



Chapter 6: Network Administration

Manage access

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Objective

- Manage access to resources.
- Manage access to shared folders.
- Manage access to files and folders by using NTFS permissions.
- Determine effective permissions.
- Managing access to shared files by using offline caching.

Content

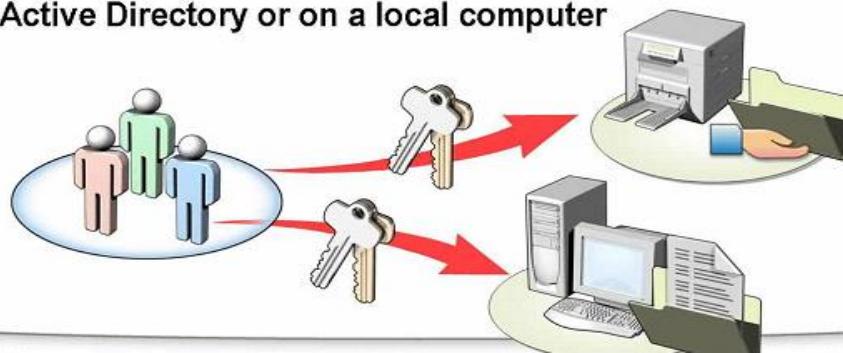
- Managing access to resources.
- Managing access to shared folders.
- Managing access to files and folders by using NTFS permissions.
- Determining effective permissions.
- Managing access to shared files by using offline caching.

Overview of Managing Access to Resources

- What are permission
- What are standard and special permissions
- Multimedia: Permission States

What Are Permissions?

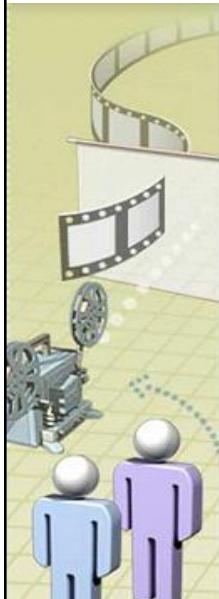
- Permissions define the type of access granted to a user, group, or computer for an object
- You apply permissions to objects such as files, folders, shared folders, and printers
- You assign permissions to users and groups in Active Directory or on a local computer



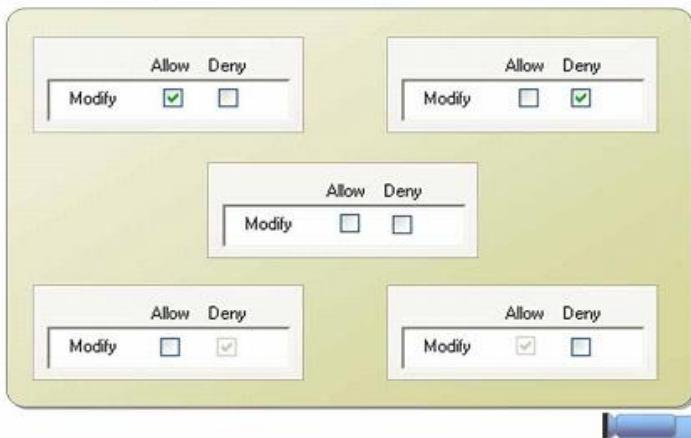
What Are Standard and Special Permissions?

Standard Permissions		Special Permissions																																																												
<p>MOC Properties</p> <p>General Sharing Security Customize </p> <p>Group or user names:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Administrators (NWTRADERS\Administrators) <input checked="" type="checkbox"/> CREATOR OWNER <input checked="" type="checkbox"/> SYSTEM <input checked="" type="checkbox"/> Users (NWTRADERS\Users) <p>Add... Remove</p> <p>Permissions for Administrators</p> <table border="1"> <thead> <tr> <th></th> <th>Allow</th> <th>Deny</th> </tr> </thead> <tbody> <tr> <td>Full Control</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Modify</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Read & Execute</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>List Folder Contents</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Read</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Write</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p>For special permissions or for advanced settings, click Advanced.</p> <p>Advanced</p> <p>OK Cancel Apply</p>			Allow	Deny	Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Modify	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Read & Execute	<input checked="" type="checkbox"/>	<input type="checkbox"/>	List Folder Contents	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Permission Entry for MOC</p> <p>Object </p> <p>Name: Administrators (NWTRADERS\Administrators) Change...</p> <p>Apply to: This folder only</p> <p>Permissions:</p> <table border="1"> <thead> <tr> <th></th> <th>Allow</th> <th>Deny</th> </tr> </thead> <tbody> <tr> <td>Full Control</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Traverse Folder / Execute File</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>List Folder / Read Data</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Read Attributes</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Read Extended Attributes</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Create Files / Write Data</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Create Folders / Append Data</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Write Attributes</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Write Extended Attributes</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Delete Subfolders and Files</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Delete</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Read Permissions</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p>Check Description</p> <p><input type="checkbox"/> Apply these permissions to objects and/or containers within this container only.</p> <p>OK Cancel Clear All</p>		Allow	Deny	Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Traverse Folder / Execute File	<input checked="" type="checkbox"/>	<input type="checkbox"/>	List Folder / Read Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Read Attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Read Extended Attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Create Files / Write Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Create Folders / Append Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Write Attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Write Extended Attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Delete Subfolders and Files	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Delete	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Read Permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Allow	Deny																																																												
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Modify	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Read & Execute	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
List Folder Contents	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
	Allow	Deny																																																												
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Traverse Folder / Execute File	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
List Folder / Read Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Read Attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Read Extended Attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Create Files / Write Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Create Folders / Append Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Write Attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Write Extended Attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Delete Subfolders and Files	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Delete	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												
Read Permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																												

Multimedia: Permission States



In this activity, you will learn the differences between the permission states and test your knowledge



Managing Access to Shared Folders

- Explain what shared folders are.
- Explain what administrative shared folders are.
- Identify the requirements for sharing folders.
- Create a shared folder.
- Explain what published shared folders are.
- Publish a shared folder.
- Explain what shared folder permissions are.
- Set permissions on a shared folder.
- Connect to shared folders.

What are Shared folders?

- Sharing a folder is when a folder is made accessible to multiple users simultaneously over the network.
- After a folder is shared, users can access the files and subfolders in the shared folder if they are granted permission.
- the default permission:
Everyone group -> The Read
- You can place shared folders on a file server and also place them on any computer on the network.

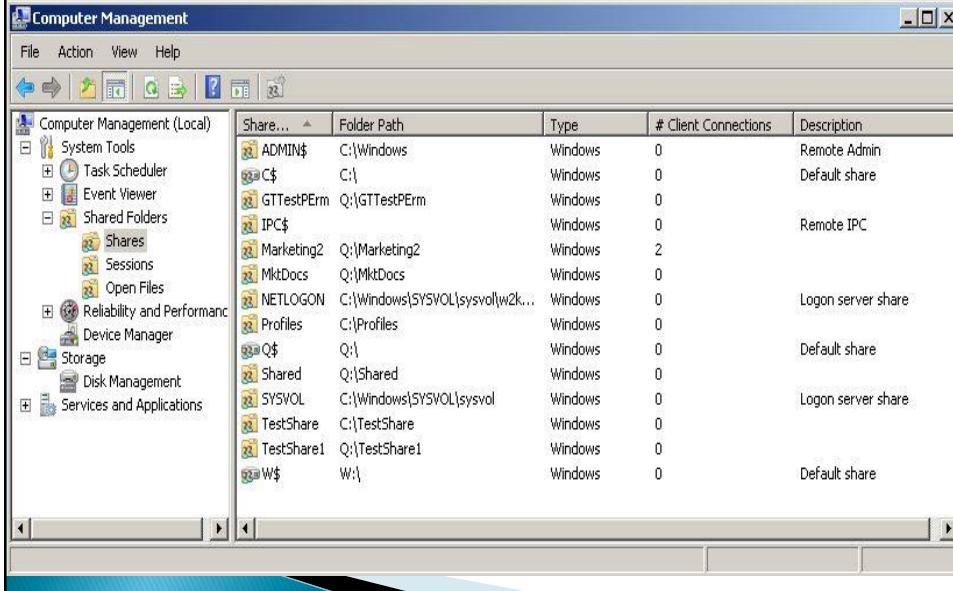
Shared Folder Permissions

Permission	Allows the user to:
Read (Default, applied to the Everyone group)	<ul style="list-style-type: none"> View data in files and attributes View file names and subfolder names Run program files
Change (Includes all Read permissions)	<ul style="list-style-type: none"> Add files and subfolders Change data in files Delete subfolders and files
Full Control	<ul style="list-style-type: none"> Includes all Read and Change permissions Enables you to change NTFS files and folders permissions

What are Shared folders?

- Copy a shared folder:
 - The original shared folder is still shared, but the copy is not shared.
- Move a shared folder:
 - The folder is no longer shared.
- Hide a shared folder:
 - Put a dollar sign (\$) after the name of the shared folder.
 - User can access the shared folder by typing the Universal Naming Convention (UNC) name, for example, \\server\secrets\$.

What Are Administrative Shared Folders?



The screenshot shows the Windows Computer Management console window. The left navigation pane is collapsed, showing icons for System Tools, Event Viewer, Shared Folders, Reliability and Performance, Storage, Disk Management, and Services and Applications. The right pane displays a table of shared folders:

Share...	Folder Path	Type	# Client Connections	Description
ADMIN\$	C:\Windows	Windows	0	Remote Admin
C\$	C:\	Windows	0	Default share
GTTestPErm	Q:\GTTestPErm	Windows	0	
IPC\$		Windows	0	
Marketing2	Q:\Marketing2	Windows	2	
MktDocs	Q:\MktDocs	Windows	0	
NETLOGON	C:\Windows\SYSVOL\sysvol\w2k...	Windows	0	Logon server share
Profiles	C:\Profiles	Windows	0	
Q\$	Q:\	Windows	0	Default share
Shared	Q:\Shared	Windows	0	
SYSVOL	C:\Windows\SYSVOL\sysvol	Windows	0	Logon server share
TestShare	C:\TestShare	Windows	0	
TestShare1	Q:\TestShare1	Windows	0	
W\$	W:\	Windows	0	Default share

Who Can Access Shared Folders?

- To share folders: You must be a member of:

- On a domain controller
 - The Administrators or
 - Server Operators group.

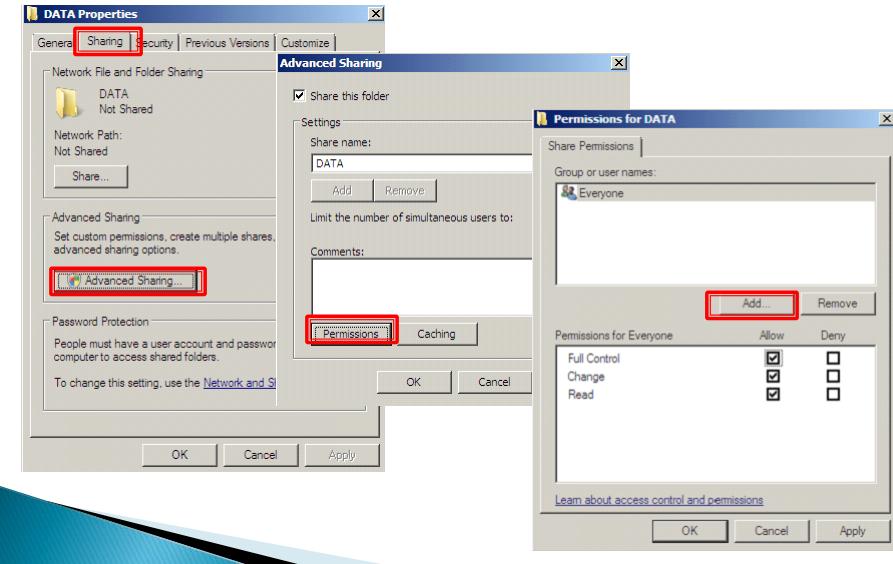
Note that the Power Users group can share folders on a member server in a Windows Server domain.

- On a stand-alone or member server running Windows Server
 - The Administrators or
 - Power Users group.

How to Create a Shared Folder?

- Create a shared folder by using Computer Management
 - Computer Management\Shared Folders\click Shares.
 - Action\click New Share.
 - Follow the steps in the Share a Folder Wizard
- Create a shared folder by using Windows Explorer:
 - Sharing\ Advance Sharing\ Permission
- Create a shared folder by using net share
Also can: deletes, or displays shared folders.
 - Type net share SharedFolderName=Drive:Path

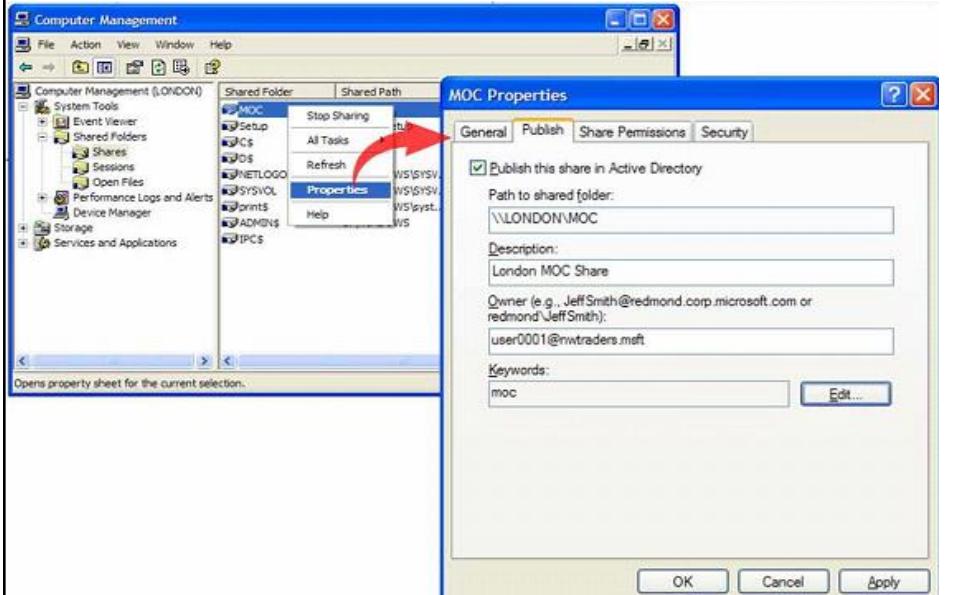
Using Windows Explorer



What Are Published Shared Folders?

- A published shared folder is a shared folder object in Active Directory
- Clients can search Active Directory for shared folders that are published
- Clients do not need to know the name of the server to connect to a shared folder

How to Publish a Shared Folder

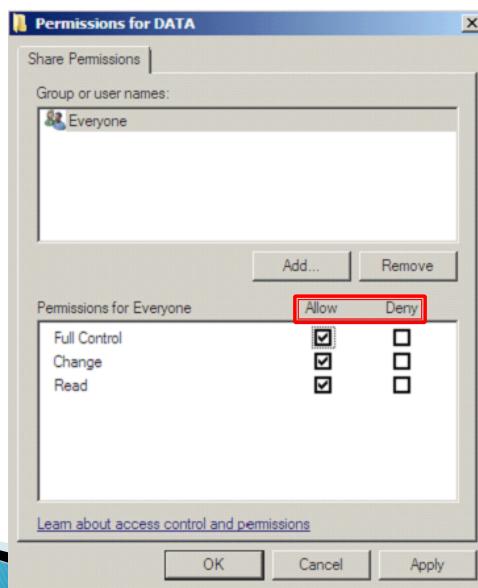


How to Publish a Shared Folder

- To publish a shared folder as a server object:
 - 1. In Computer Management\Shared Folders\then click Shares.
 - 2. Right-click a shared folder\click Properties\Publish tab\Publish this share in Active Directory check box \ then click OK.
- To publish a shared folder to an organizational unit:
 - 1. In Active Directory Users and Computers\right-click the folder\New\ \click Shared Folder.
 - 2. In the New Object - Shared Folder\Name box\ type the folder
 - 3. In the Network path\ type the UNC name\OK.

How to Set Permissions on a Shared Folder

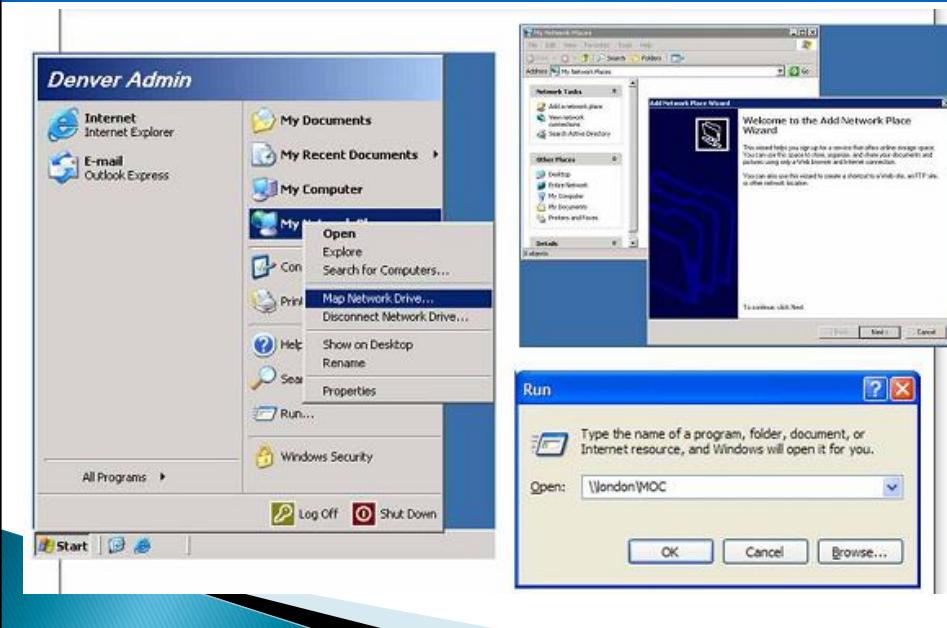
- To set permissions on a shared folder by using Computer Management:
 - 1. In Computer Management\Shared Folders\Shares\
 - 2. In the Properties\ Sharing tab\ click Permissions:
Add /remove to grant/revoke a user/group permission for a shared folder
 - 4. In the Permissions box, select the Allow or Deny \ OK.
- To set permissions on a shared folder by using Windows Explorer:
 - 1. In Windows Explorer, in the shared folder\ Sharing and Security.
 - 2. In the Properties\ Sharing tab\ click Permissions:
Add /remove to grant/revoke a user/group permission for a shared folder
 - 4. In the Permissions box, select the Allow or Deny



How to Connect to Shared Folders

- Using My Network Places
 - Open My Network Places\ Add a network place.
- Using Map Network Drive
 - Right-click My Network Places\ Map Network Drive
- Using the Run command
 - Start\ Run\ enter a UNC path

Connect to Shared Folders



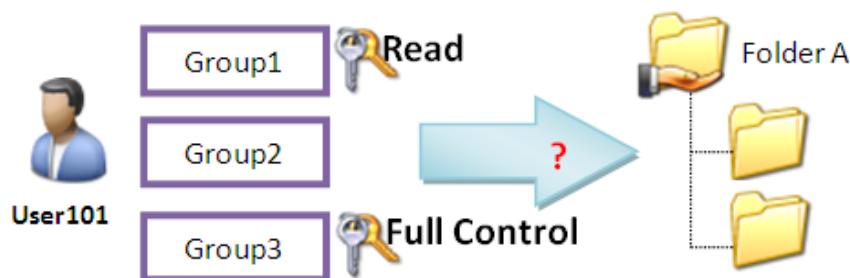
Note:

- Shared folder permissions only apply to users who connect to the folder across the network.
- it is usually most efficient to assign permissions to a group rather than to individual users.
- To restrict access to a folder, use shared folder permissions or NTFS permissions, but not both.

The best practice is to share a folder so that the Everyone group has Full Control, and then restrict access to the folder using NTFS permissions.

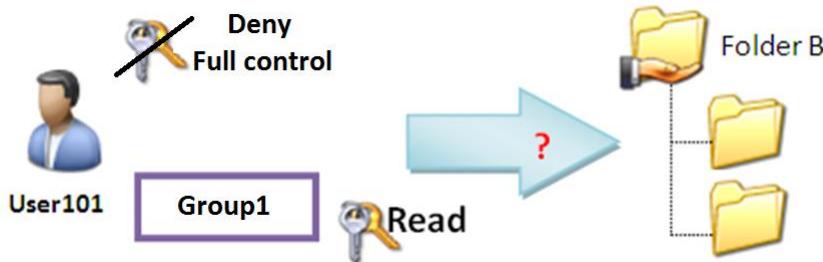
Note:

- The user's effective permissions are the combination of the user and group permissions



Note

- Denied permissions take precedence over any permissions that you otherwise allow for user accounts and groups



Practice: Managing Access to Shared Folders

- Create a shared folder
- Test Read permissions of the shared folder
- Test Full Control permissions of the shared folder

Managing Access to Files and Folders Using NTFS Permissions

- Explain what NTFS is.
- Explain what NTFS file and folder permissions are.
- Explain the effects on NTFS permissions of copying and moving files and folders.
- Explain what NTFS permissions inheritance is.
- Explain best practices for managing access to files and folders by using NTFS permissions.
- Copy or remove inherited permissions.
- Manage access to files and folders by using NTFS permissions.

What Is NTFS?

- Reliability
 - NTFS uses log file and checkpoint information to restore the integrity of the file system when the computer is restarted.
 - If there is a bad-sector error, NTFS dynamically remaps the cluster containing the bad sector and allocates a new cluster for the data.
 - NTFS also marks the cluster as unusable.
- Greater security
 - NTFS files use the Encrypting File System (EFS) to secure files and folders. can be encrypted for use by single or multiple users.
 - NTFS also stores an access control list (ACL) with every file and folder on an NTFS partition. (granted access for the file or folder and the type of access that they are granted)

What Is NTFS?

- Improved management of storage growth
 - NTFS supports disk quotas
 - NTFS supports larger files and a larger number of files per volume than FAT or FAT32.
 - NTFS also manages disk space efficiently by using smaller cluster sizes. (reduces wasted space on hard disks)
- Multiple user permissions

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



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

MCTS Windows Server 2008 Active Directory

31

detail

Write:

- Create file and folder
- Change file and folder attribute
- Write file

Read:

- View file and folder
- View file and folder attribute

Read & Execute:

- Explorer folder, run program file
- Read

List folder content:

- Explorer folder, run program file
- Read

Modify:

- Read & Execute
- Write
- Delete file and subfolder

Full Control:

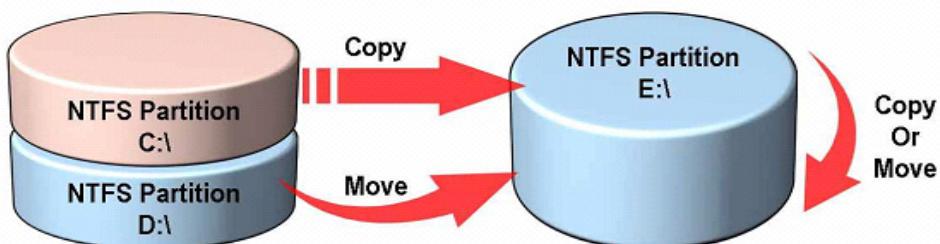
- Modify
- Change folder and file owner
- Take ownership of file ad folder

NTFS Permissions (cont.)

Special permission	Description	Included in standard permission
Full control	Same as the standard Full control permission	Full control
Traverse folder/execute file	For folders: Allows accessing files in folders or subfolders even if the user doesn't normally have access to the folder For files: Allows running program files	Full control, Modify, Read & execute, List folder contents
List folder/read data	For folders: Allows users to view subfolders and filenames in the folder For files: Allows users to view data in files	Full control, Modify, Read & execute, List folder contents, Read
Read attributes	Allows users to view file or folder attributes	Full control, Modify, Read & execute, List folder contents, Read
Read extended attributes	Allows users to view file or folder extended attributes	Full control, Modify, Read & execute, List folder contents, Read
Create files/write data	Allows users to create new files and modify the contents of existing files	Full control, Modify, Write
Create folders/append data	Allows users to create new folders and add data to the end of existing files but not change existing data in a file	Full control, Modify, Write
Write attributes	Allows users to change file and folder attributes	Full control, Modify, Write
Write extended attributes	Allows users to change file and folder extended attributes	Full control, Modify, Write
Delete subfolders and files	Allows users to delete subfolders and files in the folder	Full control
Delete	Allows users to delete the folder or file	Full control, Modify
Read permissions	Allows users to read NTFS permissions of a folder or file	Full control, Modify, Read & execute, List folder contents, Read, Write
Take ownership	Allows users to take ownership of a folder or file, which gives the user implicit permission to change permissions on that file or folder	Full control

33

Effects on NTFS Permissions When Copying and Moving Files and Folders

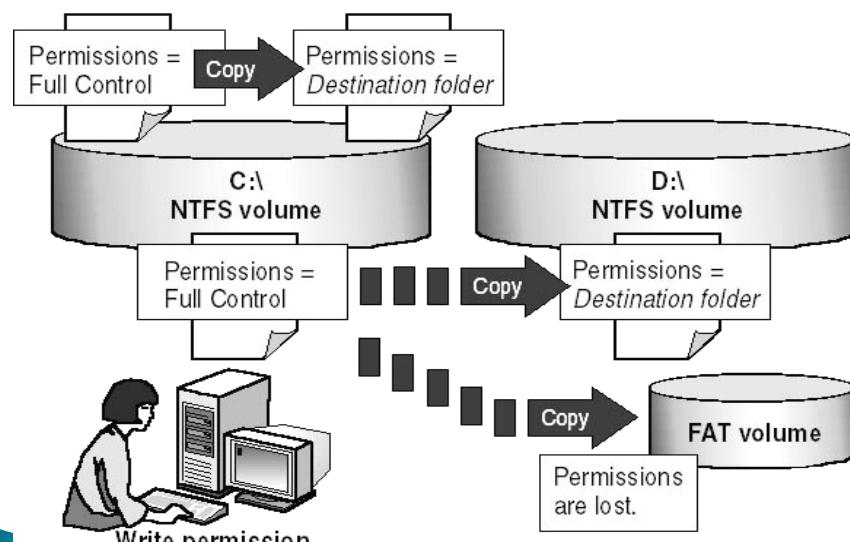


- When you copy files and folders, they inherit permissions of the destination folder
- When you move files and folders within the same partition, they retain their permissions
- When you move files and folders to a different partition, they inherit the permissions of the destination folder

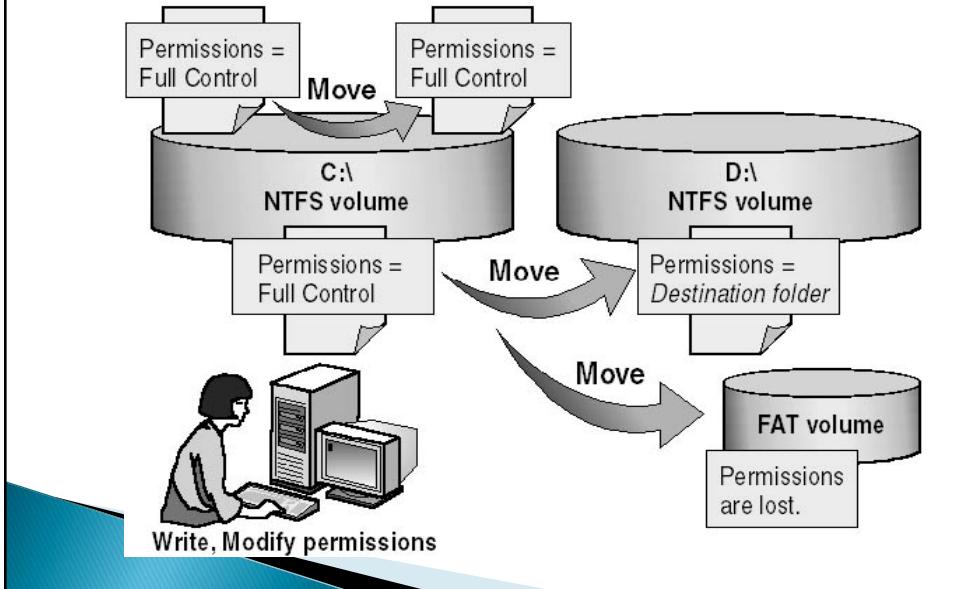
Effects on NTFS Permissions When Copying and Moving Files and Folders

- When you copy a folder or file to a non-NTFS partition, such as a FAT partition, the copy of the folder or file loses its NTFS permissions, because non-NTFS partitions do not support NTFS permissions.
- When you move a folder or a file to a non-NTFS partition, the folder or file loses its NTFS permissions, because non-NTFS partitions do not support NTFS permissions.

Copy



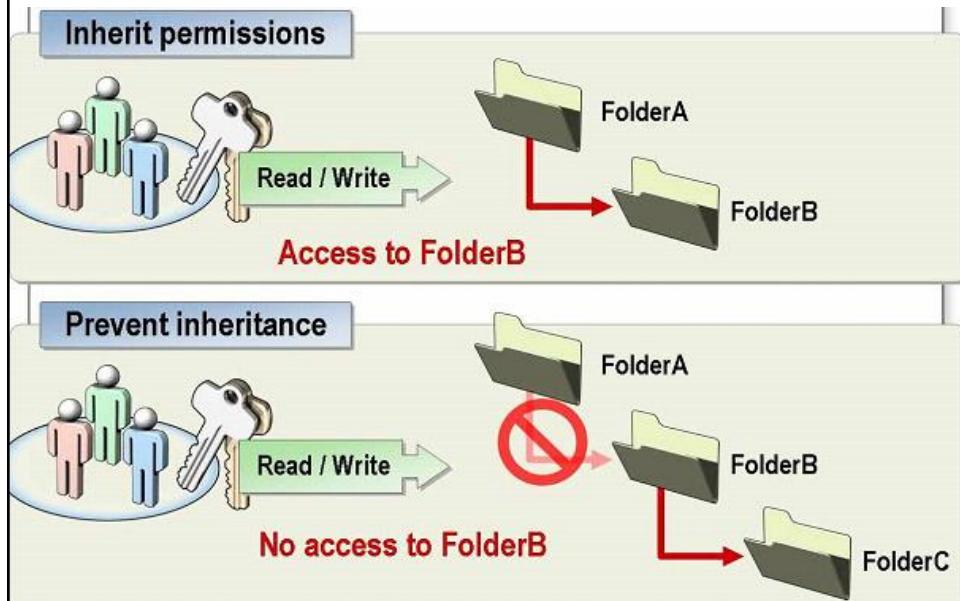
Move



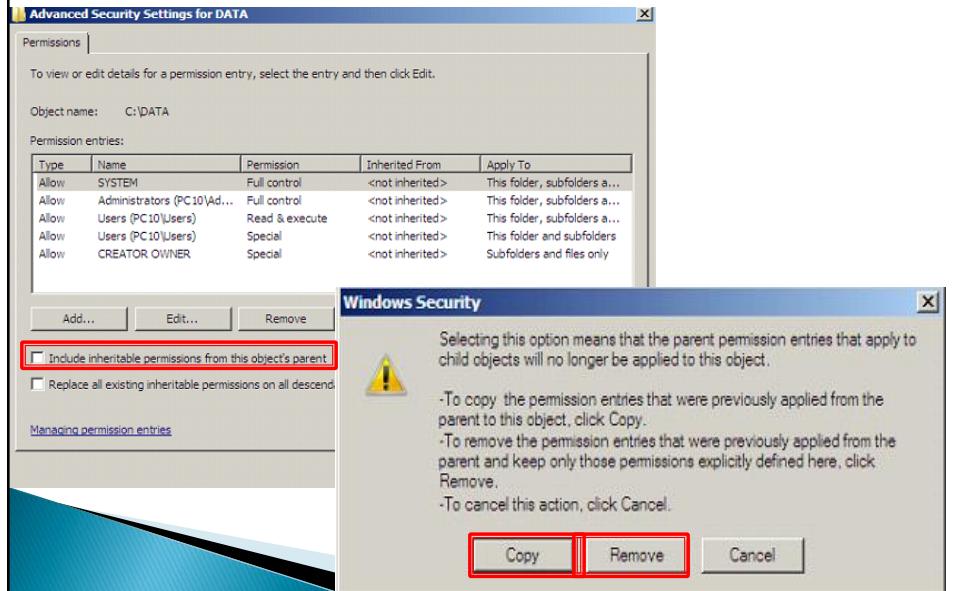
What Is NTFS Permissions Inheritance?

- By default, permissions that you grant to a parent folder are inherited by the subfolders and files that are contained in the parent folder.
- You can prevent subfolders and files from inheriting permissions that are assigned to the parent folder.
- When you prevent permissions inheritance, you can either:
 - Copy inherited permissions from the parent folder.
 - Remove the inherited permissions and retain only the permissions that were explicitly assigned.
- The folder at which you prevent permissions inheritance becomes the new parent folder, and the subfolders and files that are contained in it inherit the permissions assigned to it.

What Is NTFS Permissions Inheritance?



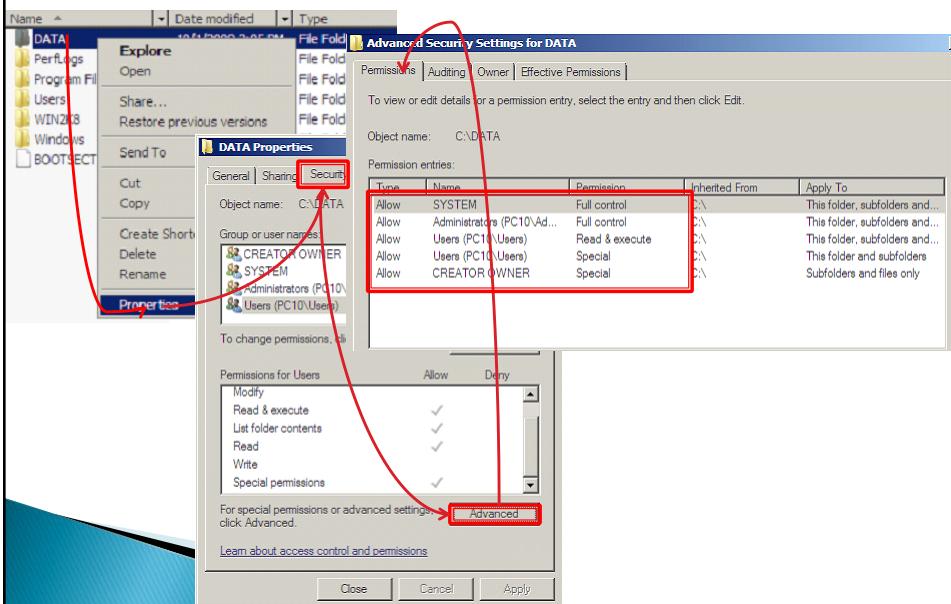
How to Copy or Remove Inherited Permissions



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

How to Manage Access to Files and Folders Using NTFS Permissions

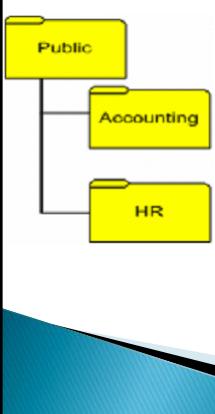


Practice: Managing Access to Files and Folders Using NTFS Permissions

- I want you to create a shared folder called Public that is accessible to the Accounting department and the HR department.
- All employees will need to access the same shared folder and will then navigate to the appropriate folder for their job tasks.
- You must create the folders represented in the following diagram and configure the shared folder and NTFS permissions:

Practice: Managing Access to Files and Folders Using NTFS Permissions

- Share the Public folder. Create folders
- Configure NTFS permissions
- Test the NTFS permissions



Folder	Group	NTFS Special Permissions
D:\Public	Authenticated Users	Traverse Folder / Execute File List Folder / Read Data Read Permissions
	ComputerName\Administrators	Full Control
D:\Public\Accounting	DL NWTraders Accounting Personnel Full Control	Full Control
	ComputerName\Administrator	Full Control
D:\Public\HR	DL NWTraders HR Personnel Full Control	Full Control
	ComputerName\Administrators	Full Control

Determining Effective Permissions

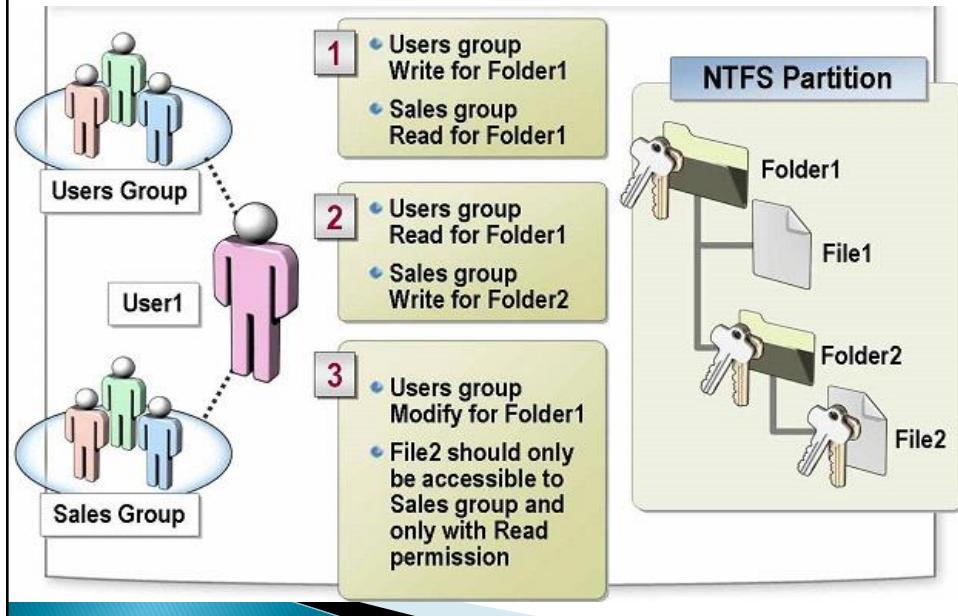
- Explain what effective permissions on NTFS files and folders are.
- Determine effective permissions on NTFS files and folders.
- Explain the effects of combined shared folder and NTFS permissions.
- Determine effective permissions on combined shared folder and NTFS permissions.

What Are Effective Permissions on NTFS Files and Folders?

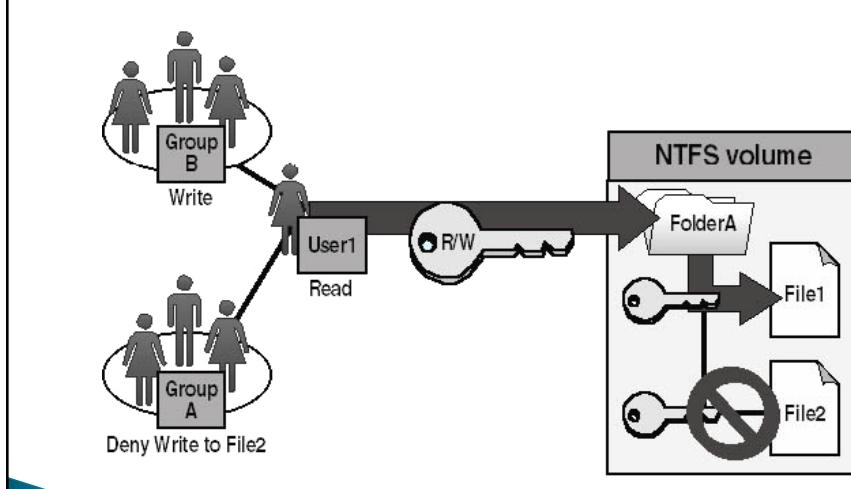
Effective permissions have the following characteristics:

- Cumulative permissions are the combination of the highest NTFS permissions granted to the user and all the groups the user is a member of.
- NTFS file permissions take priority over folder permissions.
- Deny permissions override all permissions.
- Every object is owned in an NTFS volume or Active Directory. The owner controls how permissions are set on the object and to whom permissions are granted.

Discussion: Applying NTFS Permissions



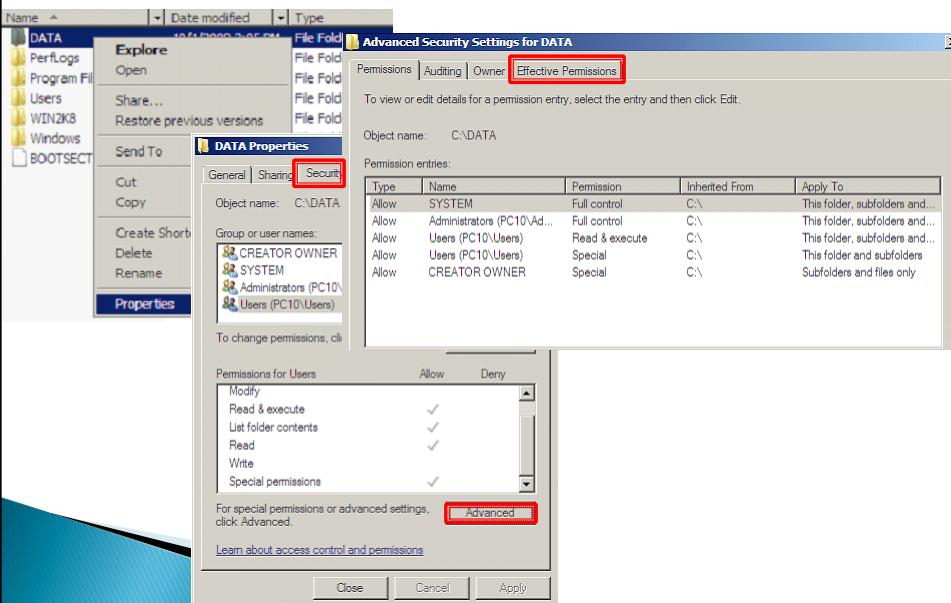
Deny NTFS permission

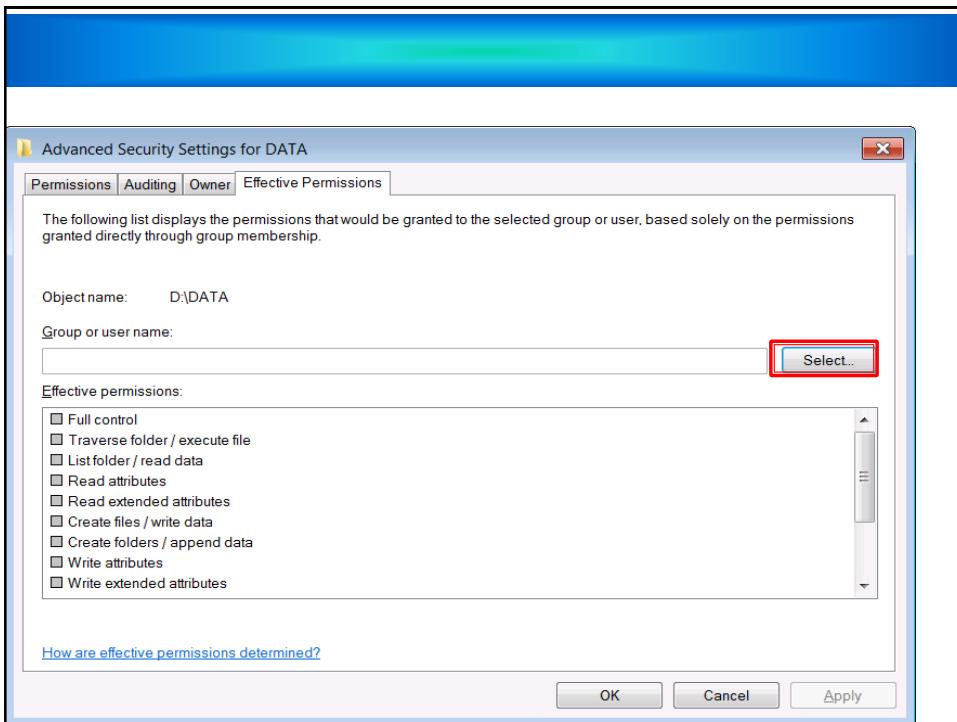


How to Determine Effective Permissions on NTFS Files and Folders

- To view the effective permissions for files and folders:
 - In Windows Explorer, right-click files and folders \ click Properties.
 - In the Properties\ Security tab\ click Advanced.
 - In the Advanced Security \ Effective Permissions\ Select.
 - In the Select, User, Computer or Group dialog box, in the Enter the object name to select box, type the name of a user or group\ OK.

Configure Effective Permission





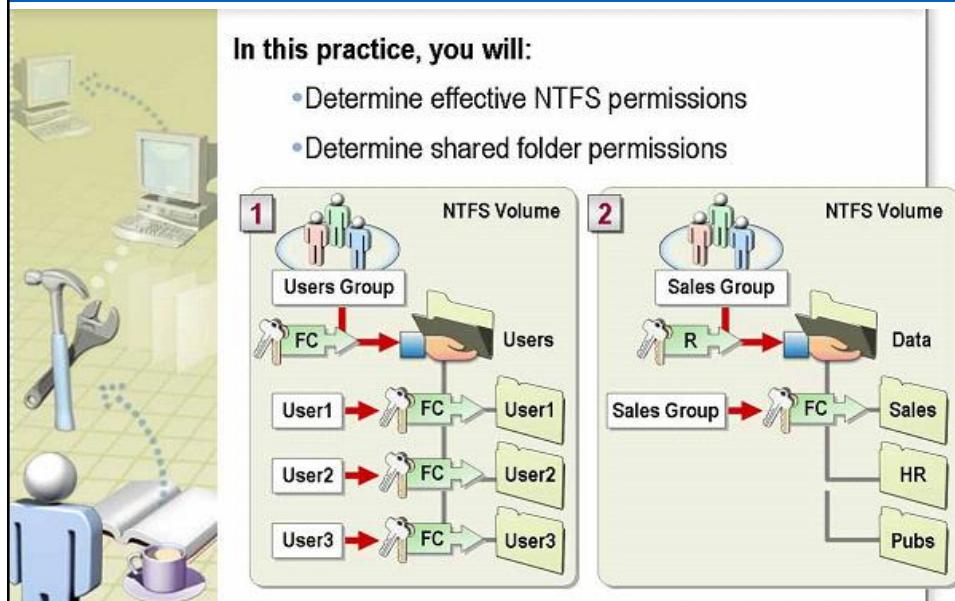
Combined Shared Folder and NTFS Permissions

- 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 Share and NTFS permissions

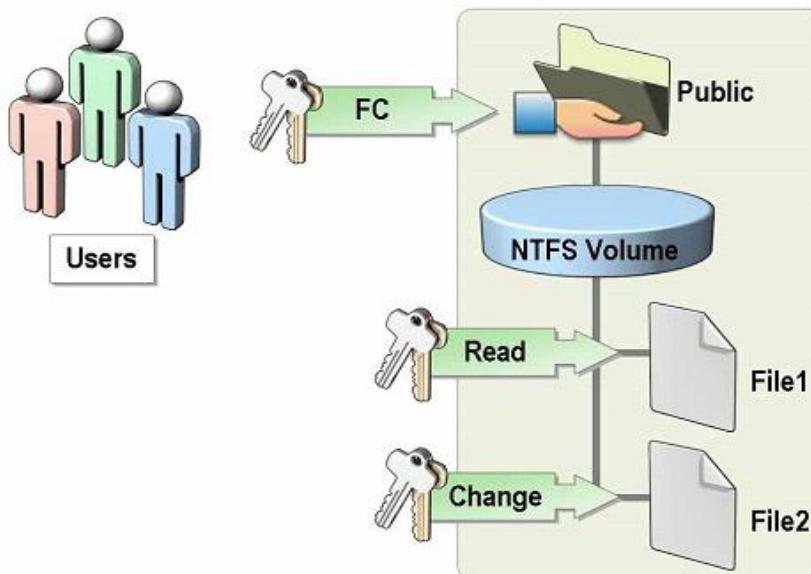
How to Determine the Effective Permissions on Combined Shared Folder and NTFS Permissions

- To determine the maximum NTFS permissions
 - WE\ Properties\ Security\ Advanced\ Effective Permissions
- To determine the maximum shared folder permissions
 - WE\ Properties\ Shared\ Advanced Sharing\ Permissions
- To determine the effective permissions for a shared folder:
 - Compare the maximum NTFS permissions with the maximum shared folder permissions.
 - The most restrictive permission for the user between the maximum NTFS and shared folder permissions is the effective permissions.

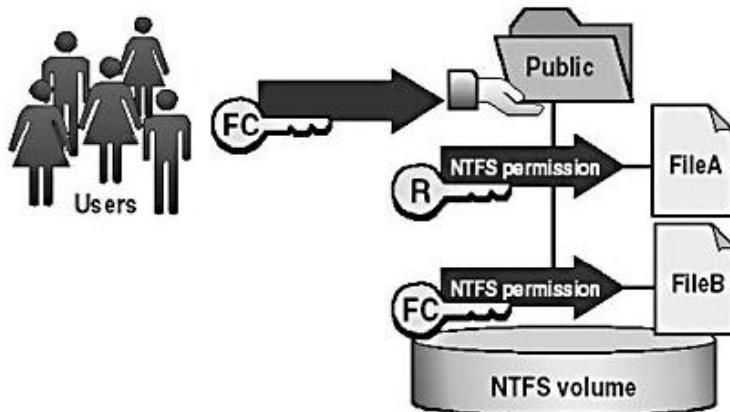
Practice: Determining Effective NTFS and Shared Folder Permissions



Effects of Combined Shared Folder and NTFS Permissions



Cont.



Lab A: Managing Access to Resources

- After completing this lab, you will be able to:
 - Create groups.
 - Configure NTFS security.
 - Configure shared folder security.
- Action:
 - Configure Access for Manufacturing Personnel
 - Configure Access for Marketing Personnel
 - Configure Access for Accounting Personnel

LAB	
Tasks	Detailed Information
1. Create a shared folder.	<ul style="list-style-type: none"> ▪ Tool: Computer Management (Glasgow) ▪ Server name: Glasgow ▪ Folder path: D:\ComputerName\Manufacturing ▪ Share name: <i>ComputerName</i> Manufacturing ▪ Shared folder permissions: <ul style="list-style-type: none"> • Grant Full Control to DL NWTraders Manufacturing Managers Full Control • Grant Read to DL NWTraders Manufacturing Personnel Read • Remove Everyone
2. Set the NTFS permissions.	<ul style="list-style-type: none"> ▪ Grant Modify to DL Manufacturing Managers Full Control ▪ Grant Read to DL Manufacturing Personnel Read ▪ Grant Full Control to GLASGOW\Administrators ▪ Copy all NTFS permissions inheritance

LAB	
Tasks	Detailed Information
1. Create a shared folder.	<ul style="list-style-type: none"> ▪ Tool: Computer Management (Glasgow) ▪ Server name: Glasgow ▪ Folder path: D:\ComputerName Marketing ▪ Share name: <i>ComputerName</i> Marketing ▪ Shared folder permissions: <ul style="list-style-type: none"> • Grant Full Control to DL NWTraders Marketing Personnel Full Control • Grant Full Control to GLASGOW\Administrators
2. Set the NTFS permissions.	<ul style="list-style-type: none"> ▪ Grant Modify to DL Marketing Personnel Full Control ▪ Grant Full Control to GLASGOW\Administrators ▪ Copy all NTFS permissions inheritance

LAB	
Tasks	Detailed Information
1. Create a shared folder.	<ul style="list-style-type: none"> ▪ Tool: Computer Management (Glasgow) ▪ Server name: Glasgow ▪ Folder path: D:\ComputerName Accounting ▪ Share name: ComputerName Accounting ▪ Shared folder permissions: <ul style="list-style-type: none"> • Grant Full Control to DL NWTraders Accounting Personnel Full Control • Grant Full Control to GLASGOW\Administrators
2. Set NTFS permissions.	<ul style="list-style-type: none"> ▪ Grant Modify to DL ComputerName Accounting Personnel Full Control ▪ Grant Full Control to GLASGOW\Administrators ▪ Copy all NTFS permissions inheritance