

Active Directory(AD) Overview

Active Directory(AD) Overview

What is Active Directory?

- Directory service developed by Microsoft to manage Windows domain networks.
- Stores information related to objects such as Computers, Users, Printers, etc. (Similar to a phonebook but for Windows)
- Authenticates using Kerberos Tickets - Other non-windows devices can authenticat to AD via RADIUS or LDAP.

AD is the most commonly used identity management service used. Can be exploited without attacking patchable exploits.

AD Components

Physical

- Data Store
- Domain Controllers
- Global catalog server
- Read-Only Domain Controller

Logical

- Partitions
- Schema
- Domains
- Domain Trees
- Forests
- Sites
- Organizartion Units(OU)

Domain Controller

A Domain Ctronller (DC) is a server with the AD DS server installed that has specifically been promoted to a DC. They:

- Host a copy of the AD DS directory store

- Provide authentication and authorize services
- Replicate updates to other domain controllers in the domain and forest
- Allow administrative access to manage user accounts and network resources.

AD DS Data Store

Contains the database files and processes that store and manage directory information for users, services, and applications.

- Consists of the Ntds.dit file
- Default location is `%SystemRoot%\NTDS` on a DC
- Is accessible only through the domain controller processes and protocols.

AD DS Schema

Defines every type of object that can be stored in the directory and enforces rules regarding object creation and configuration.

Object Types	Function	Examples
Class Object	What objects can be created in the directory	<ul style="list-style-type: none"> • User • Computer
Attribute Object	Information that can be attached to an object	<ul style="list-style-type: none"> • Display name

Domains

Used to group and manage objects in an organization

- An administrative boundary for applying policies to groups of objects
- Replication boundary for replicating data between DCs
- Authentication and authorization boundary that provides a way to limit the scope of access to resources

Trees

A Hierarchy of domains in AD DS

- Share contiguous namespace with the parent domain
- Can have additional child domains
- By default create a two-way transitive trust with other domains.

Forests

A collection of one or more domain trees

- Share a common schema
- Share a common configuration partition
- Share a common global catalog to enable searching
- Enable trusts between all domains in the forest
- Share the Enterprise and Schema Admins groups

Organization Unit (OUs)



AD containers that can contains users, groups, computers, and other OUs

- Represent your organization hierarchically and logically
- Manage a collection of objects in a consistent way
- Deletagte permissions to administer groups of objects
- Apply policies

Trusts

Provide a mechanism for the users to gain access to resources in another domain

- All domains in a forest trust all other domains in the forest
- Trusts can be extended outside the forest

Types of Trusts	Description	Diagram
Directional	The trust direction flows from trusting domain to the trusted domain	
Transitive	The trust relationship is extended beyond a two-domain trust to include other trusted domains	

Objects

Object	Description
User	<ul style="list-style-type: none"> • Enables network resource access for a user
InetOrgPerson	<ul style="list-style-type: none"> • Similar to a user account • Used for compatibility with other directory services
Contacts	<ul style="list-style-type: none"> • Used primarily to assign e-mail addresses to external users • Does not enable network access
Groups	<ul style="list-style-type: none"> • Used to simplify the administration of access control
Computers	<ul style="list-style-type: none"> • Enables authentication and auditing of computer access to resources
Printers	<ul style="list-style-type: none"> • Used to simplify the process of locating and connecting to printers
Shared folders	<ul style="list-style-type: none"> • Enables users to search for shared folders based on properties