GNS Technologies

Server History

Sr.No.	Operating System	Year
1	Win NT 3.1	1993
2	Win NT 3.4	1994
3	Win NT 4.0	1995
4	Win NT 5.0 (2000 Server)	2000
5	2003 Server	2003
6	2008 R1 Server	2008
7	2008 R2 Server	2009
8	2012 Server (R1 and R2)	2012

Workgroup	Domain
All individual computers(peer) are connected to share resources.	One or more computers are server. Computers are the members of servers
Every computer has set of users.To log on you must have user account on that computer.	Users are created on Server and user can logon to server by using client computer.
No computer can give permission and policies to another computer.	Network administrators give the permissions and policy on server and these policies and permissions are automatically applicable for all users and computer connected to domain.
Every computer gives the service(Server) and request for the service (client)	Server gives the network service and client computer request for the service.

GNS Technologies

Active Directory Domain Services

ADDS

ADDS History

Windows NT 4.0 --> Directory service name was NTDS

Windows 2000 --> Active Directory Service(ADS)

Windows 2003 --> Active Directory Service (ADS)

Windows 2008 –> Active Directory Domain Services (ADDS)

Windows 2012 –> Active Directory Domain Services (ADDS)

ADDS

- It is the Directory Service which provides Centralized hierarchy of directory database.
- The ADDS database stores information of user identity, computers, groups, services and resources.
- It is a self updating database.
- Database of ADDS is stored in NTDS folder.In NTDS folder there is a main file of ADDS database ie NTDS.dit

(New Technology Directory Service.Directory Information Tree)

Purpose of Active Directory

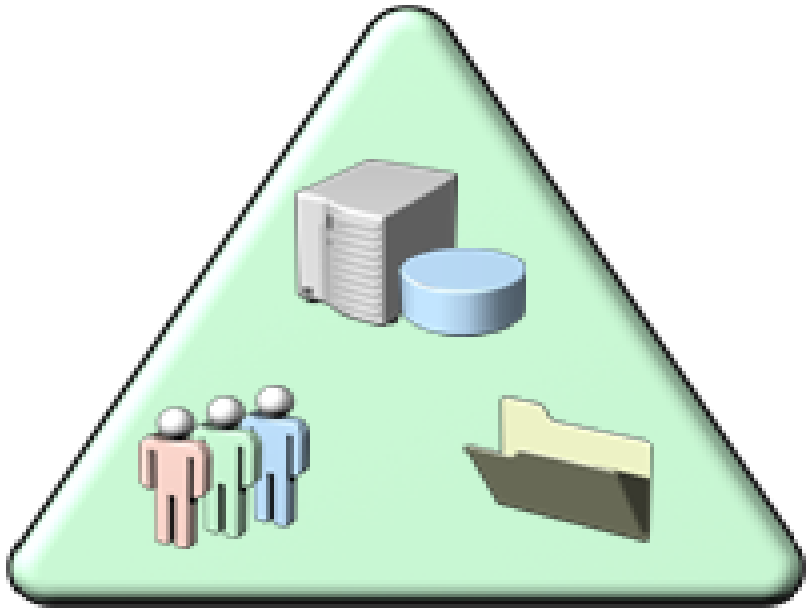
- Provides user Logon and Authentication Services using Kerberos protocol
- To Centralize and Decentralize the resource management.
- To centrally organize and manage –User Accounts, Computers, Groups, Network Resources.
- Enables authorized users to easily locate Network Resources.

AD DS is composed of both physical and logical components

Physical components	Logical components
• Data store • Domain controllers • Global catalog server • RODC	• Partitions • Schema • Domains • Domain trees • Forests • Sites • OUs

Understanding AD DS Domain Structure

- AD DS requires one or more domain controllers
- All domain controllers hold a copy of the domain database which is continually synchronized
  - The domain is the context within which users, groups, and computers are created
  - The domain is a replication boundary
  - The domain is an administrative center for configuring and managing objects
  - Any domain controller can authenticate any logon in the domain



Domain and Domain Controller

- Domain is Area or Area with boundary.
- Domain is logical group of users and computers.
- Domain is the logical secure administrative boundary of ADDS.
- To recognize every domain we have to give domain names. Example: Infosys.com
- Domain is represented by triangle.

Domain and Domain Controller

- A domain controller is a server that is configured to store a copy of the ADDS directory database(NTDS.DIT) and a copy of the SYSVOL folder.
- NTDS.DIT is the database itself, and the SYSVOL folder contains all the template settings of GPOs.
- Kerberos Authentication Service and Key Distribution Center(KDC) performs authentication.

GNS Technologies

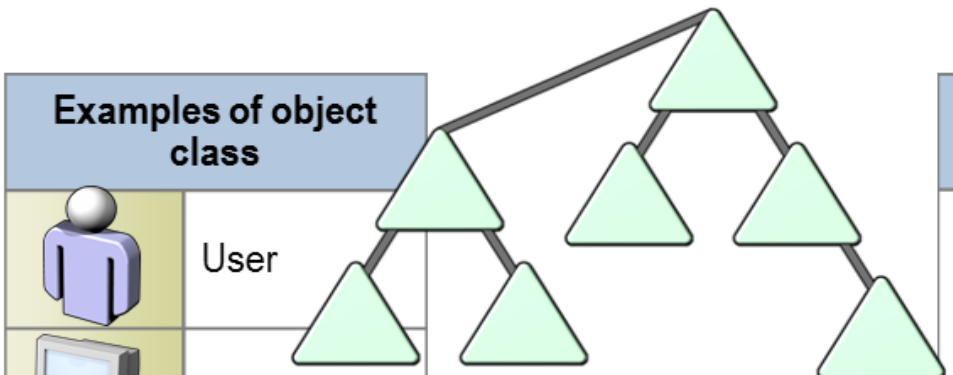
What is Active Directory Schema ?

The Active Directory schema acts as a blueprint for AD DS by defining the attributes and object classes such as:

- Attributes
  - objectSID
  - sAMAccountName
  - location
  - manager
  - department
- Classes
  - User
  - Group
  - Computer
  - Site

What Is a Schema?

- A forest-wide definition of object classes and attributes that can be extended
- Schema changes can be redefined or deactivated



Examples of object class	Examples of attributes
User	accountExpires department distinguishedName directReports dNSHostName operatingSystem repsFrom repsTo firstName lastName
Computer	
Printer	

GNS Technologies

Light Weigh Directory Access Protocol

LDAP

LDAP (Lightweight Directory Access Protocol) is an application protocol for querying and modifying items in directory service providers like Active

Directory, which supports a form of LDAP.

The **Lightweight Directory Access Protocol** (**LDAP**) is an open, vendor-neutral, industry standard **application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.**[1] **Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network.**

Kerberos 5.0

Active Directory By default uses this protocol to authenticate AD accounts.