Adam Morgan 3/14/11 Chapter 4

**Working with Organizational Units**

* Active Directory is based upon standards (LDAP and X.500)
* Lightweight Directory Access Protocol (LDAP)
* Created by the Internet Engineering Task Force (IETF)
* Based on the X.500 Directory Access Protocol (DAP)
* Forms the base around with Active Directory is built, which allows applications to use LDAP to integrate with Active Directory
* LDAP has presence on other operating systems as well, and can be used to integrate them with Active Directory
* Benefits of using OUs:
  + You can create familiar hierarchical structures based on an organizational chart to allow easy resource access
  + Delegation of administrative authority  **assign to someone**
  + Able to change OU structure easily
  + Can group users and computers for the purposes of assigning administrative and security policies
  + Can hide AD objects for confidentiality or security reasons

**OU Delegation of Control**

* Delegation of control means a person with higher security privileges assigns authority to a person of lesser security privileges to perform certain tasks
* Allows specific control of what someone with delegated control may do
* Commonly delegated tasks include:
  + Create, delete, and manage user accounts
  + Reset user passwords and force password change at next logon
  + Read all user information
  + Create, delete, and manage groups
  + Modify the membership of a group
  + Manage group policy links
  + Generate Resultant Set of Policy (Planning)
  + Generate Resultant Set of Policy (Logging)

**Active Directory Object Permissions**

* Three types of objects can be assigned permission to access an AD object: Users, groups, and computers. These object types are referred to as security principals. **ACL access control list**
* AD object’s security settings are composed of three components:
  + Discretionary Access Control List (DACL)
    - Each entry referred to as an access control entry (ACE)
  + Object Owner
    - Usually the user account that created the object or a group of user who has been assigned ownership
  + System access control list
* Each object has a list of standard permissions and a list of special permission
* Each permission can be set to Allow or Deny, and five standard permissions are available for most objects:
  + Full controls
  + Read
  + Write
  + Create all child objects
  + Delete all child objects

**Directory Partitions**

* Each section of an AD database is referred to as a directory partition. There are five directory partition types in the AD database:
  + Domain directory partition
    - Contains all objects in a domain, including users, groups, computers, OUs, and so forth
  + Schema directory partition
    - Contains information needed to define AD objects and object attributes
  + Global catalog partition
    - Holds the global catalog, which is a partial replica of all objects in the forest
  + Application directory partition
    - Used by applications and services to hold information that benefits from AD
  + Configuration partition
    - Holds configuration information that can affect the entire forest

**Operations Master Roles**

* Several operations in a forest require having a single domain controller, called the operations master, with sole responsibility for the function
* First domain controller in the forest generally takes on the role of the operations master
* If necessary, responsibility for these roles can be transferred to another domain controller
* There are five operations master roles, referred to as **Flexible Single Master Operation** (FSMO) roles in an AD forest:
  + Schema Master
  + Infrastructure master
  + Domain Naming master
  + RID master
  + PDO Emulator master (Primary Domain Controller)
* When removing DCs from a forest, be careful that these roles are not removed from the network accidentally

**Active Directory Replication**

* Replication is the process of maintaining a consistent database of information when the database is distributed among several locations
  + Intrasite replication
    - Replication between domain controllers in the same site
  + Intersite replication
    - Occurs between two or more sites
  + Multimaster replication
    - Used by AD for replacing AD objects
* **Knowledge Consistency Checker** (KCC) runs on all DCs
* Determines the replication topology, which defines the domain controller path that AD changes flow through and ensures no more than three hops exist between any two DCs

**Trust Relationships**

* In AD, a trust relationship defines whether and how security principals from one domain can access network resources in another domain
* Since Windows 2000 AD, trust relationships are established automatically between all domains in a forest
* Trusts do not equal permissions

**Effective Permissions**

* Effective permissions for an object are a combination of the allowed and denied permissions assigned to a security principal
* Can come from assignments made directly to a single user account or to a group the user belongs to
* Explicit permissions override inherited permissions, and can create some exceptions to the rule that Deny permissions override Allow permissions.

**The Role of Forests**

* The LARGEST component of AD
* All domains in a forest share some common characteristics:
  + A single schema
  + Forest-wide administrative accounts
  + Operations masters
  + Global Catalog
  + Trusts between domains
  + Replication between domains

**The importance of the global catalog server**

* First DC installed in a forest is automatically designated as a Global Catalog server, but additional global catalog servers can be configured as well
* Global catalog servers perform the following vital functions:
  + Facilitates domain and forest-wide searches (speeds searches outside my domain)
  + Facilitates logon across domains; Users can log on to computers in nay domain by using their **user principal name** (UPN) [username@domain.com]
  + Hold Universal Group membership information (accounts from multiple domains)

**Forest Root Domain**

* First domain is the forest root and is referred to as the forest root domain
* Imperative to the functionality of AD; if it disappears, the entire structure ceases to operate
* Functions the forest root domain usually handles:
  + DNS server – can’t connect by name
  + Global catalog server
  + Forest-wide administrative accounts
  + Operations masters
* Due to the importance of the forest root domain’s functionality, some organizations choose a dedicated forest root domain
* The advantages of running a dedicated forest root domain include the following:
  + More secure
  + More manageable
  + More flexible

**Choosing a Single or Multiple Forest Design**

* Most organizations operate under a single AD forest, which has a number of advantages:
  + A common AD structure
  + Easy access to network resources
  + Centralized management
* The advantages of single forest structure are also limitations in many aspects; diversity within an organization may take single forest design unfeasible. Multiple forest design includes the following advantages:
  + Differing schemas are possible
  + Security boundaries
  + Separate administration

**Understanding Trusts**

* Trusts allow users in one domain to access resources in another domain, without requiring a user account on the other domain
* Types of trust:
  + One way or tow way trusts
  + Transitive trusts
  + Shortcut trusts
  + Forest trusts
  + External trusts
  + Realm trusts

**One way and two-way trusts**

* One-way trust exists when one domain trusts another, but the reverse is not trust
  + When domain A trusts domain B, users may access resources in domain A but not vice versa
  + In this case domain A is the trusting domain and domain B is the trusted domain
* More common is the two-way trust, in which users from both domains can be given access to resources in the other domain

**Transitive trusts**

* A transitive trust is named after the transitive rule of equality in mathematics: if A=B and B=C, then A=C
* In order to authenticate a user, a referral must be made to a domain controller in each domain in the path to the destination. This can cause substantial delays.

**Shortcut trusts**

**Forest trusts**

* A forest trust provides a one-way or two-way transitive trust between forests that allows security principals in one forest to access resources in any domain in another forest
* Are not possible in Windows 2K forests
* They are transitive in the sense that all domains in one forest trust all domains in another forest, but the trust isn’t transitive from one forest to another

**External trusts**

* An external trust is a one-way or two-way non-transitive trust between two domains that aren’t in the same forest. Generally used in these circumstances:
  + To create a trust between two domains in different forests
  + To create a trust with a Windows 2K or Windows NT domain

Like a shortcut between two domains in different forests

**Realm trusts**

* Can be used to integrate users of other Oss into a Windows Server 2008 domain or forest
* This requires the OS to be running the Kerberos V5 authentication system that AD users
* Kerberos is an open-standard security protocol used to secure authentication and identification between parties in a network

External trust -> but for non-windows domains

**Understanding Sites**

* AD site represents a physical location where DCs are placed and group policies can be applied
* First DC of a forest creates a site named Default-Fire-Site-Name once installed
* Three main reasons for establishing multiple sites:
  + Authentication efficiency
  + Replication efficiency
  + Application efficiency
* Sites are created using Active Directory Sites and Services

Put DCs in sites

**Site components**

* Subnets
  + Each site is associated with one or more IP subnets, and a subnet can only be associated with a single site
* Site links
  + A site like is needed to connect two or more sites for replication purposes
  + Determine replication schedule and frequency between two sites
* Bridgehead Servers
  + Intersite replication occurs between bridgehead servers
  + One DC designated as the Inter-Site topology Generation (ISTG), which then designates a bridgehead server to handle replication for each directory partition