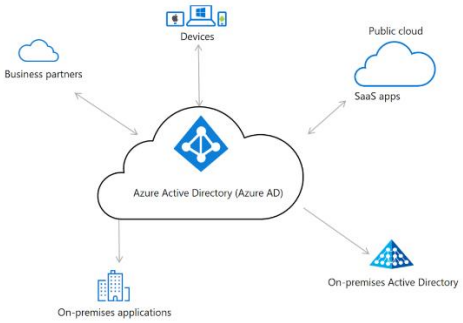
Active Directory

What is Active Directory?

Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and enables administrators to manage permissions and access to network resources.

Active Directory stores data as objects. An object is a single element, such as a user, group, application or device such as a printer. Objects are normally defined as either resources, such as printers or computers, or security principals, such as users or groups.



When we use Active Directory?

A lot of users

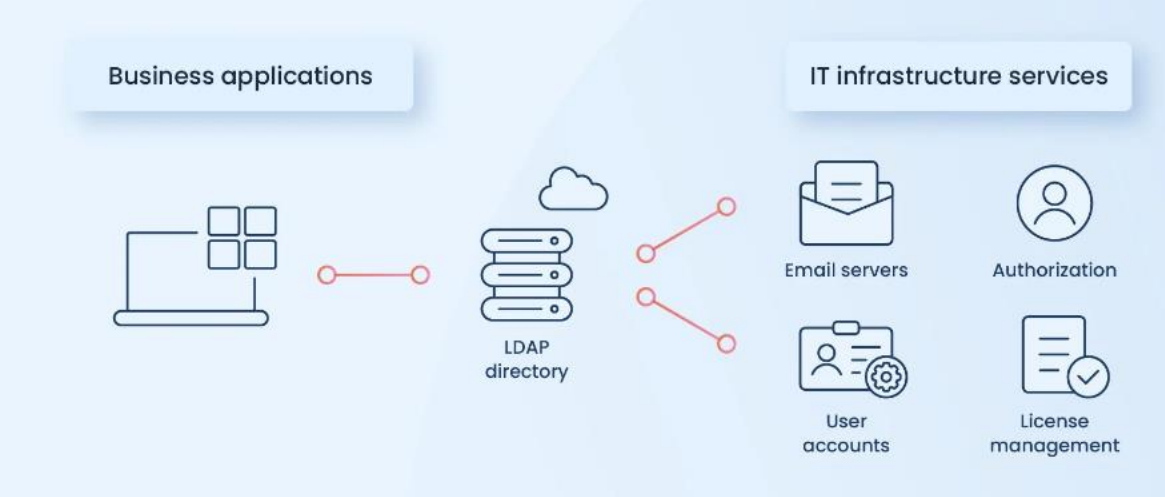
When organization need to be collaboration

Need centralize management.

If need policy to organize whole organization Control network usage.

Lightweight Directory Access Protocol (LDAP)

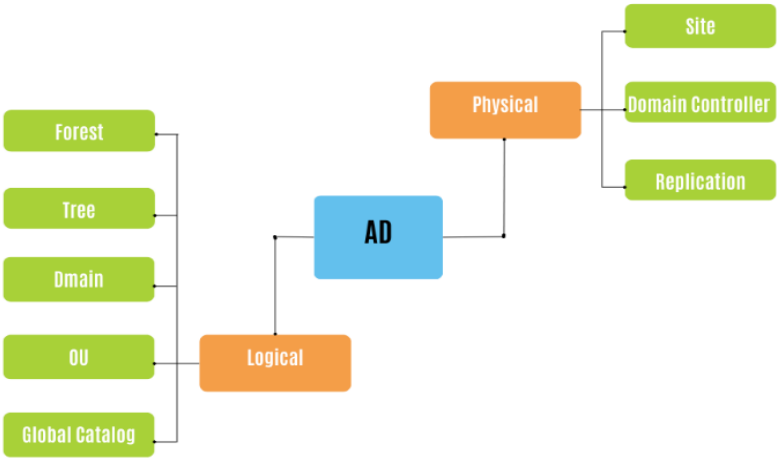
LDAP stands for Lightweight Directory Access Protocol which is a directory service similar to the database that is used for storing computers, users, objects, etc. Moreover, it helps in adding, removing, and updating computer objects in the directory.



Active Directory Web Services (ADWS)

ADWS makes it easier for administrators to manage Active Directory remotely and securely without needing to access the server directly. ADWS lets you manage Active Directory resources (like user accounts, computers, and groups) remotely, without needing to be physically at the server. You can also manage AD Lightweight Directory Services (ADLDS), which is a simpler version of AD.

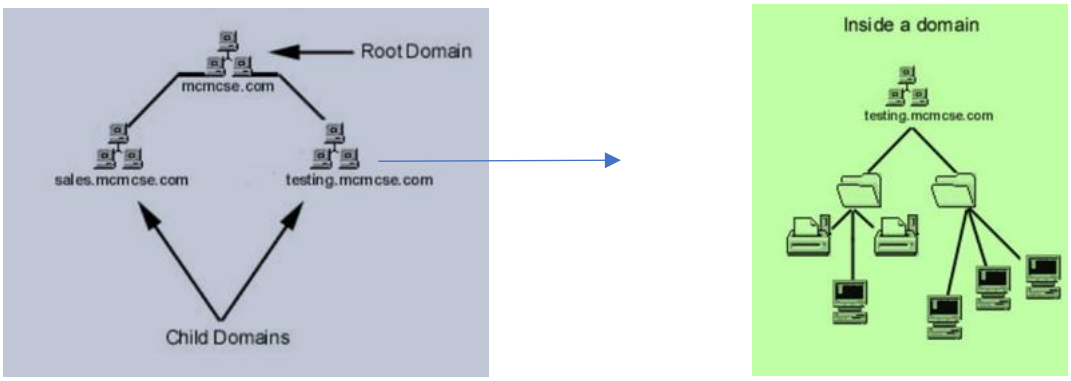
Active Directory Architecture



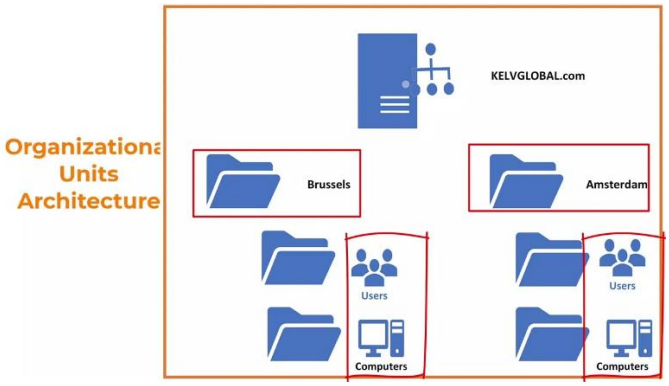
Logical

The AD hierarchy starts with a Forest, which contains Trees (holding one or more domains), and within each Domain are Organizational Units (OUs) to organize users and computers.

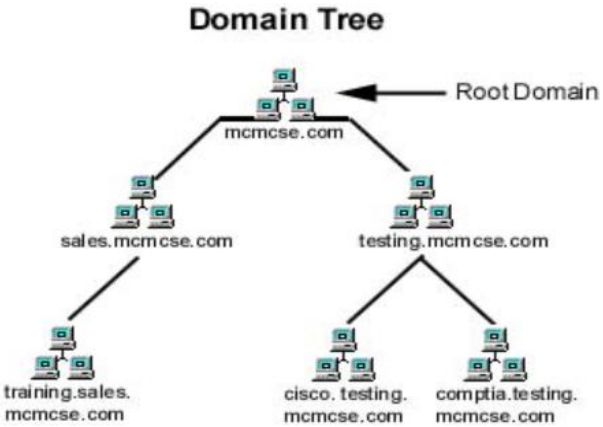
Domain: The primary component of Active Directory is the domain, which is a logical group of objects with common administrative, security, and replication settings.



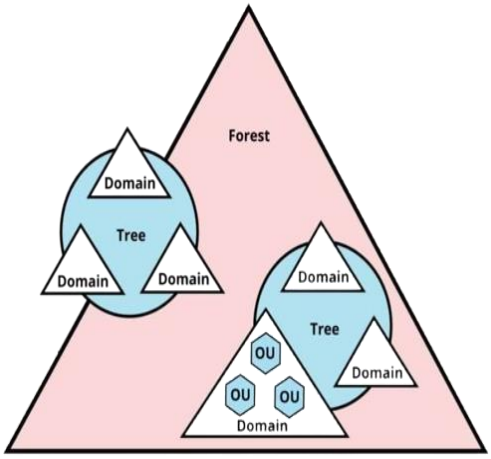
OU: An organizational unit (OU) is a container within a Microsoft Active Directory domain which can hold users, groups and computers.



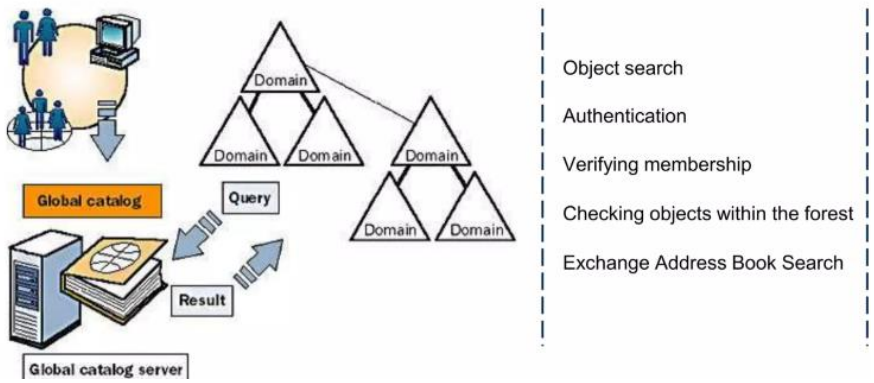
Tree: A domain tree is made up of several domains that share a common schema and configuration, forming a contiguous namespace. Domains in a tree are also linked together by trust relationships. Active Directory is a set of one or more trees.



Forest: A forest is the highest level of organization within Active Directory and is used to group one or multiple domains together. An Active Directory forest simply refers to all domains within a single AD installation and represents the security boundary of Active Directory.



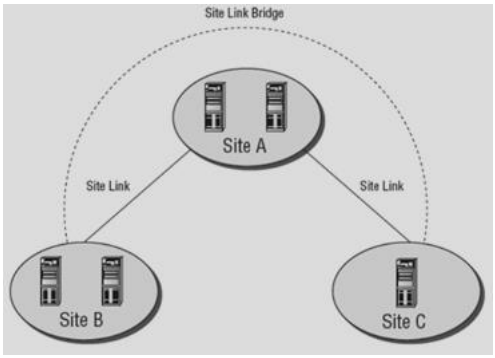
Global Catalog: The global catalog is a feature of Active Directory (AD) that allows a domain controller (DC) to provide information on any object in the forest.



Physical

In Active Directory (AD), the physical architecture refers to how the underlying network infrastructure is organized to support AD, focusing on the actual placement of servers and network resources.

Site: In Active Directory, a site is a logical grouping of network objects, such as domain controllers, that are connected by high-speed links. Sites are used to control the replication of directory data between domain controllers and to optimize network traffic.

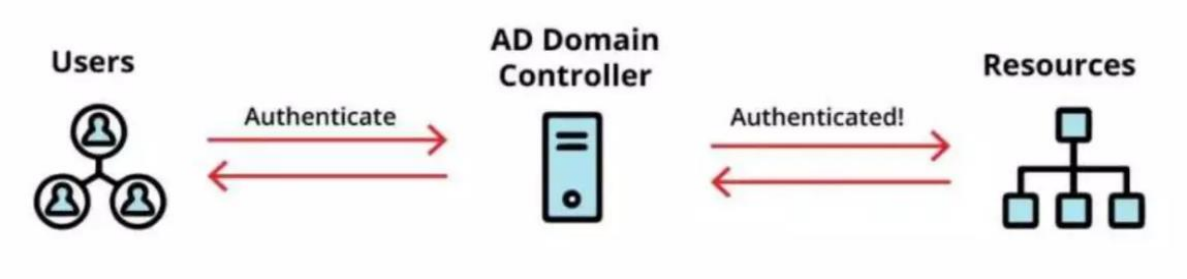


Domain Controller:

A Domain Controller is an Active Directory Server that acts as the brain for a windows server domain it supervises that entire network within the domain, it acts as a gatekeeper for user, authentication and IT resources authorization.

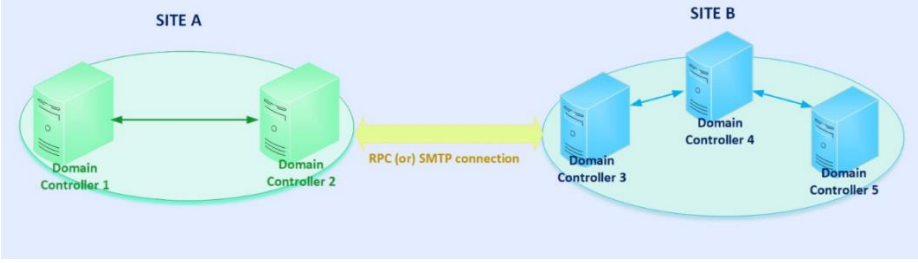
Here are some other things to know about DCs:

- Each AD domain needs at least one DC.
- DCs store a copy of the directory file and replicate changes to other DCs in the domain.
- DCs are often installed in clusters to improve reliability and availability.
- DCs can be used to detect cyberattacks.
- You can locate DCs in Active Directory by opening the Active Directory Users and Computers snap-in, connecting to the domain, and clicking on the Domain Controllers OU.



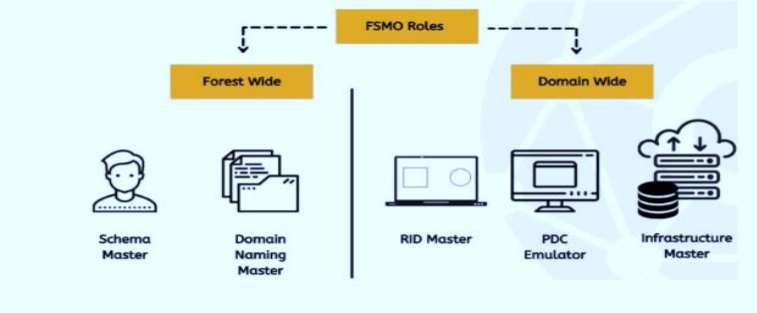
Replication:

Active Directory (AD) replication is the process by which the Active Directory database (NTDS) is copied and synchronized across multiple Domain Controllers (DCs) within the network. The goal of AD replication is to ensure consistency of data across all domain controllers in a domain or forest.



FSMO (Flexible Single Master Operations)

FSMO roles are unique responsibilities given to one or more DCs in AD to handle specific tasks that cannot be replicated.

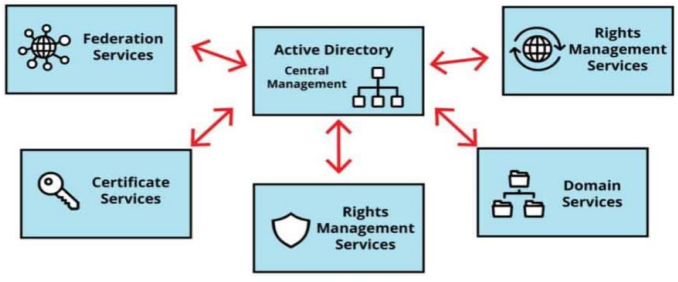


1. Schema Master An enterprise-level FSMO role. There is only one schema master in the entire forest, which is capable of handling schema changes.
2. Domain Naming Master An enterprise-level FSMO role. There is only one domain naming master, which is in charge of managing domain names.
3. Relative Identifier Master The RID is a domain-level FSMO role. It is in charge of keeping blocks of SIDs and assigning them to different DCs within the domain.
4. Primary Domain Controller Emulator A domain-wide FSMO role. The DC with the PDC Emulator role is, the DC with the highest authority within the domain. This role deals with authentication requests, passwords changes, group policy objects, and also provides the time.
5. Infrastructure Master It is a domain-level FSMO role that translates GUIDs, SIDs, and DNs between domains. This role gets references from other objects in other domains.

Active Directory Services

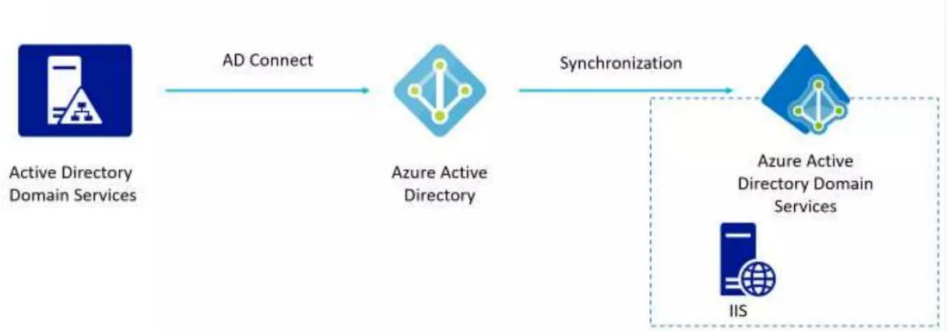
Active Directory provides multiple out-of-the-box services to manage identities, permissions, and access to a network's resources.

- Active Directory Domain Services (AD DS).
- Active Directory Federation Services (AD FS).
- Active Directory Rights Management Services (AD RMS).
- Active Directory Certificate Services (AD CS).
- Active Directory Lightweight Directory Services (AD LDS).



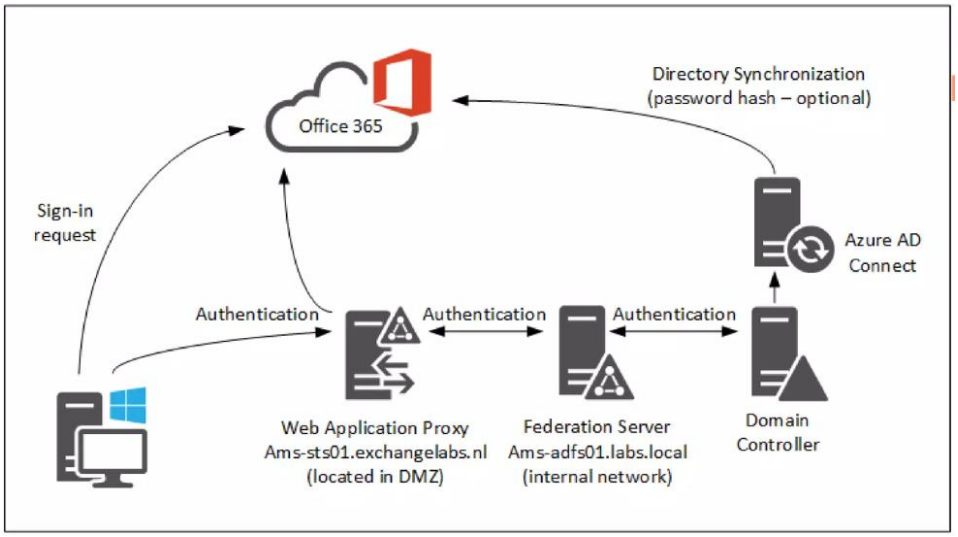
Active Directory Domain Services

Active Directory Domain Services (AD DS) is the most popular server role in Active Directory. It is the directory service that provides the technology for storing directory data. It also makes this data available and manageable for all end-users.



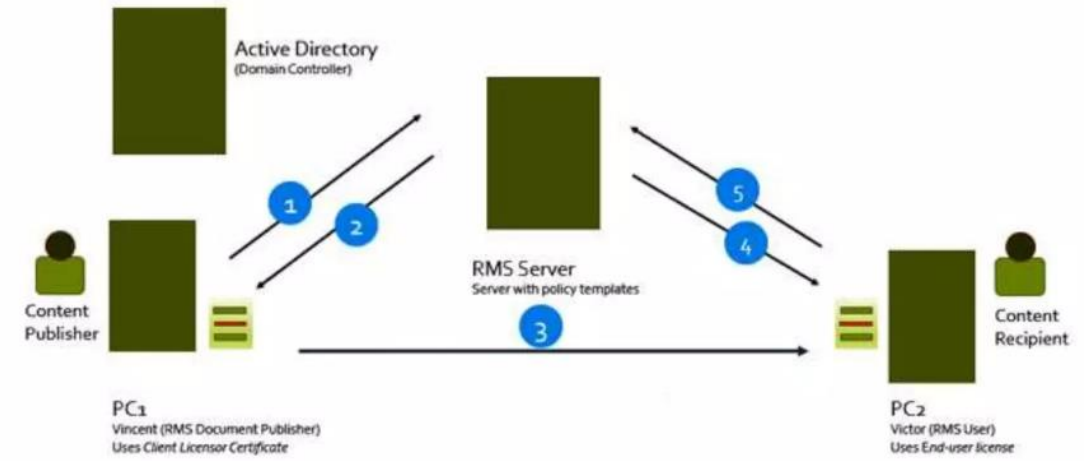
Active Directory Federation Services

Active Directory Federation Service (AD FS) is an identity management solution providing Single Sign-On (SSO) for secure access to multiple web apps and resources. It allows users to access various services with one set of credentials by sending authentication claims instead of direct credentials to third-party applications.



Active Directory Rights Management Services

Active Directory Rights Management Services (AD RMS) is a data access control solution that protects documents (e.g., emails, Office files) through encryption and enforces data access policies. It controls user permissions, restricts actions like editing or copying, and encrypts/decrypts digital content.

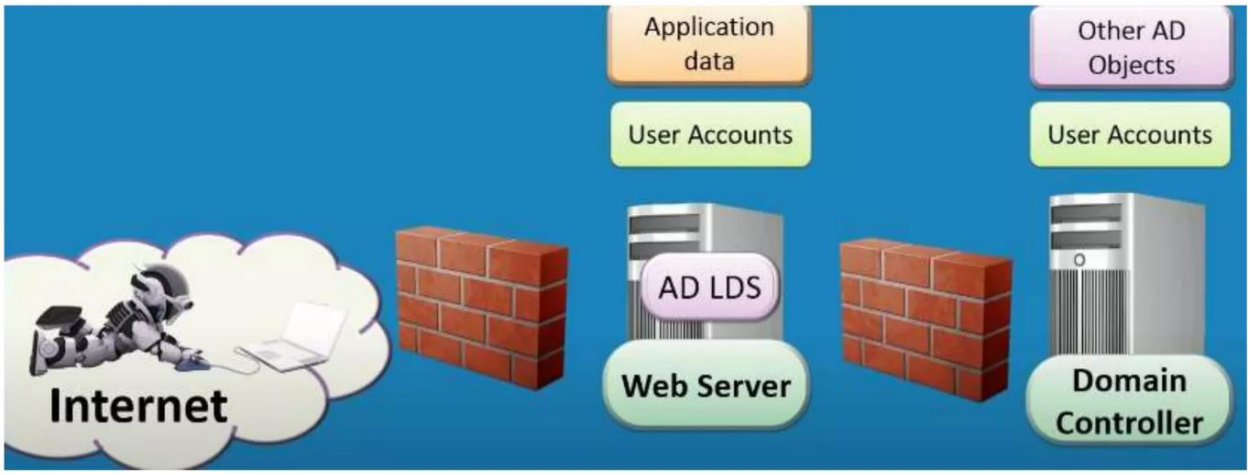


Active Directory Certificate Services

Active Directory Certificate Services (AD CS) enables managers to create and manage Public Key Infrastructure (PKI) for digital certificates. It supports certificate issuance, policy enforcement, automated provisioning, and uses Active Directory data for certificate registration and group policy enforcement.

Active Directory Lightweight Directory Services

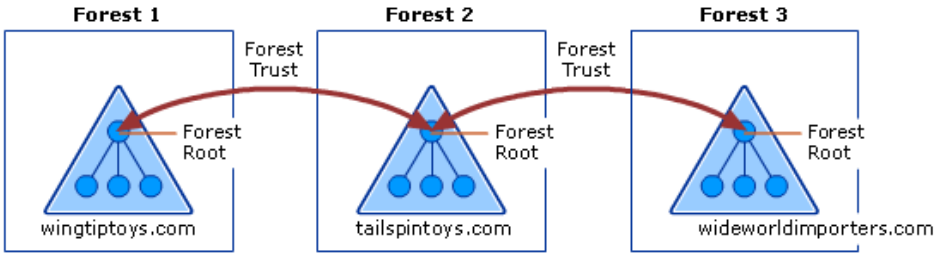
Active Directory Lightweight Directory Services (AD LDS) is an independent LDAP directory service for applications, not limited by AD domains or forests. It operates on stand-alone servers, offering its own data store and access services.



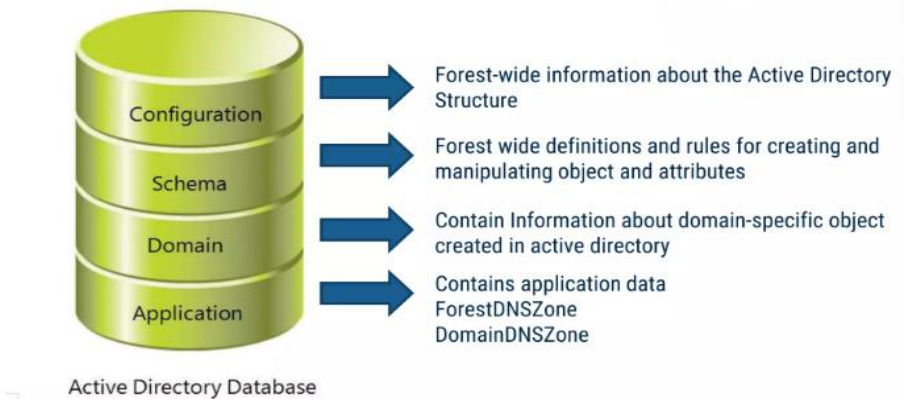
How trust relationships work for forests in Active Directory?

Forest trusts in AD DS enable secure access across multiple forests, useful for organizations with separate infrastructures, mergers, or extranets. Forest trusts create one-way or two-way transitive relationships between forest root domains for smooth authentication.

- Direct Trust: Trusts are direct; if Forest 1 trusts Forest 2, it doesn't implicitly trust Forest 3.
- One-way Access: Only members of the trusted forest can access resources in the trusting forest.
- DNS Setup: Requires proper DNS, like a root server or conditional forwarders.
- Permissions: Needs Domain Admin or Enterprise Admin roles.



Active Directory Database



SYSVOL: SYSVOL, or System Volume, is a shared folder on each domain controller (DC) in an Active Directory domain that stores essential files and scripts:

- **Group Policy Objects (GPOs):** Control settings like password complexity and desktop wallpapers.
- **Scripts:** Perform automated tasks when users interact with the domain, such as startup and shutdown scripts.
- **Logon and logoff scripts:** Required for user logins and access rights.