Adam Morgan 3/1/11 Chapter 3

The role of directory service: easy way to organize and find resources and administer them

**Windows Active Directory**

* Fire used by Windows 2000 Server
* Offers the following features:

1. Hierarchical organization
2. Centralized but distributed access
3. Scalability
4. Security
5. Flexibility
6. Policy-based administration

Overview of the AD Structure:

Physical: Location specific (Boston, NYC, Chicago, or Floor 1, Floor 2, etc)   
Logical: Business Structure (Marketing, sales)

**Active Directory’s Logical Structure**

* Organizational Units (OUs)
  + The Organizational Unit (OU) is an Active Directory container used to organize a network’s users and resources into logical administrative units  
      
    An OU contains Active Directory objects such as: Users, Groups, Computers, Printers, Shared Folders, Applications, Servers, DCs
* Domains
  + The core structural unit of an Active Directory; contains OUs and represents administrative, security, and policy boundaries  
      
    Small to medium companies usually have one domain; larger companies may have several domains to separate geographical regions or administrative responsibilities
* Trees
  + A grouping of domains that share a common naming structure  
      
    Can consist of a parent domain and possibly one or more child domains  
      
    Child domains can also have child domains
* Forests
  + A collection of one or more AD trees. A forest can consist of a single tree with a single domain, or it can contain several trees, each with a hierarchy of parent and child domains.  
      
    different namespace

**Domain Name Services Server**

* Maps IP address to a “friendly name” (FQDN)
* Sysvol folder = A shared folder that stores the information from AD that’s replicated to other domain controllers
* Directory Services Restore Mode is used to perform restore operations on AD if it becomes corrupted or parts of it are deleted accidentally

**The Active Directory Schema**

* ***Object* –** A grouping of information that describes a network resource, such as a shared printer, or an organizing structure, such as a domain or OU.
* ***Schema* –** Defines the type, organization, and structure of data stored in the Active Directory database and is shared by all domains in an Active Directory forest.
* ***Schema classes* –** The types of objects that can be stored in Active Directory, such as user or computer accounts (Category of items in a database)
* ***Scheme Attributes* –** Define what type of information is stored in each object, such as First name, Last name, and Password for a user account object.
* ***Attribute value* –** The information stored in each attribute

**Active Directory Container Objects**

**Organizational Units**

* Primary container object for organizing and managing resources in a domain
* OUs can organize multiple objects into one administrative group that can be configured with specific policies relevant to that group
* Authority of an OU can be delegated
* Nesting OUs can build a hierarchical Active Directory structure that mimics the corporate structure for easier object management

**Folder Objects**

**Four by default:**

1. *Builtin –* Houses default groups created by Windows
2. *Computers –* The default location for computer accounts created when a new computer or server becomes a domain member
3. *ForeignSecurityPrincipals –* Initially empty but later contains user accounts from other domains added as members of the local domain’s groups
4. *Users –* Stores two default users (Administrator and Guest) and several default groups

* New folder objects cannot be created
* Administrative control can be delegated (except on builtin folder)

**Domain Objects**

* Core logical structure in AD, contains OU and folder container objects, as well as leaf objects
* Larger companies may use multiple domains to separate administration, define security boundaries, and define policy boundaries
* Each domain object has a default GPO linked to it that can affect all objects in the domain

**Active Directory Leaf Objects**

**User Accounts**

* Three Types: Local, domain, and built-in

**Shared Folder**

* ***Authentication*** *– Confirms a user’s identity, and the account is then assigned permissions and rights that authorize the user to access resources and perform certain tasks on the computer or domain*
* ***Local User Account*** *– Defined on a local computer and is used on stand-alone computers or in a workgroup network with computers that aren’t part of an Active Directory domain.*
* ***Domain user account –*** Created in Active Directory and provides a single logon for users to access all resources in the domain for which they have been authorized.
* ***Built-in user accounts -***

**Groups**

* Consists of users with common permissions

***Permissions*** *–*

***Right -***

**Computer Accounts**

* Represents a computer that is a domain controller or domain member

**Other Leaf Objects**

* *Contact –*
* *Printer –*
* *Shared folder –*

**Locating Active Directory Objects**

Active Directory objects can be searched for using the Find Users, Contacts and Groups dialog box

Can search a single domain or an entire directory (all domains)

Not all objects are available to all users

**Introducing Group Policies**

Group Policy Object (GPO): A list of settings that administrators use to configure user and computer operating environments remotely.

Install Active Directory creates two GPO’s by default:

Default Domain Policy  
Default Domain Controllers Policy

You can edit existing GPO’s (including defaults) and create and manage GPO’s by using the Group Policy Management MMC (gpmc.msc)

Two notes for every GPO:

Computer Configuration: Used to set policies that apple to computers within the GPO’s scope  
User Configuration: Used to set policies that apply to all users within the GPO’s scope

**The Computer Configuration Node**

Software Settings

Enables Administrators to install and manage applications remotely (not user profile specific)

Windows Settings

Contains Scripts extension, Security Settings node, and the Policy-based QoS node

Administrative Templates

Contains the Control Panel, Network, Printers, System, and Windows Components folder.

**The User Configuration Node**

Policies folder contains the same three folders as in the Computer Configuration note, but policies defined her affect domain users within the GPO’s scope, regardless of which computer the user logs on to.

Software Settings

Can assign or publish application packages

Windows Settings – Contains six items

Remote Installation Services

Scripts extension

Security Settings node

Folder Redirection node

Policy based QoS node

Internet Explorer Maintenance node

Administrative templates