Active Directory

what?

→ like a phonebook → stores objects like printers, users, computers etc.

→ uses Kerberos for authn

→ Non windows objects can use LDAP, RADIUS to authn to AD.

Why?

→ Most commonly used identity management system

→ Doesn't always have to be an patchable exploit. abuse features, trusts etc.

Physical components

1) Domain Controller

→ Host a copy of AD DS directory store (phonebook)

→ does authn, authz

→ replicates updates to other DCs in the domain and forest.

→ allows admin access to manage user accounts and network resources.

iii) AD data store

contains the database files and processes that store and manage directory info for users, services, apps. → including passwd hashes

→ consists of Ntds.dit file
→ is stored by default in %SystemRoot% NTDS
→ accessessible only through DC procs and protos.

Logical Components

i) AD Schema : blueprint

contains definations and rules.

- about kinds of objects
- about object creation and config.

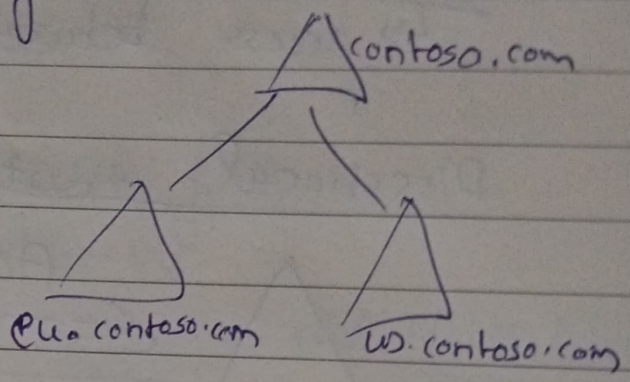
ii) Domains : used to group objects together.

uses:

→ administrative boundary for applying policies.
→ replication boundary for replicating data between domain controllers.
→ authn and authz boundary to limit scope of access to resources.

iii) Trees : hierarchy of domain

→ share a namespace
→ trust between them
(child parent)



iv) Forest : collection of trees
→ share schema, config pattern, common global catalog
→ enable trusts between all domains within forest
→ share enterprise admins and schema admins group.

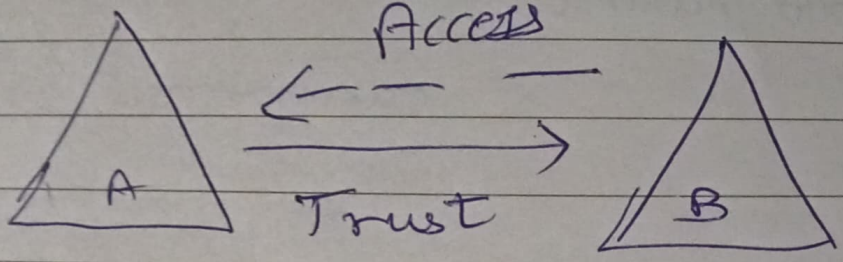
v) OUs : containers for users, groups, computers and other OUs.

used
→ rep your org hierarchaly and logically.
→ manage a collection of objects
→ delegate permission to administer group of objs.
→ apply policies.

vi) Trusts

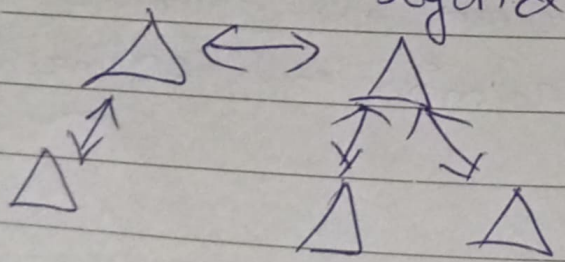
↳ access between resources

Directional trust



A trusts B, B can access A

Transitive



☆ default: domain in forest trust each other

* can be extended outside forest.

vii) Objects

user, Contacts, groups, Computers, Printers, shared folders, Inet OrgPerson ??