Chapter 6 -- Designing Organizational Unit and Group Structure

1. What is an OU and what is its primary use?

An organizational unit (OU) is a container within a Microsoft Active Directory domain which can hold users, groups and computers. It is the smallest unit to which an administrator can assign Group Policy settings or account permissions. An organizational unit can have multiple OUs within it, but all attributes within the containing OU must be unique. Active Directory organizational units cannot contain objects from other domains.

The concept of the organizational unit is derived from the Lightweight Directory Access Protocol (LDAP) standard upon which AD DS was built.

Each object in the AD DS structure can be referenced via LDAP queries that point to its specific location in the OU Structure.

2. What is a Group and how does it differ from an OU?

Groups in Windows Server 2012 come in two flavors: security and distribution groups. Groups serve to logically organize users into an easily identifiable structure.

Security groups are used to apply permissions so that large groups of users can be administered more easily. Security groups have a unique security identifier (SID) associated with them in much the same way that individual users in AD DS have a SAD.

Distribution groups is a group whose members are able to receive SMTP mail messages that are sent to the group. In most cases distribution groups are not used in environments without Exchange Server because their functionality is limited to infrastructures that can support them.

Groups can be organized into different scopes as indicated in #3 below.

3. Discuss the 4 primary group scopes in AD DS?

- Machine local groups – Built in groups in the OS and can be applied only to objects local to the machine in which they exist. They are default local groups such as Power Users and Administrators and the like created on a standalone system.
• Domain local groups – Can be used to establish permissions on resources in the domain in which they reside. Domain local groups can contain members from anywhere in an AD DS forest or trusted domain outside the forest.

• Global groups – Are used in sorting users into easily identifiable groupings and using them to apply permissions to resources. What separates global groups from universal groups is that global groups stop their membership replication at the domain boundary.

• Universal groups – Are universal and contain objects from any trusted domain and can be used to apply permissions to any resource in the domain. The limiting factor is that membership in universal groups is replicated across the entire forest.

4. What is a group policy object and what’s its use?

Group Policy is an infrastructure that allows you to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects (GPOs), which are linked to the following Active Directory directory service containers: sites, domains, or organizational units (OUs), but can be configured to apply specifically to groups. This functionality increases the domain designer’s flexibility to apply group policies.

For example, a group policy can be established to display a legal disclosure to all users who attempt to log on to a system, or it can set up to limit access to the command prompt.