# File systems security:
## Shared folders & NTFS permissions, EFS
## Disk Quotas

(March 23, 2016)

© Abdou Illia, Spring 2016


## Learning Objective

- Understand
  - Shared Folders
- Assign
  - Shared Folder permissions
  - NTFS Permissions
- Understand EFS
- Understand Disk Quotas



## FAT vs. NTFS

- Decision about what file system to use depends on:
  - Whether multiple OS will be installed on the computer
  - Security requirements for the system

| FAT |
|---|
| Supports partitions up to 4 GB (FAT16) and 2 TB (FAT32) |
| Provides only folder-level security |
| Allows limited permission setting (Read, Change, Full Control) |

| NTFS |
|---|
| Supports lager partitions size than FAT (w/o disk performance decrease) |
| File-level and Folder-level security |
| Data compression |
| File encryption (Encrypting File System) |
| Disk quotas management |
| Needed for AD services |
| Faster access to data |
| Remote storage: provides an extension to your disk space by making removable media (such as tapes) more accessible. |

**Note:** Windows and MS-DOS-based applications can read compressed files because they are automatically decompressed by NTFS when requested.

## Shared Folder ?


- A folder used to provide network users with access to file resources.
- When a folder is shared on a server, users can connect to the server and gain access to the files it contains.

4

## Shared Folders

- Requirements for creating a shared folder:
  - Any supported File system (FAT, NTFS)
  - If server in a domain, you must be Administrator or Server Operator
  - If server in a workgroup, you must be Administrator or Power user
  - If client computer running a workstation OS, you must be Administrator or Power user

**Note:** Users that are granted the Create Permanent Shared Objects right can also create shared folders on the computer where the right is assigned

To see all shared folders on a computer:

1) Click **Start**. Then click **Run**
2) Type **\\ComputerName** (where ComputerName is a valid network computer name like SRVDC18)
3) Click **OK.**

**OR**

1) Open Computer Management
2) In the console tree, double-click **Shared Folders**
3) Click **Shares**

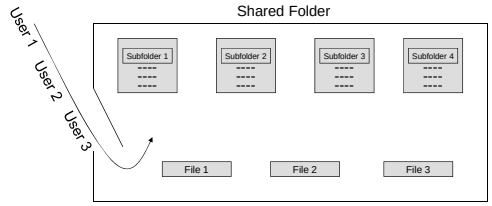
To share a folder on a computer:

1) Open **My Computer** (Right-click/Open)
2) Select a disk, then the folder to share
3) Right-click the selected folder
4) Click **Properties**
5) Click the **Sharing** tab
6) Check **Share this folder**
7) Click **Apply**, and then **OK.**

5

## Shared folder permissions

- A shared folder can contain application programs, data or other users' personnel data
- Each type of data can require different permissions




- With FAT, permissions could only be set for folders, not for individual files
- If permissions at file level are required, you need to use NTFS permissions

6

## Shared Folder Permissions

| | |
|---|---|
| **Read** | - Display folder names, filenames, file data and attributes<br>- Run program files |
| **Change** | **Read** permission +<br>- Create folders, add files to folders, change data in files, append data to files, change files attributes, delete folders and files. |
| **Full Control** | **Change** permission +<br>- Change file permissions and take ownership of files |

- Shared folder permissions do not restrict access to users who gain access to the folder at the computer where the folder is stored.
- Shared folder permissions are the only way to secure network resources on FAT partitions.
- The default folder permission is Read for Everyone.
- You can allow or deny shared folder permissions to individual users or to user groups.

7

## Assigning Shared Folders permissions

1) Open **My Computer** (Right-click/Open)
2) Select the disk, then the folder
3) Right-click the selected folder
4) Click **Properties**
5) Click the **Sharing** tab
6) Click **Permissions**
7) Assign permissions
8) Click **OK**, and then **OK.**

8

## Shared Folder Permissions' Rules

- **Multiple Permissions (The Combination Rule)**
  - **If** a user is assigned a permission for a Shared folder **and**
  - **If** the use user belongs to a group to which a different permission is assigned,
  - **Then** the user's effective permissions are the combination of the user and group permissions
- **Deny overrides Allow**
  - **If** you deny a shared folder permission to a user **and**
  - **If** you allow the same permission to a group the user belongs to
  - **Then** the user will not have that permission.
- **Copying or Moving Shared folders**
  - **If** you copy a Shared folder, the original folder is shared but not the copy
  - **If** you move a Shared folder, it is no longer shared.

9

## Guidelines for Shared Folder Permissions

- Determine which groups need access to each resource and the level of access they require.
- Assign permissions to groups instead of user accounts to simplify access administration.
- Assign the most restrictive permissions that still allow users to perform required tasks.
- Use intuitive share names so that users can easily recognize and locate resources.

10

## Administrative & Hidden shares

- Administrative shares (created by default):
  - All hard drives are shared as C$, D$, etc.
  - The system folder (\WINDOWS) is shared as Admin$
  - Driver's folder for printers (\Winnt\System32\Spool\Drivers) is shared as Print$
- Hidden shares (created by users)
  - Share name should end with $ for the share to be hidden
  - Not visible by other users unless they know the name
  - If a user knows the name of a hidden share, he/she can access the share using the UNC name
    - Start/Run. Then type \\ComputerName\ShareName$

Universal Naming Convention (UNC) name

11

## NTFS permissions

- **If** permissions at file level are required, **and/or**
- **If** more specific permissions are required
  - **Then**, NTFS permissions must be used

**Assigning NTFS permissions**

1) Open **My Computer** (Right-click/Open)
2) Select the disk, then the folder/file to share
3) Right-click the selected folder or file
4) Click **Properties**
5) Click the **Security** tab
6) Assign permissions
7) Click **Apply**, and then **OK.**

12

## Standard NTFS permissions

| | |
|---|---|
| Read | User can open and view content of files/folders. They can also view objects ownership, assigned permissions, and objects attributes (Read-Only, Hidden, etc.) |
| Write | Read permission +<br>- Create new files/subfolders in a folder<br>- Change attributes |
| List Folder Contents | Can only view names of folders/files |
| Read and Execute | Read and List Folder Content permissions +<br>- Ability for users to navigate through folders for which they don't have permission in order to get files and subfolders for which they do have permissions. |
| Modify | Read + Write + Read and Execute permissions (Users can view, create, delete, modify content of folders, etc.) |
| Full Control | Users can do everything |

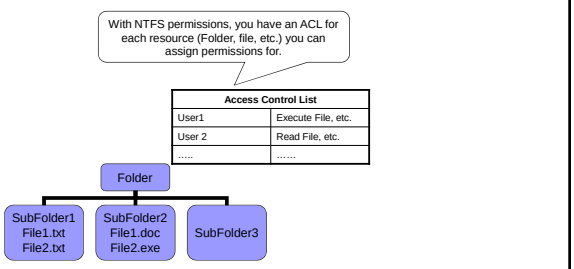
13

## Extended NTFS permissions

Execute File
List Folder / Read File
Read Attributes
Read Extended Attributes
Create Files / Write Data
Write Attributes
Write Extended Attributes
Delete Subfolders and Files
Read Permissions
Change Permissions
Take Ownership

14

## NTFS permissions




15

## NTFS Permissions' Rules

- **Multiple Permissions**
  - NTFS file permissions take priority over NTFS folder permissions
    - A user can always access files for which he/she has permissions using UNC. E.g. \\SRVDC16\Data\file1.txt
  - Denying a permission for a user blocks that permission, even if the permission is granted to a group the user belongs to.
- **Permission Inheritance**
  - By default, permissions assigned for the parent folder are inherited at subfolder and file level
  - To prevent automatic inheritance, explicit permissions assignments must be done at subfolder and/or file levels.
- **Copying or Moving Files and Folders**

Golden rule:
- When a file/folder is copied or moved to another NTFS partition on a different physical disk, it inherits the permissions & attributes from the destination folder

Exception to Golden rule:
- When a file/folder is moved within an NTFS partition, it retains its permissions
- When a file/folder is moved to another NTFS partition on the same physical disk it retains its permissions
- When a file/folder is copied to a FAT partition, it loses its NTFS permissions

16

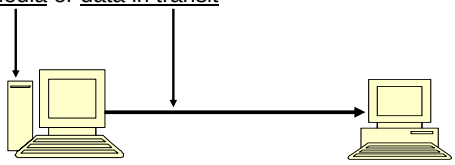
## Shares & permissions: Recap

| | Sharing folders/files | | Setting permissions | |
|---|---|---|---|---|
| | FAT | NTFS | FAT | NTFS |
| Folders/Subfolders | YES | YES | YES (but limited) | YES |
| Files | NO | NO | NO | YES |

17

## Encrypting File System

- EFS is used to encrypt data in order to prevent intruders to read.
- The Golden rule do not apply to encrypted files/folders
- EFS is used to encrypt data stored on storage media or data in transit



18

## Why use EFS?

- With NTFS permission, if someone is given the Take Ownership permission on your file/folder, they can log on, take the ownership of the file/folder, and then change permissions the way they want to.
- With EFS, in addition to access rights, a de-encryption key is needed to read a file*.
- If someone got a copy of your file, or took ownership of it, they cannot read its content.

Note 1: * When you logon, a private de-encryption key is automatically issued to you by W2003
Note 2: Only the file/folder's creator or the Recovery Agent (the Administrator) can decrypt the file/folder

19

## How to encrypt a folder

1. Right-click the folder you want to encrypt
2. Click **Properties**
3. In General tab, click the **Advanced** button

Note 1: The command line **cipher** could also be used to encrypt
Note 2: Golden rule doesn't apply to encrypted files/folders

20

## Exercise

- Create a user account for yourself with the username last (where last is your last name)
- Log off as Administrator, and logon using the last user account you have created
- Create a folder called Lab3-XX (where XX is your computer number) directly under the root of the C: drive.
- Encrypt the Lab3-XX folder
- Answer the following questions
  - If you copy the encrypted folder to another NTFS partition, it will loose it encryption properties.
    T F
  - Another user logon to your network. That user can read your encrypted file only if he/she took ownership of your encrypted file, and changed the permissions.
    T F

21

## Disk Quotas

- Disk Quotas needed because
  - Many users save data on shared folders
  - Users must be prevented from filling disk capacity
- Disk Quotas options
  - Enable Disk quotas w/o limiting disk usage
  - Set a default quota for all users (per-volume basis)
  - Set quotas on per-user basis

**Note:** Disk Quotas only available on NTFS partitions

22

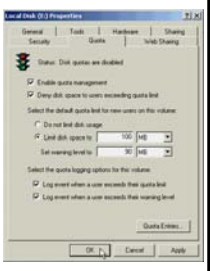
## Enable/Configure Disk Quotas

1) Open My Computer
2) Right-click the volume, and click Properties
3) Click Quota tab
4) Enable quotas management
5) Configure Disk quotas

23

## Disk Quota Parameters

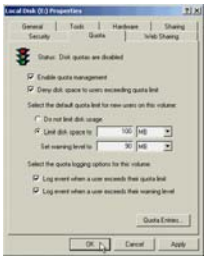
- *Enable quota management:* Sets up quota management and starts tracking disk usage
- *Deny disk space to users exceeding quota limits:* Users can't write new information after reaching their quotas
- *Do not limit disk usage:* Tracks disk usage without imposing quotas
- *Limit disk space to:* Sets the default amount of disk space for all users



24

## Disk Quota Parameters (continued)

- *Set warning level to:* Sets the default disk space that users can occupy that will trigger a warning message
- *Log event when a user exceeds their quota limit:* An event is entered in the System log when a user reaches his or her quota
- *Log event when the user exceeds the warning level:* An event is entered in the System log when a user receives a warning that he or she is approaching the quota



25

## Delete a Quota entry

1) Open My Computer
2) Right-click the volume, and click Properties
3) Click Quota tab
4) Click the Quota Entries button
5) Right-click the appropriate user account
6) Click Delete

26

## Other slides:

- Configuring Auditing
- Taking ownership

27

## Configuring Auditing

- Auditing allows to keep track of events like Write, Create, Delete, Append, etc. on folders/files
- Need to implement auditing on folders and files that involve sensitive information (accounting, payroll, research projects, etc.)

28

## Configuring Auditing

1) Right-click the folder/file you want to audit
2) Click **Properties**
3) Click **Security** tab
4) Click **Advanced** button
5) Click **Auditing** tab in the **Access Control Settings** dialog box, and click **Add**
6) Double-click the group or user you want to audit
7) Check the Successful or Failed events to audit
8) Click OK as many times as needed.

29

## Taking ownership

**Note:** If you are the owner of a folder/file (or have the **Take ownership** permission), you can change other users' permissions

1) Right-click the folder/file you want to take ownership
2) Click **Properties**
3) Click **Security** tab
4) Click **Advanced** button
5) Click **Owner** tab in the **Access Control Settings** dialog box, and click **Add**
6) Change the ownership
7) Click OK as many times as needed.

30

## Disk Quotas: Summary Questions

1) The Computer Planning Committee at your company is working to project Windows Server 2003 disk capacity needs for the next two years, as part of the computer equipment budgeting process. Because you are part of the committee, they asked you if there is any way to gather statistics on present disk use over a three-month period to help in making projections. How can you obtain the statistics that they want?
   a) Turn on disk auditing for each user's account, and compile the audit report
   b) Set the default disk quota to a low number, and gather statistics based on the resulting reports that users are out of disk space
   c) Enable disk quotas, and after three months copy the disk quotas statistics into a file (e.g. spreadsheet or word processor file)
   d) There is no easy way to gather statistics except to ask all employees to calculate the space they use.

31

## Disk Quotas: Summary Questions

2) The management in your organization wants to limit all employees to 7 MB of disk space, on each volume, which they can use to store files in shared folders and in home folders. What is the best way you can accomplish this?
   a) Set up a default disk quota of 7 MB on each shared volume.
   b) Set up a disk quota for each user via the Active Directory.
   c) Set up a default disk quota of 7 MB for each user account on each volume.
3) Sara and Richard each have a disk quota of 2 MB. Recently Sara has taken ownership of an 800 KB database file previously owned by Richard. How does this action affect their disk quotas?
   a) When ownership of a file is transferred, that file is exempt from the disk quota allotment.
   b) The disk quotas of Sara and Richard are unchanged.
   c) Sara's disk quota is now 2.8 MB, but Richard/'s stays the same.
   d) Sara has 800 KB less space out of the 2 MB quota, and Richard has 800 KB more.

32

## Disk Quotas: Summary Questions

4) The lead research scientist in your company needs to work over the weekend to prepare information for a lecture he is presenting on Monday. He does not know how close he is to reaching his disk quota and is calling you to find out. How can you determine where he stands?
   a) There is no way to determine where he stands, but you can increase her quota to make sure there is no problem.
   b) Check the Quota Entries dialog box in the properties of the shared disk volume that he uses.
   c) Open the Command prompt window and use the Quota command along with his account name to find out.

33