Adam Morgan 4/20/11 Outline

**Windows File Systems**

* A file system defines the method and format that an OS users to store, locate, and retrieve files from electronic storage media
* Modern file systems are composed of some or all of the following components:
  + Filenaming convention – Rules for naming files
  + Hierarchical Organization – C:\Program Files\Adobe
  + Date storage method
  + Metadata – Other info date/time
  + Attributes
  + Access control lists (ACLs)

**The FAT File System**

* FAT (File Allocation Table) consists of two variations: FAT16 & FAT32
* FAT16 is limited to 2GB partitions (Windows NT extends to 4GB) with a maximum file size of 2GB
* FAT32 allows partitions up to 2TB in size, but Windows 2000 and later limit size of FAT32 partitions at creation to 32GB due to performance.
* FAT32 supports files up to 4GB in size

**The NTFS File System**

* First introduced in Windows NT
* Supports File and folder permissions, an advantage over FAT
* Features added with the release of Windows 2000:
  + Disk quotas – Max space
  + Volume mount points
  + Shadow copies
  + File compression
  + Encrypting File System (EFS)

**Disk Quotas**

* Disk quotas: Help administrators control how disk space is used on a server
* Options for setting quotas:
  + Enable quota management
  + Deny disk space to users exceeding quota limit
  + Do not limit disk usage
  + Limit disk space to
  + Log event when a user exceeds their quota limit
  + Log even when a user exceeds their warning level
  + Quota Entries

**Volume Mount Points**

* Volume Mont Points: Enable you to access a volume as a folder in another volume instead of by using a drive letter
* Volume holding the folder to serve as the mount point must be NTFS
* Reasons for using:
  + Extend the apparent amount of free space on existing volume
  + Consolidate frequently accessed volumes
  + Consolidate several shared volumes under a single network share

**Shadow Copies**

* Shadow Copies: Allows access to previous versions of files, and the ability to restore files that were deleted or corrupted
* Upon enabling shadow copies, Windows will warn that default settings are not ideal for heavily used servers
* Can be configured in the Settings dialog box for Shadow Copies:
  + Located on this volume
  + Details
  + Maximum size
  + Schedule

**File Compression and Encryption**

* File encryption on NTFS made possible by **Encrypting File System [EFS]**
* Can be set on a file or a folder, but not an entire volume
* Rules for encryption behavior:
* Encrypted files that are copied or move always stay encrypted, regardless of the destination’s encryption attribute
* Unencrypted files that are moved or copied to a folder with the encryption attribute set are always encrypted
* The user who initially encrypted the file can add additional users who can decrypt it. However, a user must have a valid EFS certificate in order to be added

**Securing Access to Files with Permissions**

* Two ways to secure files
  + Share Permissions
  + NTFS Permissions
* Share permissions apply when using a network to access shared files, while NTFS permissions apply whether accessing network shares or local files
* If accessing a network share, the effective permissions will always be the most restrictive permissions between Shared and NTFS permissions

**Share permissions**

* Share permissions apply to folders and files accessed across the network
* Three share permissions:
  + Read
  + Change
  + Full Control
* Generally, the default share permissions is Read for Everyone

**NTFS Permissions**

* NTFS permissions can be configured on folders and files
* 6 permissions and 14 special permissions for folders
* 5 permissions and 13 special permissions for files
* NTFS standard permissions:
  + Read
  + Read & Execute
  + List folder contents
  + Write
  + Modify
  + Full control

**File and Folder Ownership**

* Owner of an object is granted certain implicit permissions
* A user can become the owner of a file system object in three ways:
  + Create the file or folder
  + Take ownership of a file or folder
  + Assigned ownership