Active directory functions and benefits

* Centralized resource and security administration.
* Single log on for access to global resources.
* Fault tolerance and redundancy.
* Simplified resource location.
* Centralized user and group management.

Provides 2 services

* AD DS (domain services): full-fledged directory service that is referred to as Active Directory in windows server.
* AD LDS (lightweight directory services) started in 2008: replaced LDAP. Lightweight, flexible directory platform that can be used by Active Directory developers without incurring the overhead of the full-fledged active directory service.

AD DS

* Differs from x.500 and LDAP by incorporating a "tree" concept for managing resources on a Windows network.
  + Stores information about the network resources and services, such as user data, printer, servers, databases, groups, computers, and security policies.
  + Identifies all resources on a network and makes them accessible to authorized users and applications.
  + Requires DNS as AD DS is not hierarchical in structure.

AD structure

* Forests: one or more domain trees, with each tree having its own unique name space.
* Domain trees: one or more domains with contiguous name space.
* Domains: a logical unit of computers and network resources that defines a security boundary.
* Name spaces are in a FQDN (fully qualified domain name) format.

AD Objects

* Include users, computers, servers, groups, organizational units (Ous), printers, etc
* All objects in the directory must have a name that is unique from a FQDN standpoint.
* Objects are assigned a Globally unique identifier (GUID) that is used by Active Directory to control the object.
* Objects have both required and optional attributes that define what, where, when, and how.
  + Username, group membership, phone, address, department

Understanding the schema

* Think of AD as a special database and the schema is not only the layout but also rules that govern objects.
* Defines the objects stored within AD the properties (attributes)associated within each object.
* Users, groups, and computers have diff properties. AD keeps a record of each and every piece.