Roles in Active Directory 2012:

AD 2012 follows role based administration and there are five major roles available.

* AD Domain Service Role
* AD Federation Role
* AD Certification Role
* AD RMS Role (Rights Management Service)
* AD LDS (Light Weight Directory Service)

# AD Domain Service Role (AD DS)

* AD DS provides authentication and authorization within a network
* A server that is running AD DS is called a domain controller.
* Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use.
* Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.
* This data store, also known as the directory, contains information about Active Directory objects.
* These objects typically include shared resources such as servers, volumes, printers, and the network user and computer accounts.

# AD Federation Role (AD FS)

* AD FS provides simplified, secured identity federation and Web single sign-on (SSO) capabilities for end users who want to access applications within an AD FS-secured enterprise, in federation partner organizations, or in the cloud.
* The function of providing extranet access to applications and services that are secured by AD FS is now performed by a new Remote Access role service called Web Application Proxy.
* Web Application Proxy is a server role designed to provide access for the AD FS-related extranet scenario and other extranet scenarios.

# AD Certification Role (AD CS)

* AD CS provides customizable services for issuing and managing digital certificates used in software security systems that employ public key technologies.
* The digital certificates that AD CS provides can be used to encrypt and digitally sign electronic documents and messages. These digital certificates can be used for authentication of computer, user, or device accounts on a network.
* Digital certificates are used to provide:
  + Confidentiality through encryption
  + Integrity through digital signatures
  + Authentication by associating certificate keys with computer, user, or device accounts on a computer network

# AD LDS (Application)

* AD LDS is a Lightweight Directory Access Protocol (LDAP) directory service designed for use with directory-enabled applications.
* A directory-enabled application is one that uses a directory, as opposed to a database or flat file, for its data store.
* AD LDS serves as an identity provider for business scenarios that desire an extranet directory to store customer user accounts, where these accounts need to be separate from the enterprise Active Directory Domain Services (AD DS) user account store.
* AD LDS is also a supported store for authorization policy by Windows Authorization Manager.
* In environments where AD DS exists, AD LDS can use AD DS for the authentication of Windows security principals.

# AD RMS

* AD RMS can serve to reinforce the security strategy in your organization - protecting documents using IRM (Information Rights Management) technology.
* AD RMS allows individuals or administrators to set permissions to access documents, workbooks, and presentations via IRM policies.
* This helps to prevent the printing, forwarding or copying of sensitive information by persons who do not have permission to do so.
* When access to a file is limited by IRM, it forces access restrictions regardless of where the information is because the file permissions are stored in the document file itself.
* AD RMS and IRM help individuals enforce their personal preferences regarding the transfer of personal or private information.
* They also enable organizations to enforce corporate policies that control and distribute confidential or proprietary information.