backward compatibility with NT4, GPOs.
Infrastructure Master	Domain	Maintains references to objects in other domains.

🔄 Replication in AD DS

- **Multi-Master Replication:** Changes made on any DC are replicated to all others.
- **Intra-site Replication:** Fast and uses compression.
- **Inter-site Replication:** Occurs over WAN, configurable schedule, and uses **site links**.

🔐 Authentication in AD DS

- Uses **Kerberos** (default) for secure authentication.
- Supports **NTLM** for legacy systems.
- Integration with **smart cards**, **biometric**, **certificates**, etc.

💼 Active Directory Database (NTDS.dit)

- Stored in `%SystemRoot%\NTDS\ntds.dit`
- Contains all domain objects and attributes.
- Backed up regularly to avoid data loss.

🛠️ Group Policy (GPO)

Group Policy is a feature tightly integrated with AD to control **user and computer settings**:

- Login scripts
- Password policies
- Desktop restrictions
- Software deployment
- Security configurations

GPOs can be linked to:

- Sites
- Domains
- OUs

📂 AD DS Installation (Simplified)

Graphical:

1. Open **Server Manager** → **Add Roles and Features**.
2. Select **Active Directory Domain Services**.
3. Promote server to **Domain Controller**.
4. Create **new forest** or join existing domain.

PowerShell:

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools Import-Module
ADDSDeployment Install-ADDSForest -DomainName "corp.local"
```

💉 Example Scenarios of AD DS

🏢 Example 1 – Corporate Environment

- Company `XYZ Ltd.` has 2000 employees.
- AD is used to:
  - Manage **user accounts** centrally.
  - Apply **password policies** using Group Policy.
  - Control **access to files** based on **group membership**.
  - Integrate **printers and applications** with AD.

🏫 Example 2 – School Environment

- A university runs `school.edu` domain.
- Students and staff have separate OUs.
- GPOs restrict student accounts from installing software.
- Lab PCs are auto-reset using GPO logoff scripts.

🧳 Example 3 – Multi-site Organization

- Global company with offices in **India, USA, UK**.
- AD Sites are created to match each physical location.
- DCs are deployed in each region to **optimize login and replication**.
- Inter-site replication is scheduled during off-peak hours.

📊 Active Directory Administrative Tools

Tool	Purpose
Active Directory Users and Computers (ADUC)	Manage users, groups, computers, OUs.
Active Directory Sites and Services	Manage replication, sites, and subnets.
Active Directory Domains and Trusts	Manage domain relationships and trust.
Group Policy Management Console (GPMC)	Create and manage Group Policies.
PowerShell	Automate administrative tasks.

🔍 Useful PowerShell Commands for AD

List all users:

```
Get-ADUser -Filter * -Properties *
```

Create new user:

```
New-ADUser -Name "John Doe" -SamAccountName jdoe -AccountPassword (ConvertTo-SecureString
"P@ssw0rd!" -AsPlainText -Force) -Enabled $true
```

Add user to group:

```
Add-ADGroupMember -Identity "IT Staff" -Members jdoe
```

🔐 Security Features in AD DS

- **Fine-Grained Password Policies**
- **Account Lockout Policies**
- **Delegation of Control**
- **Read-Only Domain Controllers (RODCs)**
- **Kerberos Authentication**
- **Auditing and Monitoring**

🛡️ Backup and Recovery

- Use **Windows Server Backup** or **3rd-party tools**.
- **System State Backup** includes AD database, SYSVOL, registry.
- You can restore:
  - **Authoritative restore**: Force restored objects to replicate.
  - **Non-authoritative restore**: DC syncs with others post-recovery.

☑️ Best Practices

- Always deploy at least **2 Domain Controllers** per domain.
- Use **OUs + GPOs** for structured management.
- Keep **backups of System State** regularly.
- Avoid using DCs for file sharing or application hosting.
- Monitor **replication health** using tools like `repadmin`.
- Delegate admin tasks using **least privilege** principle.

🏁 Conclusion

Active Directory Domain Services (AD DS) is a cornerstone of **enterprise IT infrastructure**. It centralizes **identity** management, access control, and resource organization, making it easier for administrators to enforce security, automate processes, and maintain consistent user experiences across the network.

AD DS is scalable from **small businesses** to **large multi-site enterprises**, and with proper planning and maintenance, it delivers high levels of **security**, **efficiency**, and **reliability**.