# Active Directory Overview

Its like a phone book.

1. Directory services developed by Microsoft to manage Windows Domain Network.
2. Stores information related to objects such as computers, users, Printers etc.
3. Authenticates using **Kerberos Tickets**. [The Kerberos ticket is a certificate issued by an authentication server, encrypted using the server key]
4. **Non-windows devices** like linux, firewalls etc can authenticate to Active Directory via **RADIUS/ LDAP.**

| ***RADIUS*** | ***LDAP*** | ***KERBEROS*** |
|---|---|---|
| **Remote Authentication Dial-In User Service** | **Lightweight Directory Access Protocol** | **Named as Kerberos** |
| **RADIUS is an intermediate service that Authenticates, Accounts, and Authorizes user's information from a central location** | **LDAP protocol Authorizes the details of the accounts only when accessed** | **Kerberos secures management of credentials** |
| **Do not support two factor authentication** | **Two factor authentication is available but only with RADIUS protocol** | **Supports two factor authentication** |
| **Not an open source software but supports Free RADIUS implementations which are open-source** | **Not an open source software but supports Open LDAP implementations which are open-source** | **Kerberos is an open source software** |
| **Uses network access server (NAS), a RADIUS client to provide authentication** | **Supports SASL or anonymous authentication** | **Supports mutual authentication** |
| **Supports authentication in multi tier applications** | **Supports authentication in multi tier applications** | **Supports authentication in multi tier applications** |

| | | |
|---|---|---|
| **Less complex to configure** | **Less complex to configure** | **More complex to configure than LDAPContent** |
| **Supports single sign on (SSO) features Content** | **Supports single sign on (SSO) features** | **Supports single sign on (SSO) features** |
| **It is compatible with UNIX and Microsoft Windows** | **It is a cross platform compatible with Linux/UNIX, Mac OS X, Microsoft Windows** | **It is compatible with all operating systems including Windows, Linux, FreeBSD, Apple macOS and Web Apps** |
| **RADIUS is commonly used in ISPs, Microsoft's Network Policy Server, accounting, college campuses, and enterprise infrastructures** | **OpenVPN, Docker, Jenkins, Atlassian Jira & Confluence, Linux Samba servers, Kubernetes are applications that use LDAP** | **FreeBSD, Apple's Mac OS X, Sun's Solaris, IBM's AIX, HP's OpenVMS are a few use cases.** |

WHY Active Directory?

1. most commonly used identity management service in the world
2. Can be exploited without ever attacking patchable exploits by abusing future, trust, components

***Physical Active Directory Components:***

1. **Domain Controller**: It is a server with the AD DS server role installed that has specially been promoted to a domain controller.
   a. Host a copy of AD DS directory store
   b. Provide authentication and authorization services
   c. Replicate updates to other domain controller in the domain and forest
   d. Allow administrative access to manage user accounts and network resources .

2. **AD DS Data Store**: contains the database files and process that store and manage directory information for users, services, and applications .

a. consists of the *Ntds.dit* file.[very sensitive=contains everything stores in AD data like all users, groups, passwords etc.]

b. it is stored by default in the %SystemRoot%\NTDS folder on all domain controllers

c. it is accessible only through the domain controller process and protocols.

***Logical AD Components:***

1. **AD DS Schema** :

   a. *rule book/blueprint* that defines every objects that can be stored in the directory .

   b. Enforces rules against object creation and configuration.

2. **Domains**:

   a. used as groups and manage objects in an organization

3. **Trees**:

   a. group of domain

   b. by default create a two-way transitive trust with other domains

4. **Forests**: collection of one or more domain trees

**Organizational Units (OUS)** : OUs are active directory containers that can contain users, groups, computers, and other OUs.

**Trusts** : Provide a mechanism for users to gain access to resources in another domain

a. **Directional** : The trust direction flows from trusting domain to trusted domain

b. **Transitive** : The trust relationship is extended beyond a two-domain trust to include other trust domains.

- All domains in a forests trust all other domains in the forest
- Trust can extend outside the forest

**Objects** : objects are inside our OUs. like= User, InetOrgPerson, Contacts, Groups, Computers, Printers, Shared Folders.