

## 8.7.4 Active Directory Facts

Active Directory is a centralized database that contains user account and security information. In a workgroup, security and management are decentralized as they take place on each individual computer, with each computer holding separate information about users and resources. With Active Directory, all computers share the same central database.

Active Directory organizes network resources and simplifies management using the following components:

| Component                | Description   |
|--------------------------|---|
| Domain                   | A <i>domain</i> 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. Depending on the network structure and requirements, the entire network might be represented by a single domain with millions of objects, or the network might require multiple domains.   |
| Trees and Forests        | Multiple domains are grouped together in the following relationship: <ul style="list-style-type: none"> <li>A <i>tree</i> is a group of related domains that share the same contiguous DNS namespace.</li> <li>A <i>forest</i> is a collection of related domain trees. The forest establishes the relationship between trees that have different DNS namespaces.</li> </ul>  |
| Organizational Unit (OU) | An <i>organizational unit</i> is like a folder that subdivides and organizes network resources within a domain. An organizational unit: <ul style="list-style-type: none"> <li>Is a container object</li> <li>Can hold other organizational units</li> <li>Can hold objects such as users and computers</li> <li>Can be used to logically organize network resources</li> <li>Simplifies security administration</li> </ul>   |
| Generic Container        | Like OUs, generic containers are used to organize Active Directory objects. Generic container objects: <ul style="list-style-type: none"> <li>Are created by default</li> <li>Cannot be moved, renamed, or deleted</li> <li>Have very few properties you can edit</li> </ul> You cannot create generic containers; use OUs instead.   |
| Object                   | Within Active Directory, each resource is identified as an <i>object</i> . Common objects include: <ul style="list-style-type: none"> <li>Users</li> <li>Groups</li> <li>Computers</li> <li>Printers</li> <li>Shared folders</li> </ul> Each object contains additional information about the shared resource that can be used for locating and securing resources. Groups are composed of other directory objects that have a common level of access. The <i>schema</i> identifies the object classes (the type of objects) that exist in the tree and the attributes (properties) of the objects. <p>In Active Directory, each user is assigned a SAM account name; therefore, each user name must be unique.</p> |
| Domain Controller        | A <i>domain controller</i> is a server that holds a copy of the Active Directory database that can be written to. <i>Replication</i> is the process of copying changes to Active Directory between the domain controllers. In contrast, <i>member servers</i> are servers in the domain that do not have the Active Directory database.   |

Active Directory is a hierarchical database. Hierarchical directory databases have the following advantages over flat file database structure:

- Organization
- Delegation
- Replication
- Scalability