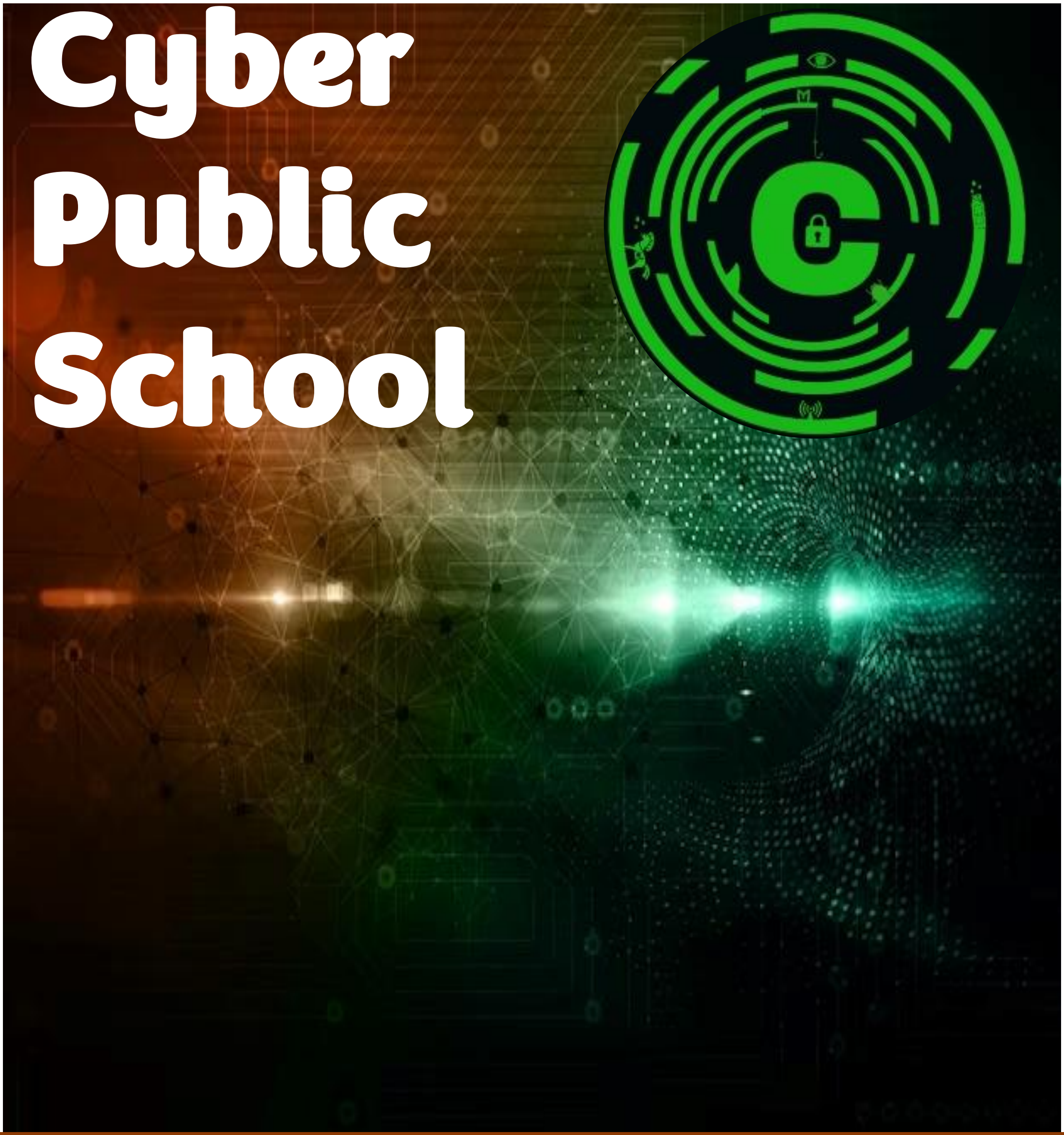


Cyber
Public
School

Basics of Active Directory

https://cyberpublicschool.com/

AD

Active Directory

Basics of Active Directory

“What” and “Why” Active directory

In simple terms, Active Directory (AD) is a Microsoft technology that helps organizations manage and organize their computer systems, users, and resources. It acts like a digital directory or address book for a network, keeping track of information about users, computers, and other networked devices.

Some key purposes and benefits of using Active Directory:

- Centralized Management
- User Authentication and Authorization
- Security
- Group Policy
- Resource Management
- Scalability
- Single sign-on

Centralized Management → All network resources can be managed and controlled in an organised and centralised manner with the help of Active Directory. Computers, printers, user accounts, and other networked equipment fall under this category.

User Authentication and Authorization → It functions as a central authentication system, enabling users to log in with just their username and password and granting access according to their roles and permissions on the network.

Security → Active Directory enables the implementation of security policies and access controls. To guarantee that only authorised users have access to particular resources, administrators can establish and enforce security settings.

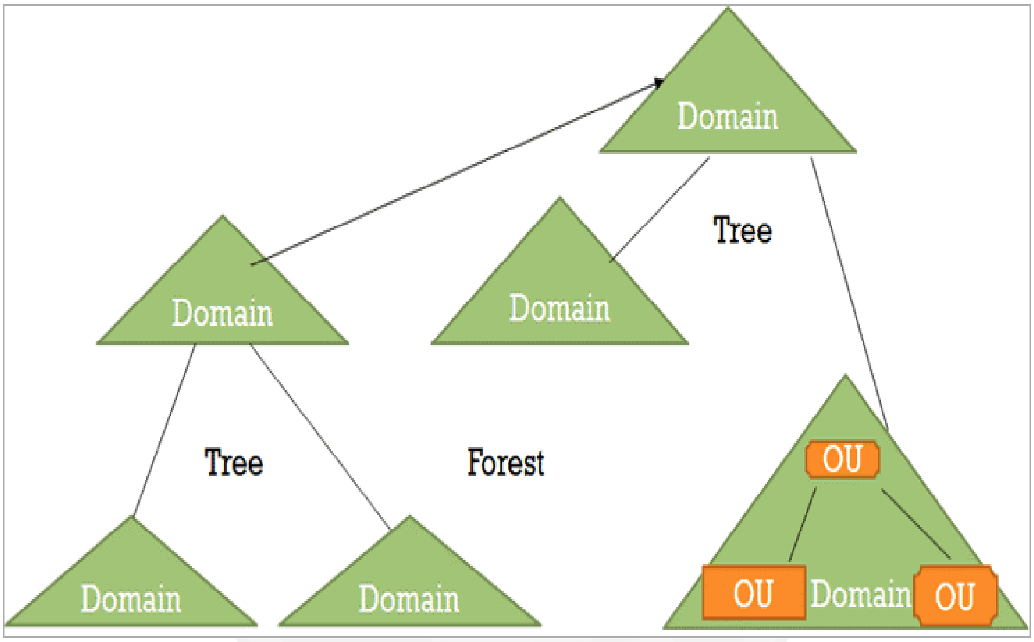
Group Policy → Group Policy allows network administrators to apply and enforce settings on several computers at once. This aids in keeping software installations, security settings, and configurations consistent.

Resource Management → It enables network resources like printers, files, and apps an organised way to be arranged and managed. This makes it easier for administrators to allocate resources efficiently.

Scalability → The increase in the size of the organisation will not affect the functionality of Active Directory. The directory structure can readily accommodate more users, computers, and resources as the organisation expands.

Single sign-on → Users can utilise a single set of credentials to access a variety of resources and services while using Active Directory. This improves user convenience and streamlines the login procedure.

Main Terminologies and Components of Active Directory



Tree → A tree is one or more domains grouped together.

Forest → A forest is a group of multiple trees.

Organizational Unit → Organizational Units (OUs) organize users, groups and devices. Each domain can contain its own OU.

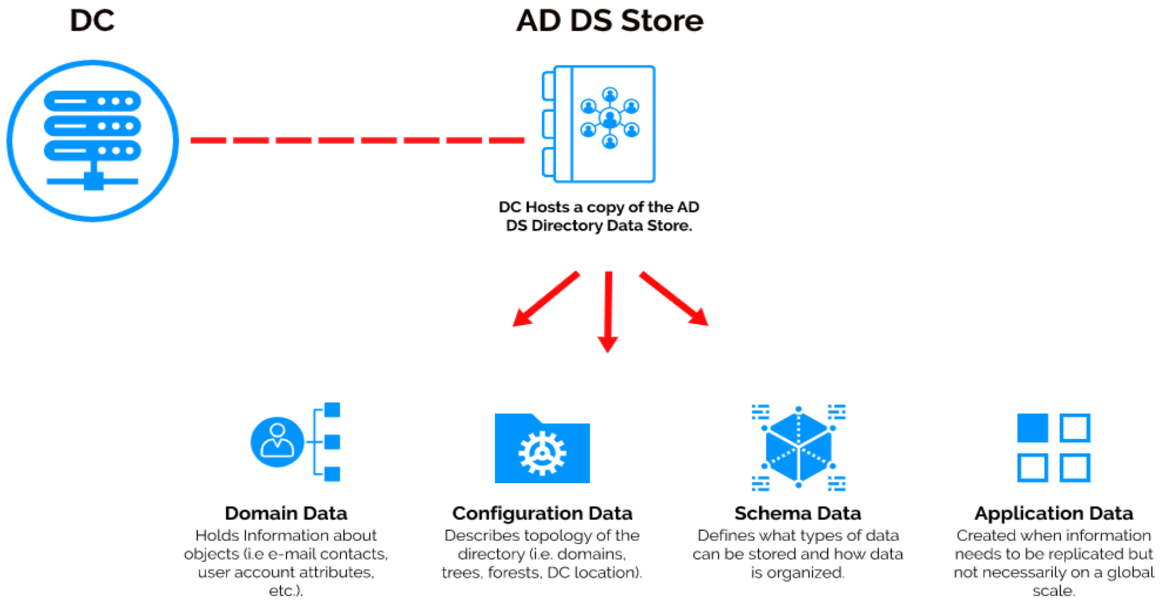
Containers → Containers and OUs are comparable but container objects cannot be linked or applied to by Group Policy Objects.

Trust → By creating an Active Directory trust (AD trust), two different Active Directory domains (or forests) can be connected so that users in one domain can authenticate against resources in the other.

Trusting Domain → This domain trusts another domain to authenticate users for them.

Trusted Domain → This domain authenticates users on behalf of another domain.

Domain controller and AD DS Data Store



DC

AD DS Store

DC Hosts a copy of the AD DS Directory Data Store.

Domain Data
Holds Information about objects (i.e e-mail contacts, user account attributes, etc.).

Configuration Data
Describes topology of the directory (i.e. domains, trees, forests, DC location).

Schema Data
Defines what types of data can be stored and how data is organized.

Application Data
Created when information needs to be replicated but not necessarily on a global scale.

Domain controller → Domain controllers are the center of Active Directory. They are in charge of controlling the rest of the domain components.

Functions of Domain controllers

- handles authentication and authorization services
- Synchronize updates from additional domain controllers across the entire forest.

- Grants administrative access for the management of resources within the domain.
- holds the AD DS data store.

AD DS Data Store → All directory information is stored in a data store by the Active Directory directory service. Information on domains, users, groups, machines, organisational units, and security rules are all contained in the directory. The AD DS data store consists of :-

>>>Consists of the Ntds.dit file (Ntds.dit file consist of information about user objects, groups, and group membership. It includes the password hashes for all users in the domain.)

>>>Is stored by default in the %SystemRoot%\NTDS folder on all domain controllers

>>>Is accessible only through the domain controller processes and protocols

Users and Groups

Users → In Active Directory network, there are four basic categories of users; however, based on an organization's access management practices, more user types may exist. The four types of users are :-

- Domain Admins
- Service Accounts
- Local Administrator
- Domain users

Domain Admins → These are accounts with administrative privileges at the domain level. Domain administrators have extensive control over the Active Directory domain, including the ability to add and remove users, manage group policies, and perform other administrative tasks.

Service Accounts → These accounts are used by services and applications to interact with the domain. Service accounts are configured with specific permissions and are often used for running services like web servers, database servers, or other applications that need to access network resources.

Local Administrator → This refers to an account that has administrative privileges on a specific computer or device. These rights are confined to the local machine and do not extend to the entire domain. Having local administrator rights allows a user to perform tasks such as installing software, configuring system settings, and managing other user accounts on that specific computer.

Domain users →These are standard user accounts that are used by individuals to log in to the domain and access resources for which they have permissions. They are typically assigned to individual employees in an organization.

GROUPS → Groups make it easier to give permissions to users and objects by organizing them into groups with specified permissions. Some default groups may include :-

- - Domain controllers
- - Domain guests
- - Domain users
- - Domain Computers
- - Domain Admins
- - Group Policy Creator owners
- - DNS Admins, and the list goes on…

Domain Trusts and Domain Policies

Domain Trust— is a relationship established between two domains in Active Directory that allows users from one domain to access resources in another domain. Trusts are used to enable authentication and authorization across domain boundaries.

There are two types of trusts that determine how the domains communicate. Those are known as :-

- **- Directional →**The direction of the trust flows from a trusting domain to a trusted domain
- **- Transitive →** A transitive trust is one that can extend beyond two domains to include additional trusted domains. If Domain A trusts Domain B, and Domain B trusts Domain C, then Domain A can implicitly trust Domain C.
- **Domain Policy—** typically refers to the security policies and configurations applied to all computers within a specific domain through Group Policy.

Domain Services

Domain services are exactly what they sound like. The rest of the domain or tree receives these services from the domain controller. An extensive range of services can be added to a domain controller. Some of them are :-

>>> LDAP — Lightweight Directory Access Protocol; provides communication between applications and directory services .

>>>Certificate Services — allows the domain controller to create, validate, and revoke public key certificates.

>>>DNS, LLMNR, NBT-NS — Domain Name Services for identifying IP hostnames.

Contacts us

https://cyberpublicschool.com/

https://www.instagram.com/cyberpublicschool/

Phone no.: +91 9631750498 India
+91 73047 08634

Our Successful Oscp Student.