Diploma in Infocomm & Security

IT2654: Systems Administration & Security

TOPIC 6: MANAGING FILE ACCESS

Objectives

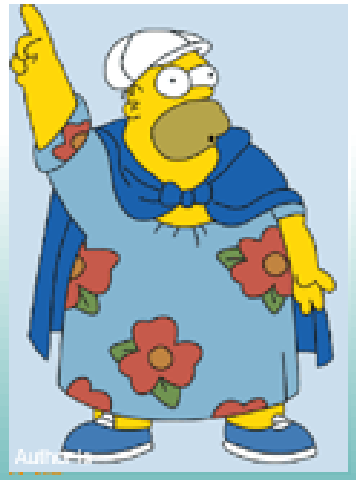
- Windows Server file systems
- Shared folders
- File system permissions
  - NTFS permissions
  - Shared permissions
  - Effective permissions
  - Combining shared and NTFS permissions

Windows Server File Systems

- Four main file systems
  1. File Allocation Table (FAT)
  2. FAT32
  3. NTFS
  4. ReFS
- Final choice of file system depends on
  - How system will be used
  - Whether there are multiple operating systems
  - Security requirements
- NTFS is mandatory for Windows Server 2016

FAT

- Used by MS-DOS
- Supported by all versions of Windows since
- Windows Server version supports partitions up to 4 GB
- Limitations
  - Small partition sizes
  - No file system security features
  - Disk space usage is poor
- Max file size 2 GB



FAT32

- A derivative of the FAT file system
- Supports partition sizes up to 8TB.
- Max file size of 4 GB
- Still does not provide advanced security features
  - Cannot configure permissions on file and folder resources

NTFS

- Introduced with Windows NT operating system
- Max file size – see below
- Advantages:
  - Greater scalability and performance on larger partitions
  - Multiple user permissions – files & folders (ACL)
  - Built-in support for compression and encryption
  - Ability to configure disk quotas for individual users
  - Hard links, Journaling, Self-healing, Indexing

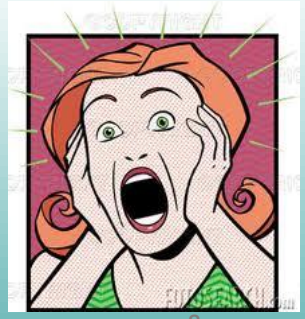
Cluster size	Largest volume	Largest file
4 KB (default size)	16 TB	16 TB
8 KB	32 TB	32 TB
16 KB	64 TB	64 TB
32 KB	128 TB	128 TB
64 KB (maximum size)	256 TB	256 TB

Converting a FAT Partition to NTFS

- For highest security, partitions and volumes should be configured to use NTFS
- Command-line utility, CONVERT, will convert FAT or FAT32 partitions and volumes to NTFS
- All existing files and folders are retained
- CONVERT cannot convert NTFS to FAT or FAT32
- convert *d:* /fs:ntfs
  - Where *d* is the drive letter you want to convert.
  - If you convert system volume, you must restart

ReFs (Refined File System)

- Introduced in Windows Server 2012
- Offers unlimited file and directory sizes
- Increased resiliency and eliminates need for error checking
  - it can auto detect data corruption and perform repair without taking the volume offline
- Does not support some NTFS features
- Cannot be used by systems older than Windows Server 2012 and Windows 8



ReFS vs NTFS

NTFS

```
C:\>fsutil fsinfo volumeinfo f:
Volume Name : DATA
Volume Serial Number : 0xcaf17d11
Max Component Length : 255
File System Name : NTFS
Is ReadWrite
Supports Case-sensitive filenames
Preserves Case of filenames
Supports Unicode in filenames
Preserves & Enforces ACL's
Supports file-based Compression
Supports Disk Quotas
Supports Sparse files
Supports Reparse Points
Supports Object Identifiers
Supports Encrypted File System
Supports Named Streams
Supports Transactions
Supports Hard Links
Supports Extended Attributes
Supports Open By FileID
Supports USN Journal
```

ReFS

```
C:\>fsutil fsinfo volumeinfo i:
Volume Name : REFSVOL01
Volume Serial Number : 0x90806ed1
Max Component Length : 255
File System Name : ReFS
Is ReadWrite
Supports Case-sensitive filenames
Preserves Case of filenames
Supports Unicode in filenames
Preserves & Enforces ACL's
Supports Sparse files
Supports Reparse Points
Supports Open By FileID
Supports USN Journal
```

Setting Up Shared Folders

- Shared folder
  - A data resource made available over a network to authorized network clients
  - Specific permissions required for creating, reading, modifying
- Groups that can create shared folders:
  - Administrators
  - Server Operators
  - Power Users (only on member servers)

Configuring Shared Folders and Shared Folder Permissions

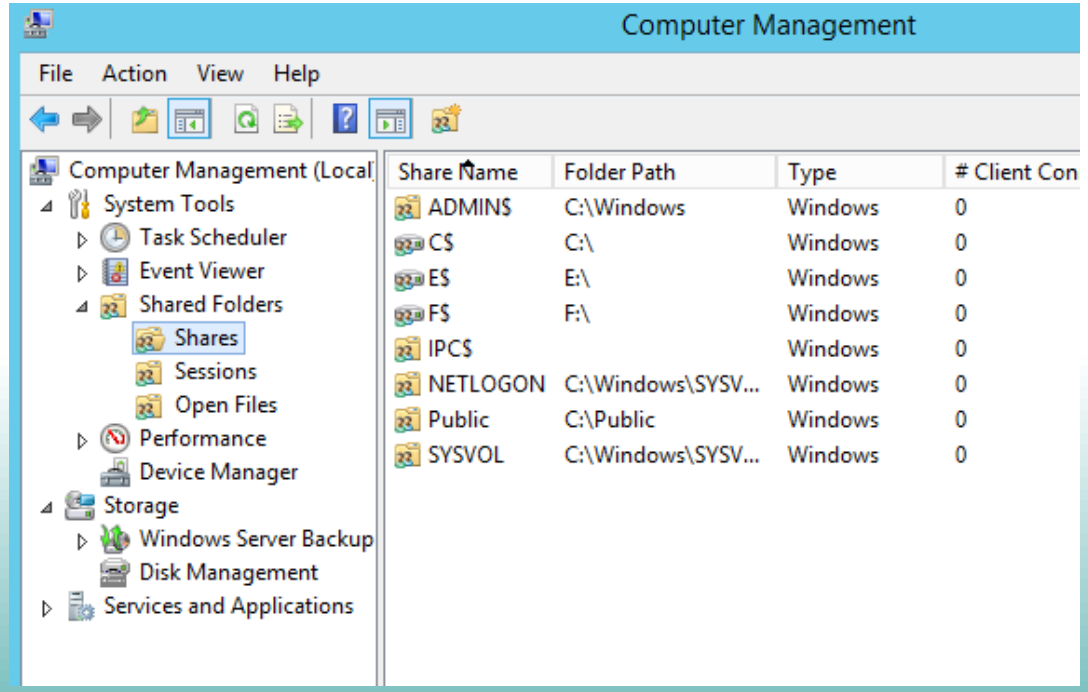
- The first step for sharing a folder over the network is to turn on file sharing
- Several ways to create shared folders
- Two important methods
  - Windows Explorer Interface
  - Computer Management console
    - Also allows shared folders to be monitored

Using Windows/File Explorer

- Can create, maintain, and share folders
- Folders can be on any drive connected to the computer
- Folders are shared in Windows Explorer by accessing the Sharing tab of folder's properties
- Shared folders can be hidden from My Network Places and Network Neighborhood
  - Place dollar sign ($) after name, e.g., Salary$
  - Number of hidden administrative shares created automatically at installation

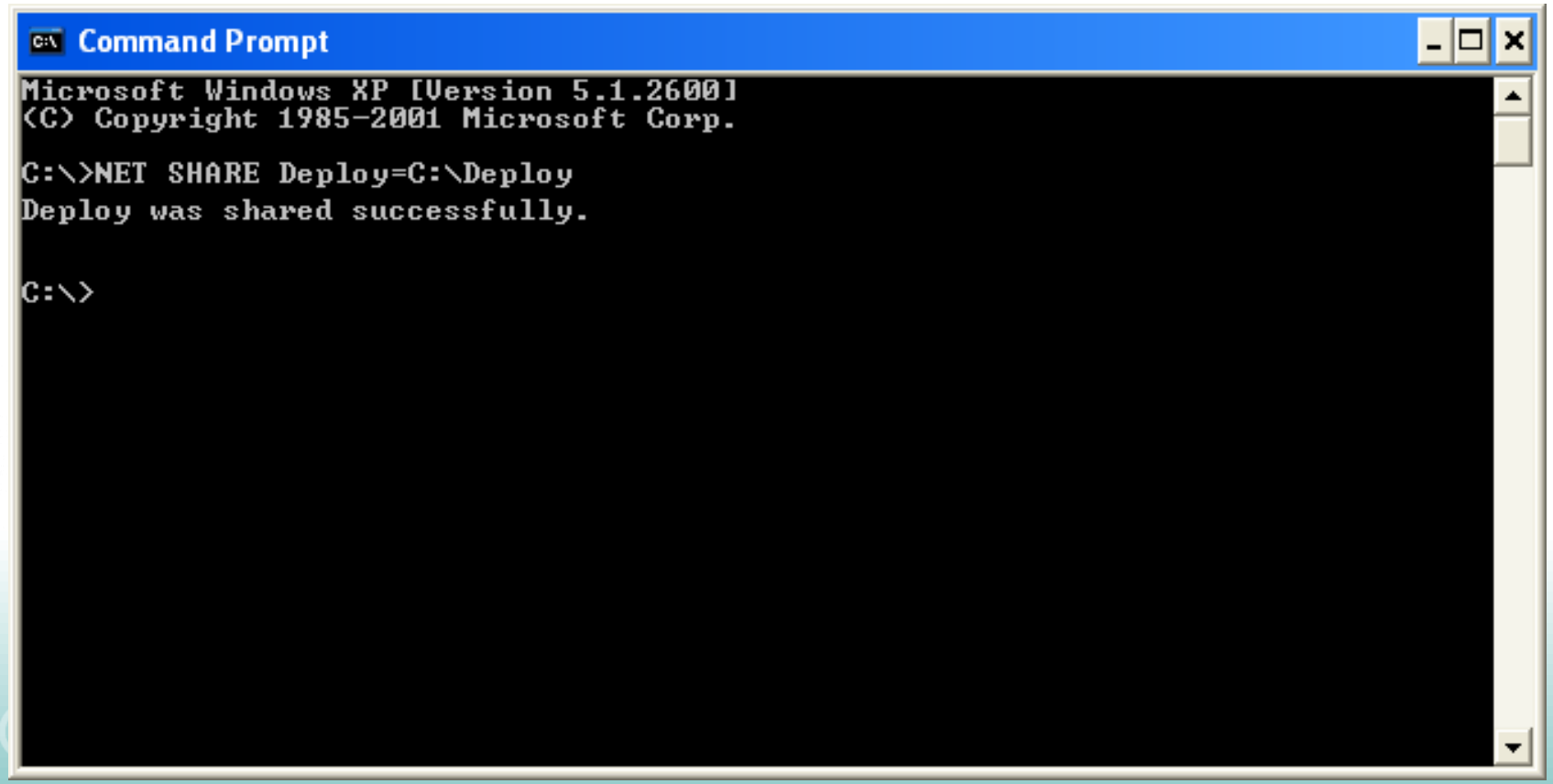
Administrative Shares

- Root of each volume is shared automatically as C$, D$, E$ etc.
  - Allows full control by Administrator
- C:\Windows is shared as ADMIN$
  - Required for remote administration



Sharing Folders - Command Line

- *NET SHARE*



Copy / Move a Shared Folders

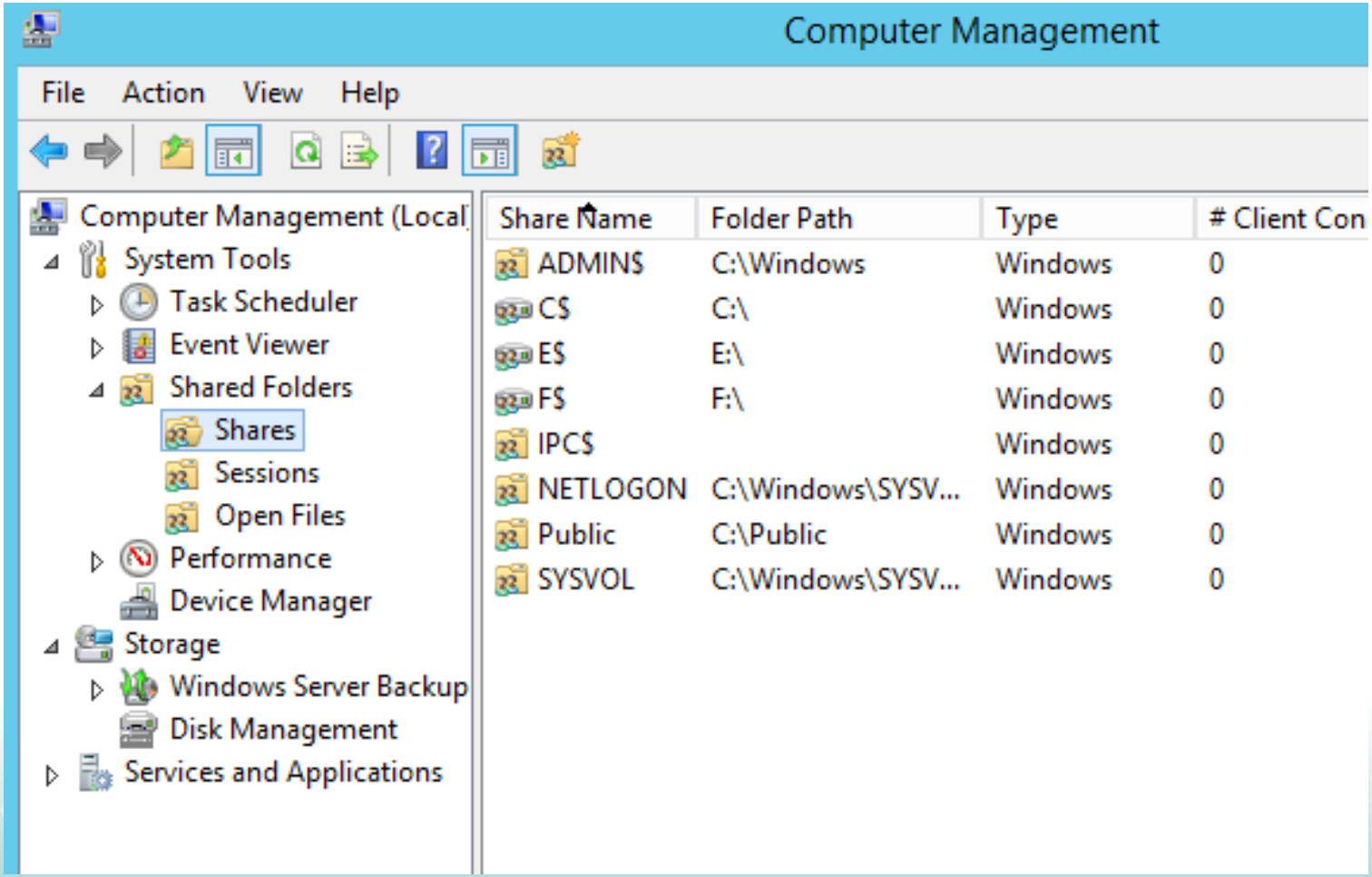
- Copy a shared folder
  - The original shared folder is still shared, but the copy of the folder is not shared
- Move or rename a shared folder
  - The folder is no longer shared

Monitoring Access to Shared Folders

- Monitoring involves
  - Who is using shared files
  - What shared files are open at any given time
- Other functions
  - Disconnect users from a share
  - Send network alert messages*
- Primary monitoring tool is Computer Management

*msg /SERVER:[PCNAME] [USERNAME] [TEXT]

Monitoring Shared Folders (Continue)

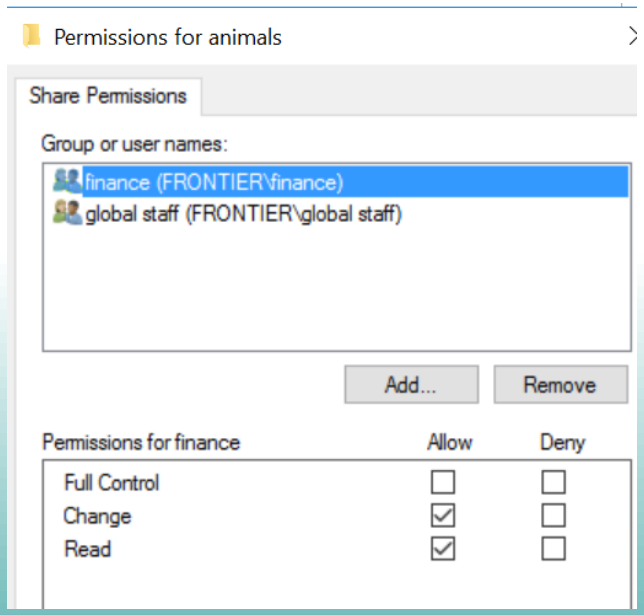


Managing Folder and File Security

- Creating accounts and groups are the initial steps for sharing resources
  - The next steps are to create access control lists (ACLs) to secure these objects and then to set them up for sharing
- **Discretionary ACL (DACL)**
  - An ACL that is configured by a server administrator or owner of an object
- **System control ACL (SACL)**
  - Contains information used to audit the access to an object

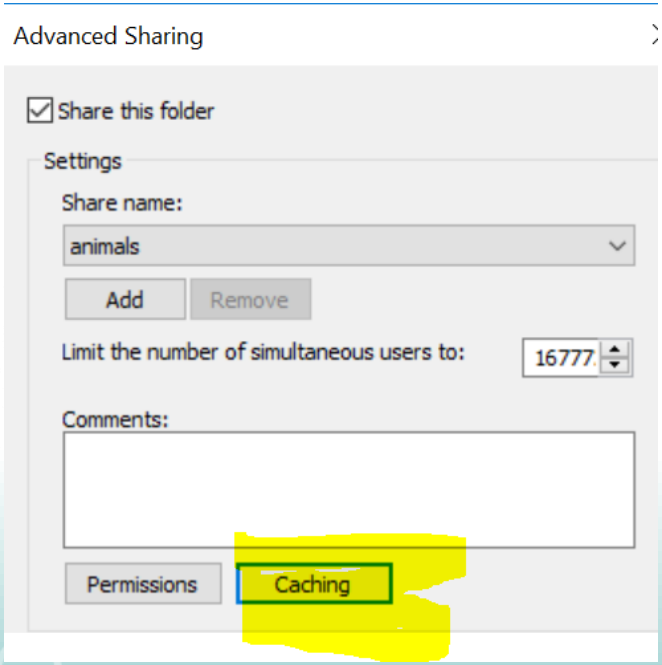
Configuring Shared Folders and Shared Folder Permissions (continued)

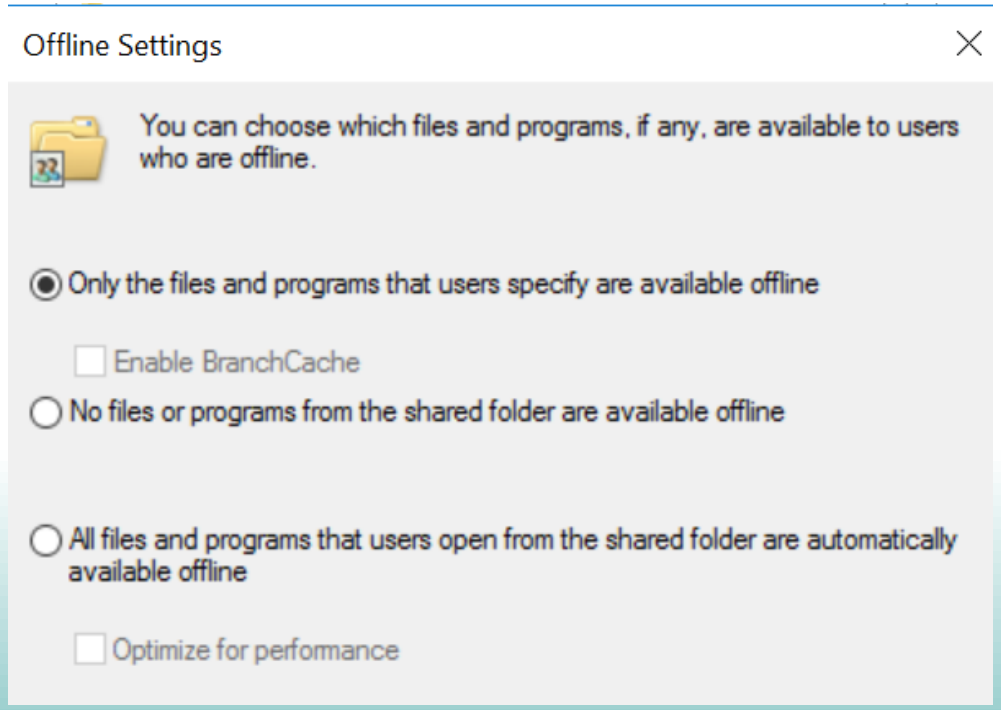
- Shared permissions are cumulative
  - Deny permissions override all
- Share permissions:
  1) Full Control
  2) Change (Read/Write)
  3) Read



Configuring Share - Offline Settings

- You can cache a folder to make the contents of a shared folder available offline





STOP Sharing Folders

- Computer Management: choose Stop Sharing from shortcut menu
- Windows Explorer: select Do Not Share This Folder
- NET SHARE: *NET SHARE <sharename> /DELETE*

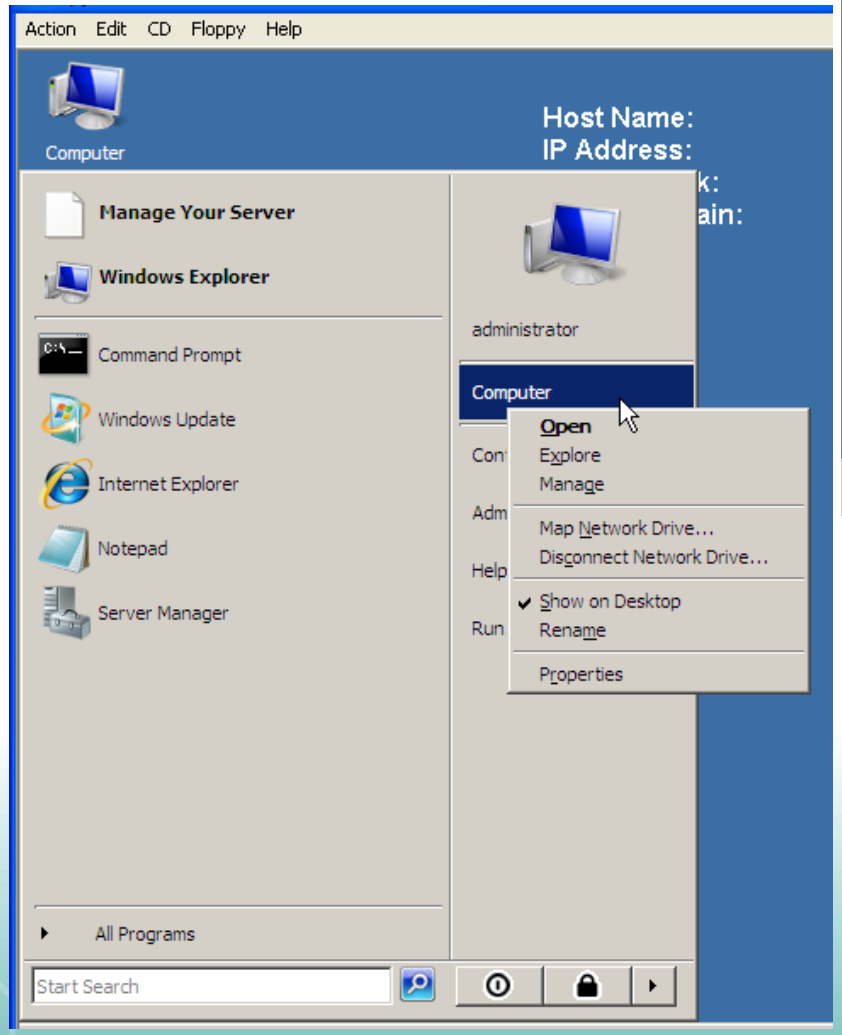
How to Connect to Shared Folders

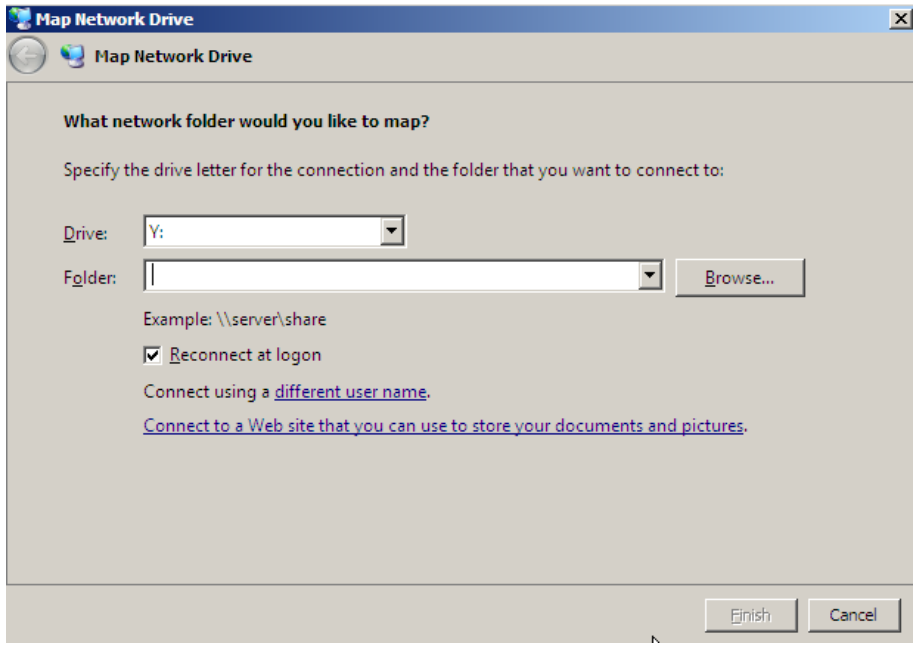
- My Network Places
- Mapped drives (Windows Explorer)
- Mapped drives (*NET USE*)
- Run dialog box

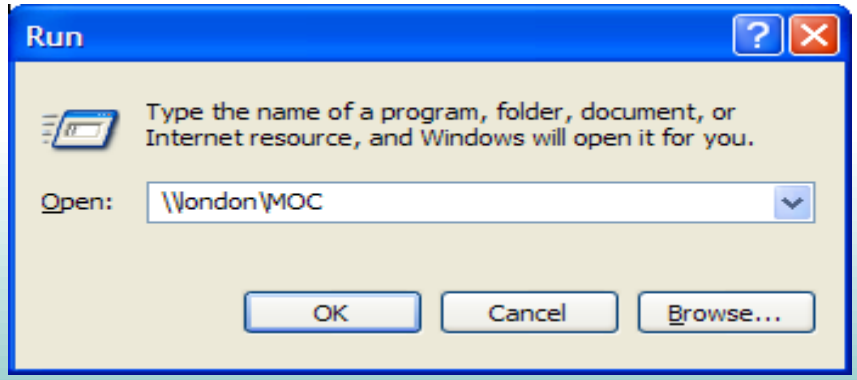
UNC Paths

\\servername\sharename\subfolder

Connecting to Shared Folders (demo)

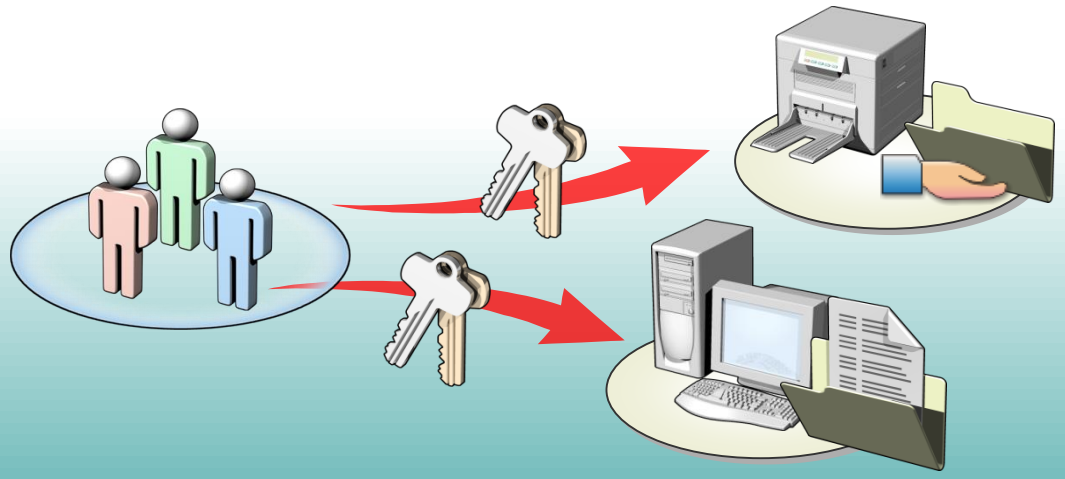






Configuring File System Permissions

- Permissions define the type of access granted to a user, group, or computer for an object
- You apply permissions to objects such as files, folders, shared folders, and printers
- You assign permissions to users and groups in Active Directory or on a local computer



NTFS Permission

- Only NTFS format has this permission.
- NTFS permissions are configured via the Security tab
- NTFS permissions are cumulative
- Access denial always overrides permitted access
- NTFS folder permissions are inherited unless otherwise specified
- NTFS permissions can be set at file or folder level
- A new ACE (Access Control Entry) has default permission
  - Read and (Read and Execute) for files
  - List Folder Contents for folders

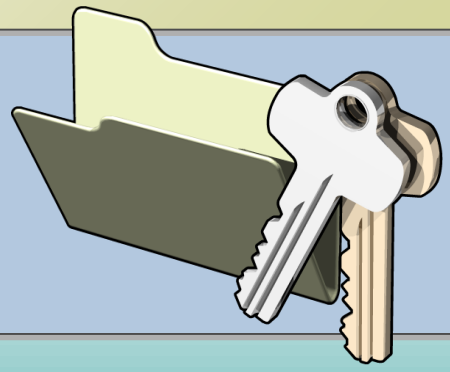
NTFS File and Folder Permissions

File permissions

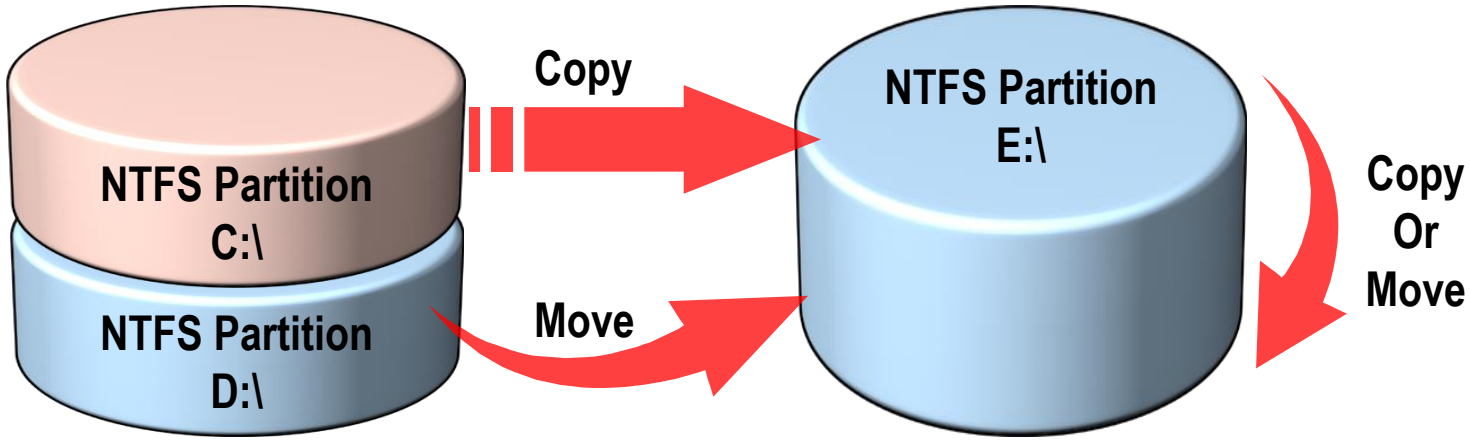
- Full Control
- Modify
- Read & Execute
- Write
- Read

Folder permissions

- Full Control
- Modify
- Read & Execute
- Write
- Read
- List Folder Contents



Effects on NTFS Permissions When Copying and Moving Files and Folders



- When you copy files and folders, they inherit permissions of the destination folder
- When you move files and folders within the same partition, they retain their permissions
- When you move files and folders to a different partition, they inherit the permissions of the destination folder

Determining Effective Permissions

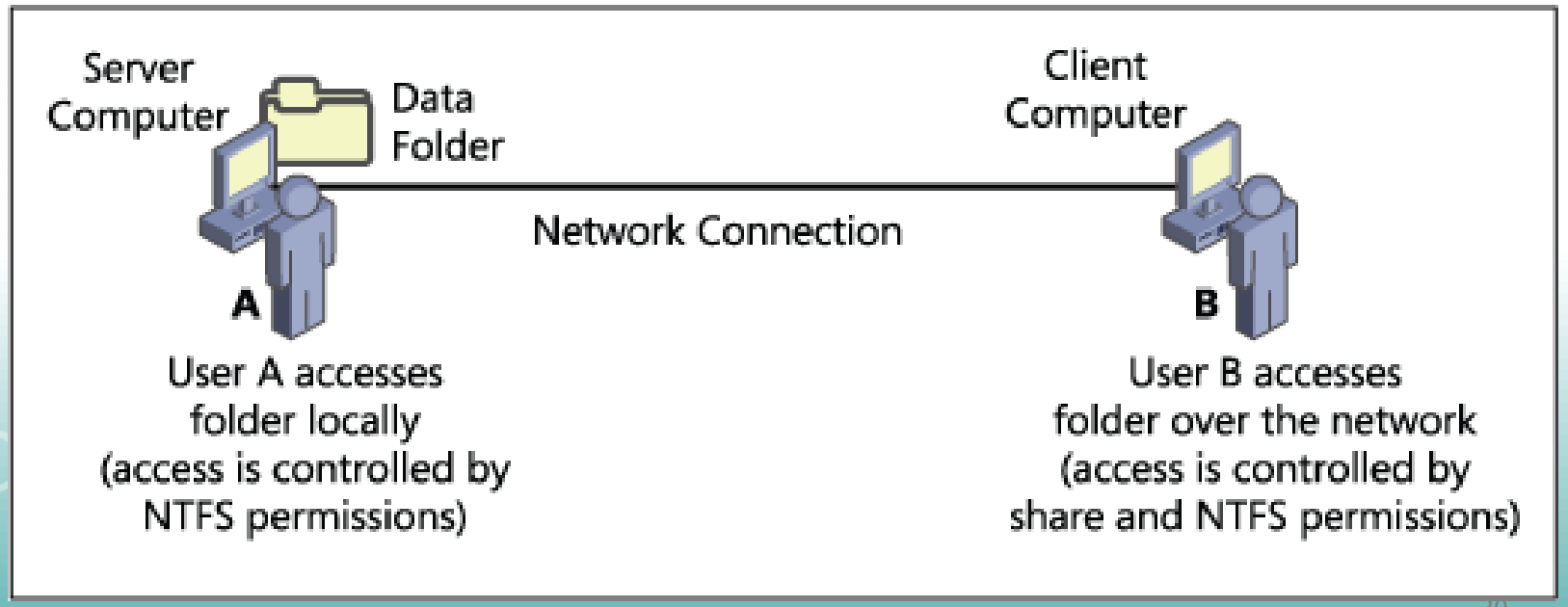
- Permissions are cumulative – Permissions that actually apply to a user can be the result of membership in multiple groups
- Prior to Windows Server 2008, determining effective permissions was done manually
- In latest Windows Server, there is an Effective Permissions tab in Advanced Security Settings dialog box for resource
  - Shows specific permissions for a user or group

Effective Permission Rules

- File permissions override folder permissions
- Allow permissions are cumulative.
- Deny permissions take precedence over Allow permissions
- Explicit permissions take precedence over inherited permissions

Combining Shared Folder and NTFS Permissions (!!!)

- NTFS permissions can be combined with share permissions
  - When accessing a share across a network, if both apply, use **MOST RESTRICTIVE**
  - When accessing a file **LOCALLY**, only NTFS permissions apply



Best Practices for Managing Access to Files and Folders Using NTFS Permissions

- Grant permissions to domain local groups as opposed to users
- Group resources to simplify administration
- Allow users only the level of access that they require
- Grant Read & Execute permission for application folders
- Grant Read & Execute and Write permissions for data folders

Summary

- Windows Server supports 4 file systems:
  FAT, FAT32, NTFS, ReFS
- How to create share & connect to it.
  - Tools are Windows Explorer, Computer Management, and NET SHARE command
- Permissions
  - Shared permissions
  - NTFS permissions
  - Shared and NTFS permissions are combined resulting in most restrictive over network access
  - Only NTFS permissions applied for local access