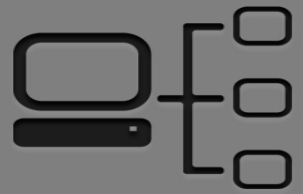
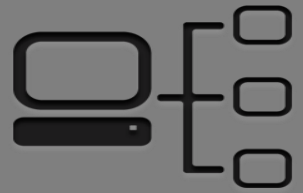
# What is Active Directory (AD)?



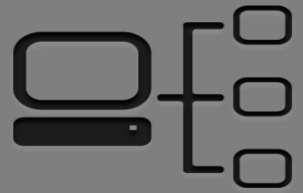
- Active Directory is a directory service database, developed by Microsoft to manage Windows Domain network.
- It’s single database repository for all sorts of user and computer-related information on a network:
  - User Accounts
  - Computer Accounts
  - Security Groups
  - Files
  - Etc.

# AD Provides Centralized Security



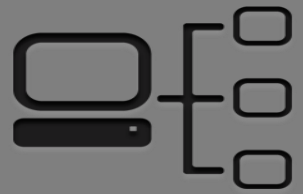
- Active Directory provides centralized authentication, authorization, and accounting (AAA) through:
  - Single Sign-on Functionality
  - Logical Access Control
  - Security Groups
  - Organizational Units (OUs)
  - Group Policy Objects (GPOs)
- Ensures that only authorized users can logon to AD network computers.
- Provides centralized storage of all user and computer accounts.

# AD Provides Centralized Management



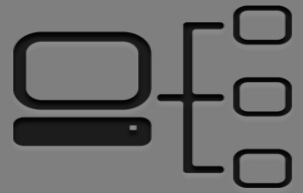
- Active Directory
  - Enables a domain administrators to centrally manage users and network resources.
  - Allows domain administrators to easily locate information.
  - Allows domain administrators to group objects into OUs.
  - Uses Group Policies to specify policy-based settings.

# AD Domain Controllers



- A Domain Controller (DC) is a Windows Server in which AD has been installed and activated.
- This is accomplished by adding the Active Directory Domain Services (AD DS) Role and promoting a server to a DC.
- AD DS uses domain controllers to give network users access to permitted resources on the network via a single sign-on.

# Understanding LDAP



- AD is based on the Lightweight Directory Access Protocol (LDAP).
- LDAP is a protocol designed for querying and modifying directory services by the University of Michigan in the early 1990s.
- It provides a common language for clients and servers to speak to one another.