7.1.3 Active Directory Facts

Active Directory is a centralized database that contains user account and security information used for authentication and access control. In a workgroup, authentication and access control are managed separately on each computer, with each computer holding information about users and resources. With Active Directory, all computers share the same central database, which is stored in a file called **Ntds.dit**. This is the database file that stores all directory data.

The Active Directory structure contains the following components:

Component	Description

Trees and Forests	Multiple domains are grouped in the following relationship:
	▪ A *tree* is a group of related domains that share the same contiguous DNS namespace.
	▪ A *forest* is a collection of related domain trees. The forest establishes the relationship between trees that have different DNS name spaces.
	Trees and forests have the following characteristics:
	▪ The *forest root domain* is the top-level domain in the top tree. It is the first domain created in the Active Directory forest.
	▪ The *tree root domain* is the highest domain in a tree.
	▪ Each domain in the tree that is connected to the tree root domain is called a *child domain*.
	▪ A *domain tree* is a group of domains based on the same namespace. Domains in a tree:
	  ▪ Are connected with a two-way transitive trust.
	  ▪ Can share resources with any other domain in the forest.
	  ▪ Share a common schema.
	  ▪ Have common global catalogs.

Domain	A *domain* is an administratively-defined collection of network resources that share a common directory database and security policies. The domain is the basic administrative unit of an Active Directory structure.
	▪ Database information is replicated (shared or copied) within a domain.
	▪ Security settings are not shared between domains.
	▪ Each domain maintains its own set of relationships with other domains.
	▪ Domains are identified using DNS names.
	  ▪ The common name is the domain name itself.
	  ▪ The distinguished name includes the DNS context or additional portions of the name.
	Depending on the network structure and requirements, the entire network might be represented by a single domain with millions of objects. Alternatively, the network structure and requirements may require multiple domains.

Organizational Unit (OU)	An *organizational unit* is like a folder that subdivides and organizes network resources within a domain. An organizational unit: ▪ Is a container object. ▪ Can logically organize network resources. ▪ Simplifies security administration. You should know the following OU facts: ▪ OUs can contain other OUs or any type of leaf object (e.g. users, computers, and printers). ▪ First-level OUs are sometimes called *parents*. ▪ Second-level OUs are sometimes called *children*.
Default Containers	Like OUs, default containers are used to organize Active Directory objects. Default containers: ▪ Are created by default ▪ Cannot be created, moved, renamed, or deleted ▪ Have very few editable properties ▪ Cannot have Group Policy settings applied to them
Objects	Within Active Directory, each resource is identified as an *object*. Common objects include: ▪ Users ▪ Groups ▪ Computers

	You should know the following about objects: ▪ Each object contains *attributes* (information about the object, such as a user's name, phone number, and email address), which are used to locate and secure resources. ▪ The *schema* identifies the object classes, or object types, that exist in the tree and the attributes, or properties, of the object. ▪ Active Directory uses DNS to locate and name objects. ▪ Container objects hold or group other containers or leaf objects.
Domain Controller	A *domain controller* is a server that holds a copy of the Active Directory database that can be written to. ▪ A domain controller is a member of only one domain. ▪ Any domain controller can make changes to the Active Directory database. ▪ *Replication* is the process of copying changes to the Active Directory database between domain controllers.
Global Catalog	The global catalog (GC) is a database that contains a partial replica of every object from every domain within a forest. A server that holds a copy of the global catalog is a *global catalog server*. The global catalog facilitates faster searches because it doesn't require referencing different domain controllers.