Introduction of Active Directory Domain Services

Active Directory (AD)

- A directory is a hierarchical structure that stores information about objects on the network. A directory, in the most generic sense, is a comprehensive listing of objects. A phone book is a type of directory that stores information about people, businesses, and government organizations. Phone books typically record names, addresses, and phone numbers.

- Active Directory (AD) is a Microsoft technology used to manage computers and other devices on a network. It is a primary feature of Windows Server, an operating system that runs both local and Internet-based servers.

- The main service in Active Directory is Domain Services (AD DS), which stores directory information and handles the interaction of the user with the domain. AD DS verifies access when a user signs into a device or attempts to connect to a server over a network. AD DS controls which users have access to each resource. For example, an administrator typically has a different level of access to data than an end user

- A server running Active Directory Domain Service (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user. Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services: Certificate Services, Active Directory Federation Services, Lightweight Directory Services, and Rights Management Services.

Active Directory Services

- Active Directory Services consist of multiple directory services. The best known is Active Directory Domain Services, commonly abbreviated as AD DS or simply AD.

- **Domain Services**

- **Lightweight Directory Services**

- **Certificate Services**

- **Federation Services**

- **Rights Management Services**

Forests, trees and domains

- The Active Directory framework that holds the objects can be viewed at a number of levels. The forest, tree, and domain are the logical divisions in an Active Directory network.

- Within a deployment, objects are grouped into domains. The objects for a single domain are stored in a single database (which can be replicated). Domains are identified by their DNS name structure, the namespace.

- A domain is defined as a logical group of network objects (computers, users, devices) that share the same Active Directory database.

- A tree is a collection of one or more domains and domain trees in a contiguous namespace, and is linked in a transitive trust hierarchy.

- At the top of the structure is the forest. A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest represents the security boundary within which users, computers, groups, and other objects are accessible

Domain Name System (DNS)

- Domain Name System (DNS) is one of the industry-standard suite of protocols that comprise TCP/IP, and together the DNS Client and DNS Server provide computer name-to-IP address mapping name resolution services to computers and users.

- Active Directory Domain Services (AD DS) uses DNS as its domain controller location mechanism. When any of the principal Active Directory operations is performed, such as authentication, updating, or searching, computers use DNS to locate Active Directory domain controllers. In addition, domain controllers use DNS to locate each other.

- The DNS Client service is included in all client and server versions of the Windows operating system, and is running by default upon operating system installation.
- When you configure a TCP/IP network connection with the IP address of a DNS server, the DNS Client queries the DNS server to discover domain controllers, and to resolve computer names to IP addresses.