Microsoft®
Training &
Certification

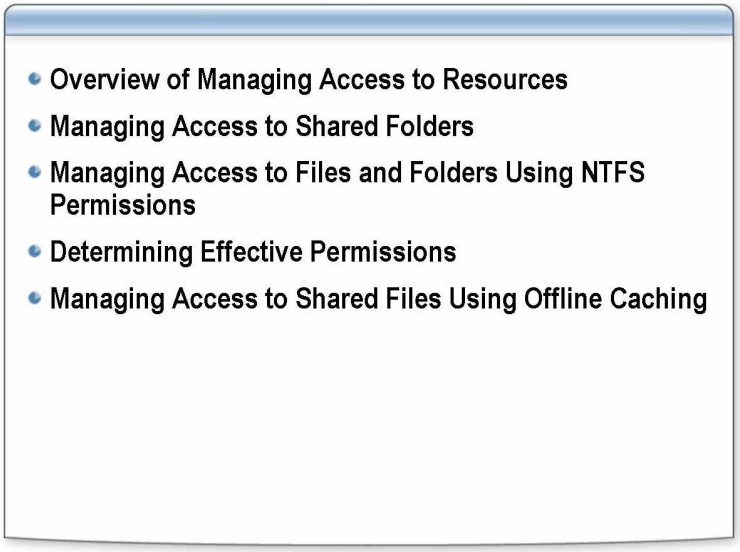
Microsoft® Official
Curriculum

Module 4: Managing Access to Resources

Contents

Microsoft®

Overview



Introduction

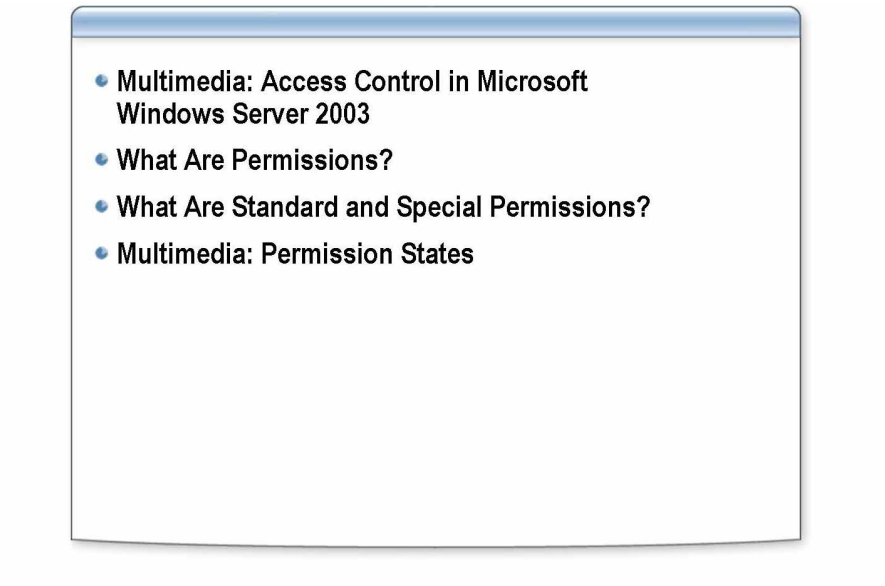
This module introduces the job function of managing access to resources. Specifically, the module provides the skills and knowledge that you need to explain; manage access to files and folders by using shared folder permissions, NTFS permissions, or effective permissions; and manage access to shared files using offline caching.

Objectives

After completing this module, you will be able to:

- 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.

Lesson: Overview of Managing Access to Resources



Introduction

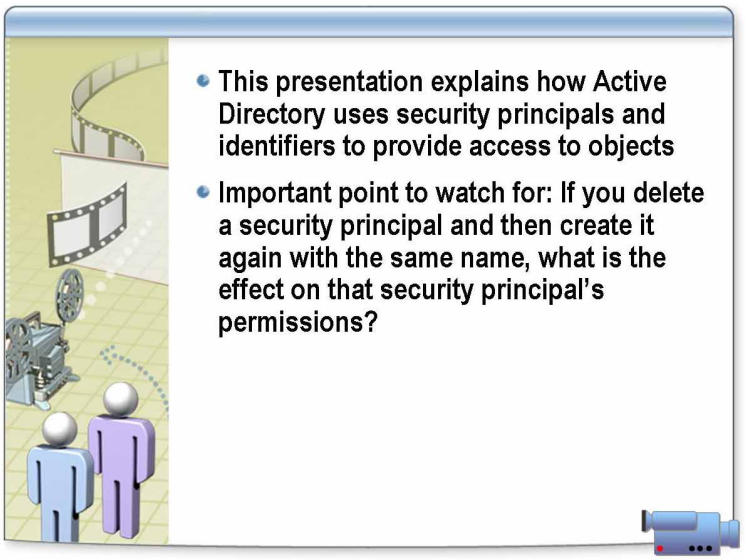
The information in this lesson presents the knowledge that you need to manage access to resources.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the components of access control in Microsoft® Windows® Server 2003.
- Define permissions.
- Explain the differences between standard and special permissions.
- Explain the characteristics of implicit and explicit permission states.

Multimedia: Access Control in Microsoft Windows Server 2003



File location

To view the *Access Control in Microsoft Windows Server 2003* presentation, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Key points

Key points from the presentation are summarized in the following list:

- Security principal

  A security principal is an account that can be authenticated.

- Security identifier (SID)

  A SID is an alphanumeric structure that is issued when an account is created and that uniquely identifies a security principal.

- Discretionary access control list (DACL)

  Each resource is associated with a DACL, which identifies the users and groups that are allowed or denied access to that resource.

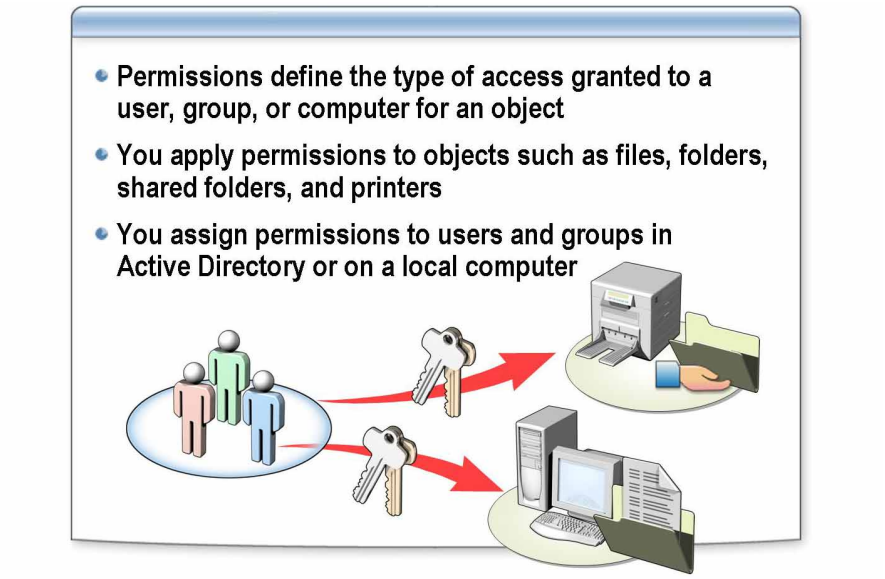
- Access control entry (ACE)

  A DACL contains multiple ACEs. Each ACE specifies a SID, special permissions, inheritance information, and an Allow or Deny permission.

Additional reading

For more information about access control, see "Access Control Components" at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/access_control_components.asp.

What Are Permissions?



Definition

Permissions define the type of access granted to a user, group, or computer for an object. For example, you can let one user read the contents of a file, let another user make changes to the file, and prevent all other users from accessing the file. You can set similar permissions on printers so that certain users can configure the printer and other users can only print from it.

Permissions are also applied to any secured objects, such as files, objects in the Active Directory® directory service, and registry objects. Permissions can be granted to any user, group, or computer.

You can grant permissions for objects to:

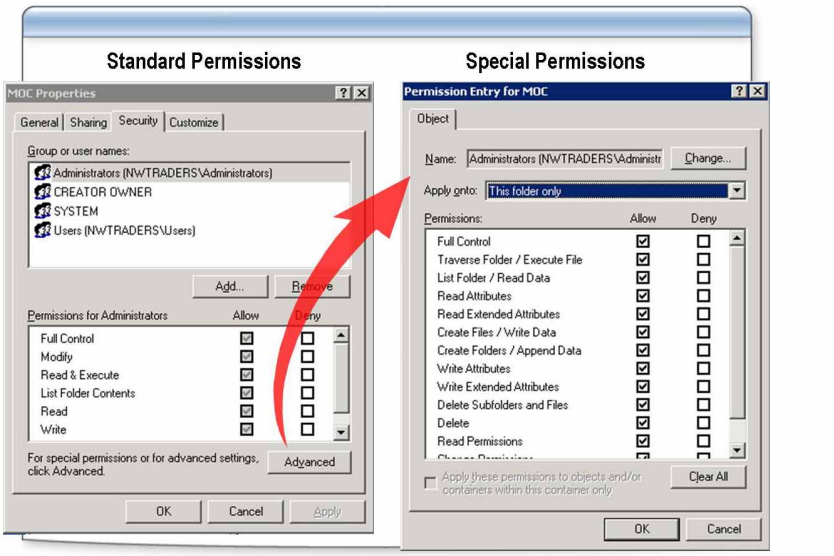
- Groups, users, and special identities in the domain.
- Groups and users in any trusted domains.
- Local groups and users on the computer where the object resides.

Permission types

When you set permissions, you specify the level of access for groups and users. The permissions attached to an object depend on the type of object. For example, the permissions that are attached to a file are different from those that are attached to a registry key. Some permissions, however, are common to most types of objects. The following permissions are common permissions:

- Read permissions
- Write permissions
- Delete permissions

What Are Standard and Special Permissions?



Introduction

You can grant standard and special permissions for objects. Standard permissions are the most frequently assigned permissions. Special permissions provide you with a finer degree of control for assigning access to objects.

Standard permissions

The system has a default level of security settings for a specific object. These are the most common set of permissions that a systems administrator uses on a daily basis. The list of standard permissions that are available varies depending on what type of object you are modifying the security for.

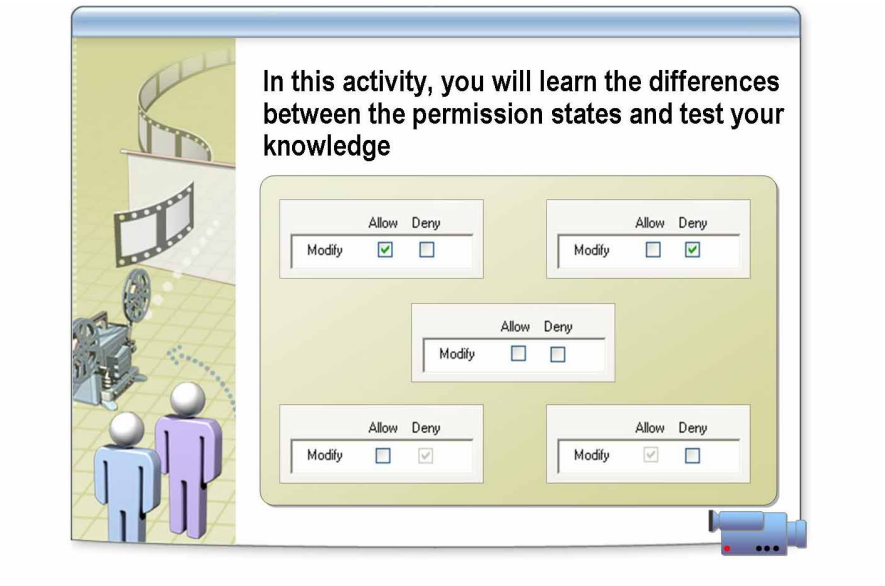
Special permissions

Special permissions are a more detailed list of permissions. A standard NFTS permission of Read is related to the following special permissions:

- List Folder/Read Data
- Read Attributes
- Read Extended Attributed
- Read Permissions

If the systems administrator removes a special permission that relates to a standard permission, the check box for the standard permission is no longer selected. The check box for the special permission under the standard permission list is selected.

Multimedia: Permission States



File location

To start the *Permission States* activity, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the activity.

Lesson: Managing Access to Shared Folders

Introduction

The Windows Server 2003 family organizes files into directories that are graphically represented as folders. These folders contain all types of files and can contain subfolders. Some of these folders are reserved for operating system files and program files. Users should never place any data into the operating system folders or program file folders.

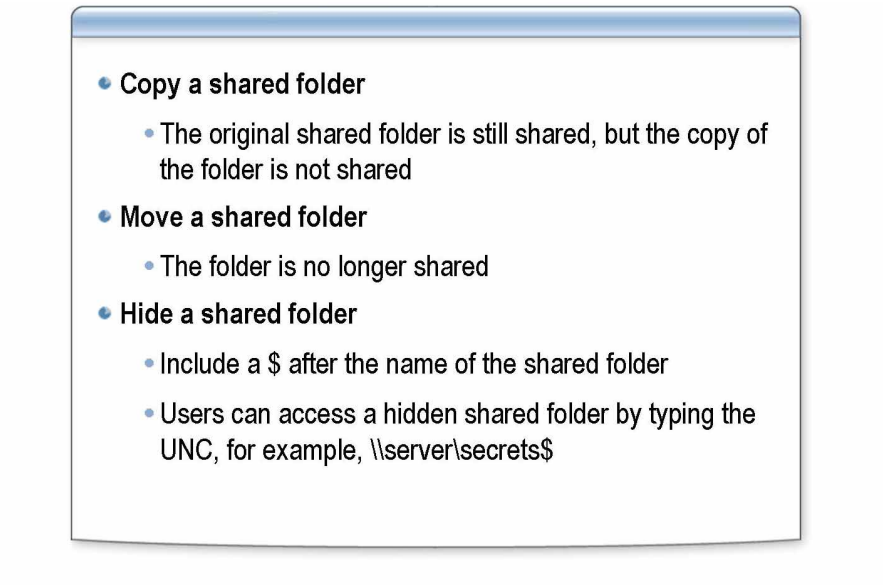
Shared folders give users access to files and folders over a network. Users can connect to the shared folder over the network to access the folders and files they contain. Shared folders can contain applications, public data, or a user's personal data. Using shared application folders centralizes administration by enabling you to install and maintain applications on a server instead of client computers. Using shared data folders provides a central location for users to access common files and makes it easier to back up data contained in those files.

Lesson objectives

After completing this lesson, you will be able to:

- 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?



Introduction

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 all of the files and subfolders in the shared folder if they are granted permission.

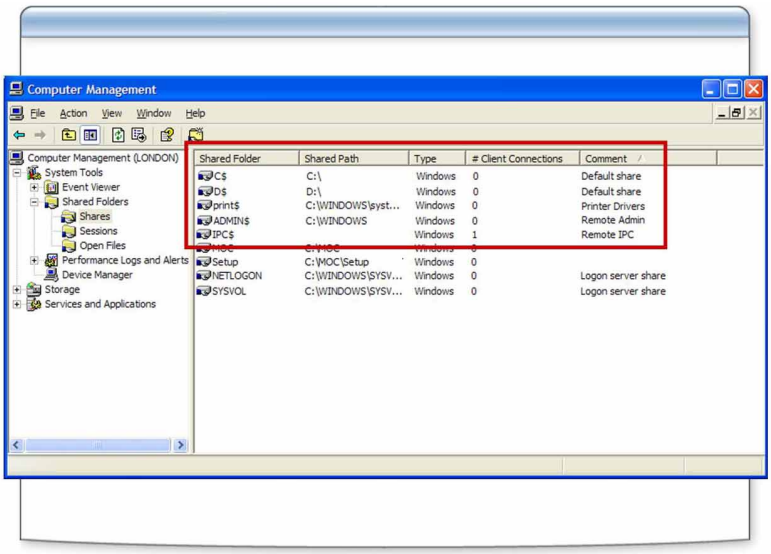
You can place shared folders on a file server and also place them on any computer on the network. You can store files in shared folders according to categories or functions. For example, you can place shared data files in one shared folder and shared application files in another.

Characteristics of shared folders

Some of the most common characteristics of shared folders are as follows:

- A shared folder appears in Windows Explorer as an icon of a hand holding the folder.
- You can only share folders, not individual files. If multiple users need access to the same file, you must place the file in a folder and then share the folder.
- When a folder is shared, the Read permission is granted to the Everyone group as the default permission. Remove the default permission and grant the Change permission or Read permission to groups as needed.
- When users or groups are added to a shared folder, the default permission is Read.
- When you copy a shared folder, the original shared folder is still shared, but the copy is not shared. When a shared folder is moved to another location, the folder is no longer shared.
- You can hide a shared folder if you put a dollar sign ($) after the name of the shared folder. The user cannot see the shared folder in the user interface, but a user can access the shared folder by typing the Universal Naming Convention (UNC) name, for example, \\server\secrets$.

What Are Administrative Shared Folders?



Introduction

Windows Server 2003 automatically shares folders that enable you to perform administrative tasks. They are designated by an appended dollar sign ($) at the end of the folder name. The dollar sign hides the shared folder from users who browse to the computer in My Network Places. Administrators can quickly administer files and folders on remote servers by using these hidden shared folders.

Types of administrative shared folders

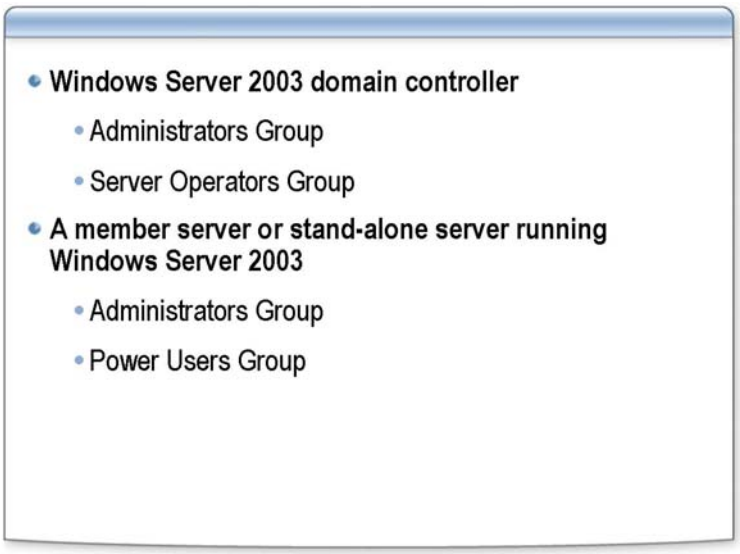
By default, members of the Administrators group have the Full Control permission for administrative shared folders. You cannot modify the permissions for administrative shared folders. The following table describes the purpose of the administrative shared folders that Windows Server 2003 automatically provides.

Shared folder	Purpose
C$, D$, E$	You use these shared folders to remotely connect to a computer and perform administrative tasks. The root of each partition (that has a drive letter assigned to it) on a hard disk is automatically shared. When you connect to this folder, you have access to the entire partition.
Admin$	This is the systemroot folder, which is C:\Winnt by default. Administrators can access this shared folder to administer Windows Server 2003 without knowing the folder in which it is installed.
Print$	This folder provides access to printer driver files for client computers. When you install the first shared printer, the *Systemroot*\System32\Spool\Drivers folder is shared as Print$. Only members of the Administrators, Server Operators, and Print Operators groups have Full Control permission for this folder. The Everyone group has Read permission for this folder.
IPC$	This folder is used during remote administration of a computer and when viewing a computer's shared resources.
FAX$	This shared folder is used to temporarily cache files and access cover pages on the server.

Additional reading

For more information on IPC$, see article 101150, “Operating Characteristics and Restrictions of Named Pipes” in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=101150.

Who Can Access Shared Folders?



Introduction

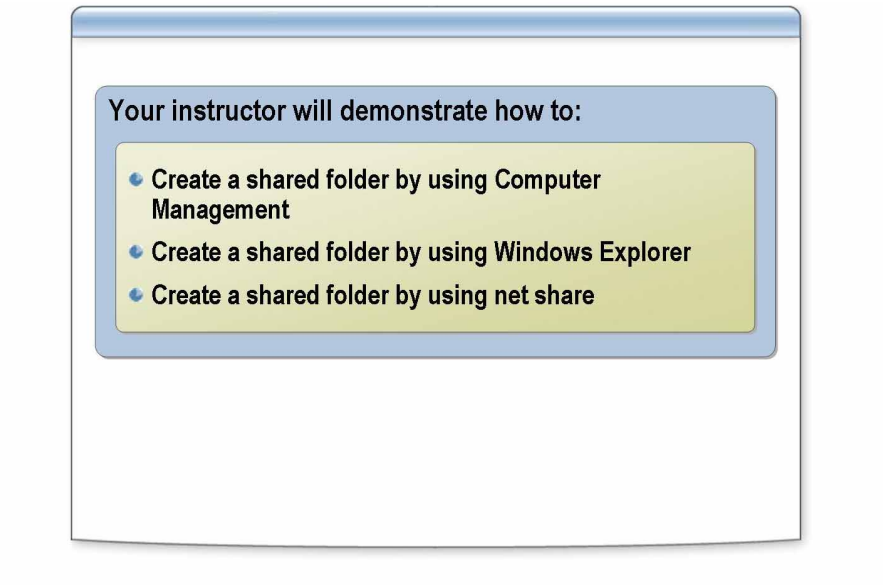
In Windows Server 2003, the only groups that can access shared folders are the Administrators, Server Operators, and Power Users groups. These groups are built-in groups that are placed in the Group folder in Computer Management or the built-in folder in Active Directory Users and Groups.

Groups that can access shared folders

The following table describes who can access shared folders.

To share folders:	You must be a member of:
On a Windows Server 2003 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 2003 domain.
On a stand-alone or member server running Windows Server 2003	The Administrators or Power Users group.

How to Create a Shared Folder



Introduction

When you create a shared folder, you give it a shared folder name and provide a comment that describes the folder and its contents. You can also limit the number of users who can access the folder, grant permissions, and share the same folder multiple times.

Procedure using Computer Management

To create a shared folder by using Computer Management:

1. In Computer Management, in the console tree, expand **Shared Folders** and then click **Shares**.
2. On the **Action** menu, click **New Share**.
3. Follow the steps in the Share a Folder Wizard.

Procedure using Windows Explorer

To create a shared folder by using Windows Explorer:

1. In Windows Explorer, right-click the folder, and then click **Sharing and Security**.
2. In the **Properties** dialog box, on the **Sharing** tab, configure the options described in the following table.

Option	Description
Share this folder	Click to share the folder.
Share name	Enter the name that users from remote locations use to connect to the shared folder. The default shared folder name is the folder name. This option is required. **Note**: Some client computers that connect to a shared folder only see a limited number of characters.
Description	Enter an optional description for the shared folder. You can use this comment to identify the contents of the shared folder.
User Limit	Enter the number of users who can concurrently connect to the shared folder. This option is not required if you click **Maximum Allowed**, current Windows client operating systems supports up to 10 concurrent connections.
Permissions	Click to set the shared folder permissions that apply only when the folder is accessed over the network. This option is not required. By default, the Everyone group is granted the Read permission for all new shared folders.

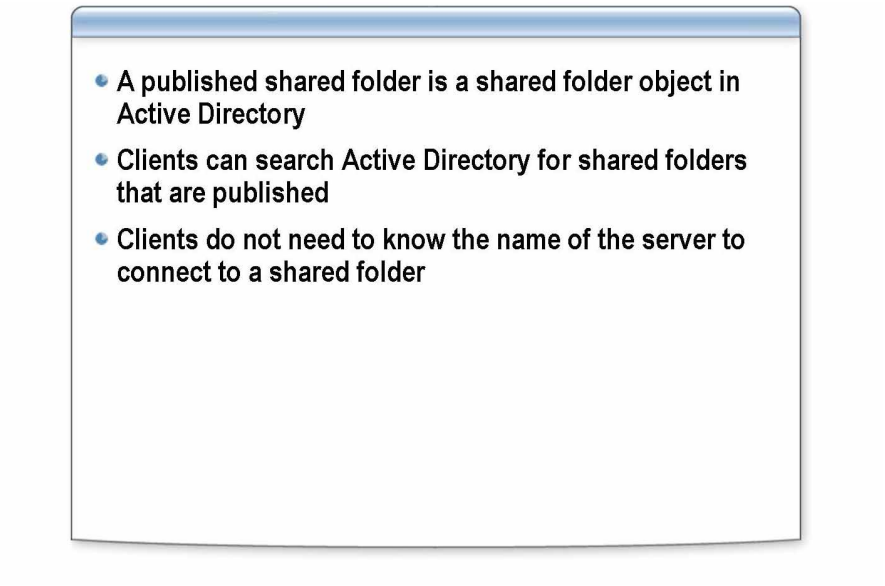
Using a command line

The **net share** command creates, deletes, or displays shared folders. To create a shared folder by using **net share**:

1. Open a command prompt.
2. Type **net share** *SharedFolderName=Drive***:***Path*

Value	Description
*SharedFolderName=Drive***:***Path*	This is the network name of the shared folder and the absolute path of its location.

What Are Published Shared Folders?



Definition

Publishing resources and shared folders in Active Directory enables users to search Active Directory and locate resources on the network even if the physical location of the resources changes.

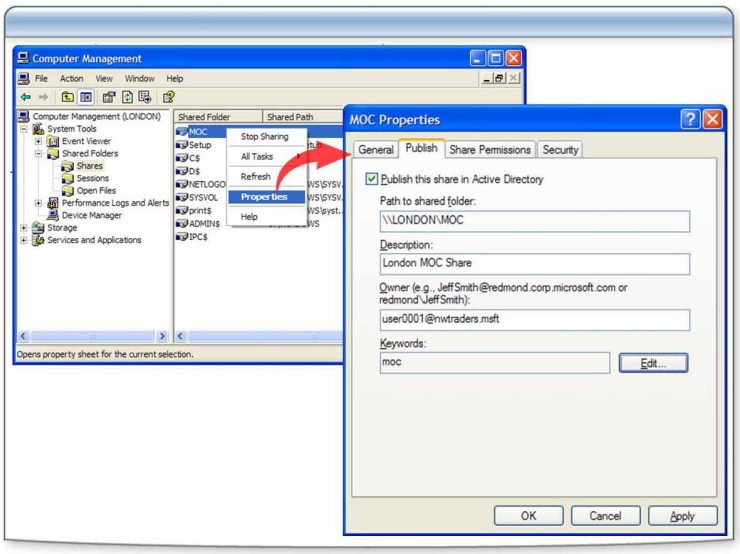
For example, if you move a shared folder to another computer, all shortcuts pointing to the Active Directory object that represents the published shared folder continue to work, as long as you update the reference to the physical location. Users do not have to update their connections.

Publishing the folder

You can publish any shared folder in Active Directory that can be accessed by using a UNC name. After a shared folder is published, a user at a computer running Windows Server 2003 can use Active Directory to locate the object representing the shared folder and then connect to the shared folder.

When the shared folder is published to Active Directory, the shared folder becomes a child object of the computer account. To view shared folders as an object, in Active Directory Users and Computers, on the **View** menu, click **Users, Group, and Computers as containers**. Then, in the console tree, click the computer account. On the details pane, you will see all the published shared folders that are associated with the computer account.

How to Publish a Shared Folder



Introduction

Publishing information about network resources in Active Directory makes it easy for users to find them on the network. You can publish information about printers and shared folders by using Computer Management or Active Directory Users and Computers.

Procedure for publishing a shared folder as a server object

To publish a shared folder as a server object:

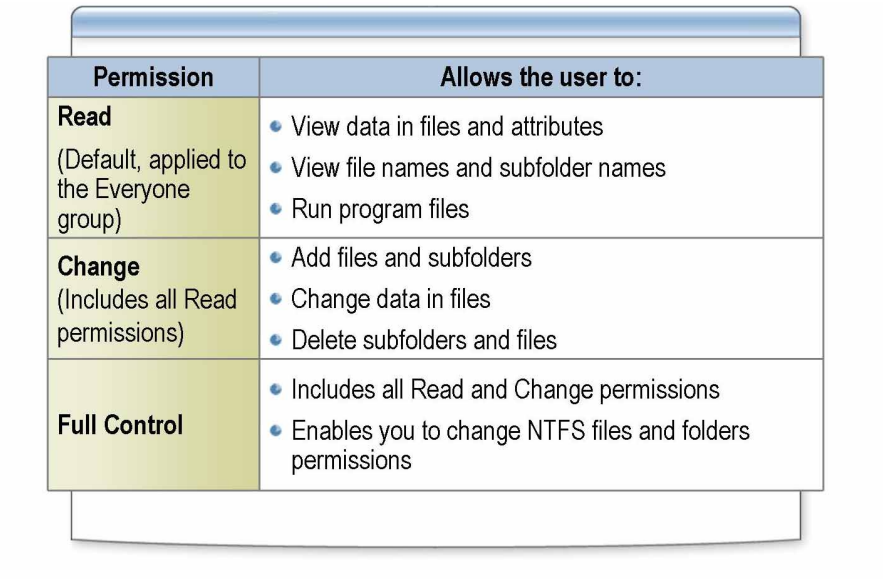
1. In Computer Management, in the console tree, expand **Shared Folders** and then click **Shares**.
2. Right-click a shared folder, and then click **Properties**.
3. In the **Properties** dialog box, on the **Publish** tab, select the **Publish this share in Active Directory** check box, and then click **OK**.

Procedure for publishing a shared folder to an organizational unit

To publish a shared folder to an organizational unit:

1. In Active Directory Users and Computers, in the console tree, right-click the folder in which you want to add the shared folder, point to **New**, and then click **Shared Folder**.
2. In the **New Object – Shared Folder** dialog box, in the **Name** box, type the name of the folder you want clients to use.
3. In the **Network path** box, type the UNC name that you want to publish in Active Directory, and then click **OK**.

Shared Folder Permissions



Permission	Allows the user to:
Read (Default, applied to the Everyone group)	• View data in files and attributes • View file names and subfolder names • Run program files
Change (Includes all Read permissions)	• Add files and subfolders • Change data in files • Delete subfolders and files
Full Control	• Includes all Read and Change permissions • Enables you to change NTFS files and folders permissions

Introduction

Shared folder permissions only apply to users who connect to the folder over the network. They do not restrict access to users who access the folder at the computer where the folder is stored. You can grant shared folder permissions to user accounts, groups, and computer accounts.

Permissions

Shared folder permissions include the following:

- Read

  Read is the default shared folder permission and is applied to the Everyone group. Read permission enables you to:

  - View file names and subfolder names.
  - View data in files and attributes.
  - Run program files.

- Change

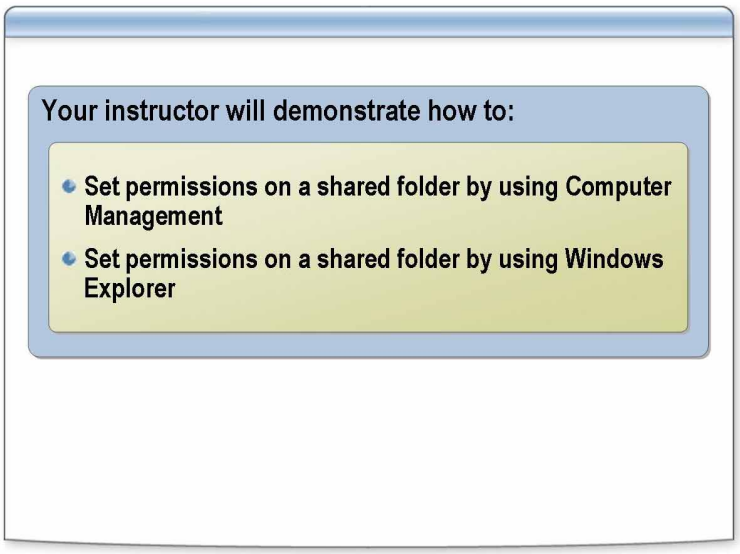
  The Change permission includes all Read permissions and also enables you to:

  - Add files and subfolders.
  - Change data in files.
  - Delete subfolders and files.

- Full Control

  Full Control includes all Read and Change permissions and also enables you to change permissions for NTFS files and folders.

How to Set Permissions on a Shared Folder



Introduction

Use the following procedure to set permissions on a shared folder.

Procedure using Computer Management

To set permissions on a shared folder by using Computer Management:

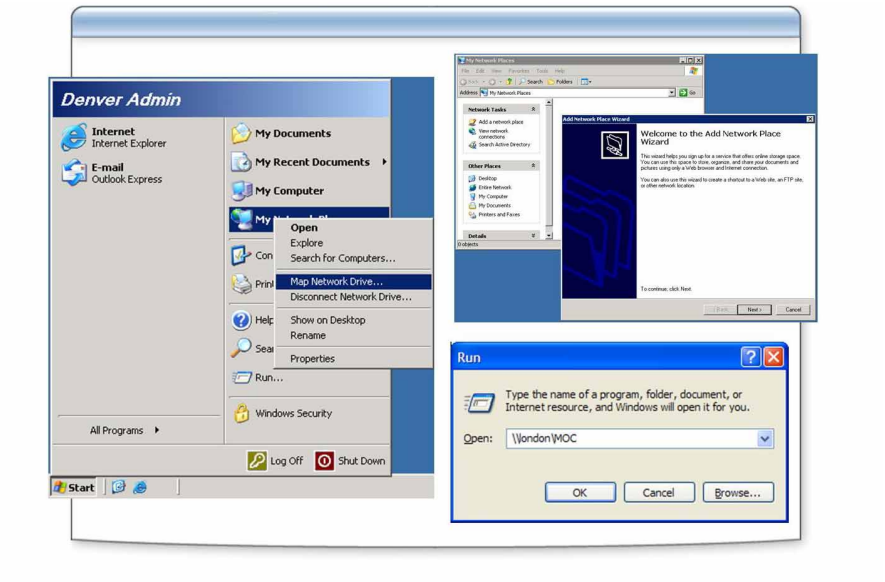
1. In Computer Management, in the console tree, expand **Shared Folders**, and then click **Shares**.
2. In the details pane, right-click the shared folder for which you want to set permissions, and then click **Properties**.
3. In the **Properties** dialog box, on the **Share Permissions** tab, do one of the following:
   - Click **Add** to grant a user or group permission for a shared folder. In the **Select Users, Computers, or Groups** dialog box, select or type the user or group name, and then click **OK**.
   - Click **Remove** to revoke access to a shared folder.
4. In the **Permissions** box, select the **Allow** or **Deny** check boxes to set individual permissions for the selected user or group, and then click **OK**.

Procedures using Windows Explorer

To set permissions on a shared folder by using Windows Explorer:

1. In Windows Explorer, right-click the shared folder for which you want to set permissions, and then click **Sharing and Security**.
2. In the **Properties** dialog box, on the **Sharing** tab, click **Permissions**.
3. In the **Permissions** dialog box, do one of the following:
   - Click **Add** to grant a user or group permission for a shared folder. In the **Select Users, Computers, or Groups** dialog box, select or type the user or group name, and then click **OK**.
   - Click **Remove** to revoke access to a shared resource.
4. In the **Permissions** box, select the **Allow** or **Deny** check boxes to set individual permissions for the selected user or group.

How to Connect to Shared Folders



Introduction

After you create a shared folder, users can access the folder across the network. Users can access a shared folder on another computer by using My Network Places, the **Map Network Drive** feature, or the **Run** command on the **Start** menu.

Procedure using My Network Places

To connect to a shared folder by using My Network Places:

1. Open My Network Places and double-click **Add a network place**.
2. In the Add Network Place Wizard, on the **Welcome** page, click **Next**.
3. On the **Where do you want to create this network place** page, click **Choose another network location**, and then click **Next**.
4. On the **What is the address of this network place** page, type the UNC path of the shared folder or click **Browse**.
   a. If you click **Browse**, expand **Entire Network**.
   b. Expand **Microsoft Windows Network**.
   c. Expand the domain and server you want to connect to.
   d. Click the shared folder that you want to add, and then click **OK**.
5. Click **Next**.
6. On the **What do you want to name this place** page, type the name of the network place, and then click **Next**.
7. On the **Completing the Add Network Place Wizard** page, click **Finish**.

Note When you open a shared folder over the network, Windows Server 2003 automatically adds it to My Network Places.

Procedure using Map Network Drive

When you want a drive letter and icon associated with a specific shared folder, you must map to a network drive. This makes it easier to refer to the location of a file in a shared folder. You can also use drive letters to access shared folders for which you cannot use a UNC path, such as a folder for an older application.

To connect to a shared folder by using My Network Places:

1. Right-click **My Network Places**, and then click **Map Network Drive**.
2. In the **Map Network Drive** dialog box, in the **Drive** box, select the drive that you want to use.
3. In the **Folder** box, type the name of the shared folder you want to connect to or click **Browse**.
4. For a shared folder that you will use on a recurring basis, select the **Reconnect at logon** check box to connect automatically to the shared folder each time you log on.

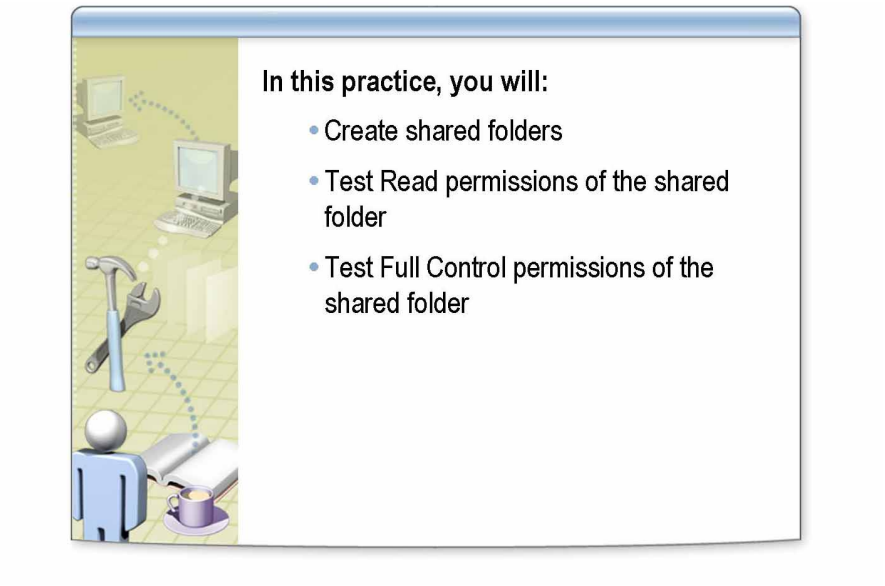
Procedure using the Run command

When you use the **Run** command on the **Start** menu to connect to a network resource, a drive letter is not required. This enables you to connect to the shared folder an unlimited number of times, independent of available drive letters.

1. Click **Start**, and then click **Run**.
2. In the **Run** dialog box, enter a UNC path, and then click **OK**.

   When you enter the server name, a list of available shared folders appears. Windows Server 2003 gives you the option to choose one of the entries based on the shared folders that are available to you.

Practice: Managing Access to Shared Folders



Objective

In this practice, you will create a shared folder, grant Read and Full Control permissions to two separate groups, and test the permissions.

Instructions

Before you begin this practice:

- Log on to the domain as *ComputerName*Admin.

> **Note** You cannot use the **Run as** command with Windows Explorer, so you must log on as *ComputerName*Admin to have the permissions that you need to complete this practice.

- Ensure that CustomMMC contains Computer Management (Local).
- Review the procedures in this lesson that describe how to perform this task.

Scenario

You have been asked to create a shared folder for the Human Resources department. The Human Resources department needs a shared folder for which Human Resources personnel will have Full Control permissions and all Accounting managers will have read access. You must create the shared folder with the proper permissions to meet the needs of the Human Resources personnel and Accounting managers.

Practice

► Create a shared folder

- Using Computer Management, create a shared folder on your student computer with the following parameters:
  - Folder location: D:\
  - Folder name: **HR Reports**
  - Security:
    - Grant Full Control permissions to DL NWTraders HR Personnel Full Control
    - Grant Read permissions to DL NWTraders Accounting Managers Read
    - Remove the Everyone group

► Test Read permissions of the shared folder

1. Log on as **AccountingManager** with a password of **P@ssw0rd**.
2. Connect to the shared folder *ComputerName*\HR Reports.
3. Try to create a text file in the HR Reports folder.

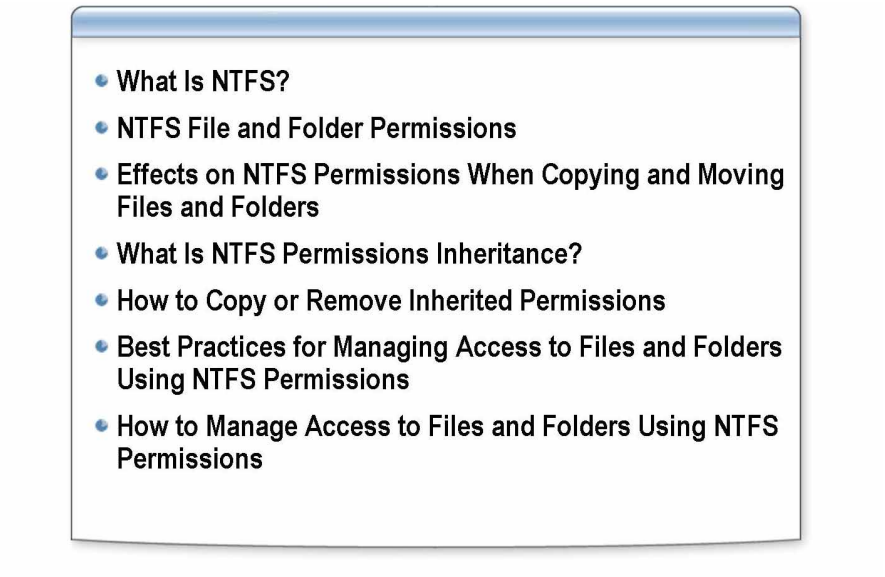
   You *should not* be able to create a text file in the shared folder.

► Test Full Control permissions of the shared folder

1. Log on as **HRUser** with a password of **P@ssw0rd**.
2. Connect to the shared folder *ComputerName*\HR Reports.
3. Try to create a text file in the HR Reports folder.

   You *should* be able to access the shared folder.

Lesson: Managing Access to Files and Folders Using NTFS Permissions



Introduction

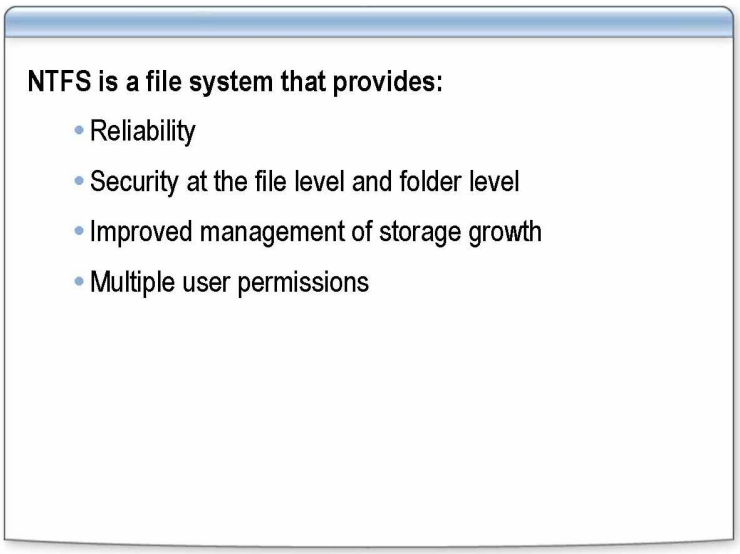
The information in this lesson presents the skills and knowledge that you need to manage access to files and folders by using NTFS permissions.

Lesson objectives

After completing this lesson, you will be able to:

- 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?



Introduction

NTFS is a file system that is available on Windows Server 2003. NTFS provides performance and features that are not found in either FAT (file allocation table) or FAT32.

Benefits of NTFS

NTFS provides the following benefits:

- 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. If EFS is enabled, files and folders can be encrypted for use by single or multiple users. The benefits of encryption are data confidentiality and data integrity, which means that data is protected against malicious or accidental modification. NTFS also enables you to set access permissions on a file or folder. Permissions can be set to Read, Read and Write, or Deny.

  NTFS also stores an access control list (ACL) with every file and folder on an NTFS partition. The ACL contains a list of all user accounts, groups, and computers that are granted access for the file or folder and the type of access that they are granted. For a user to access a file or folder, the ACL must contain an entry, called an ACE, for the user account, group, or computer that the user is associated with. The ACE must specifically allow the type of access the user is requesting for the user to access the file or folder. If no ACE exists in the ACL, Windows Server 2003 denies the user access to the resource.

- Improved management of storage growth

  NTFS supports disk quotas, which enable you to specify the amount of disk space that is available to a user. By using disk quotas, you can track and control disk space usage and configure whether users are allowed to exceed a warning level or storage quota limit.

  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. For example, a 30-gigabyte (GB) NTFS volume uses four-kilobyte (KB) clusters. The same volume formatted with FAT32 uses 16-KB clusters. Using smaller clusters reduces wasted space on hard disks.

- Multiple user permissions

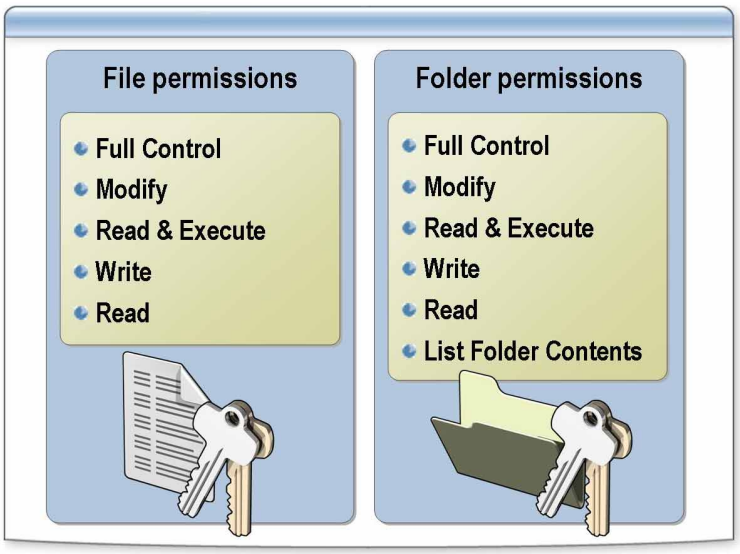
  If you grant NTFS permissions to an individual user account and to a group to which the user belongs, then you grant multiple permissions to the user. There are rules for how NTFS combines these multiple permissions to produce the user's effective permissions.

Additional reading

For more information on NTFS, see "NTFS" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/ntfs.asp.

For more information on FAT and NTFS, see "Choosing Between FAT and NTFS" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/ittasks/deploy/fat.asp.

NTFS File and Folder Permissions



Introduction

NTFS permissions are used to specify which users, groups, and computers can access files and folders. NTFS permissions also dictate what users, groups, and computers can do with the contents of the file or folder.

NTFS file permissions

The following table lists the standard NTFS file permissions that you can grant and the type of access that each permission provides.

NTFS file permission	Allows the user to:
Full Control	Change permissions, take ownership, and perform the actions permitted by all other NTFS file permissions
Modify	Modify and delete the file and perform the actions permitted by the Write permission and the Read & Execute permission
Read & Execute	Run applications and perform the actions permitted by the Read permission
Write	Overwrite the file, change file attributes, and view file ownership and permissions
Read	Read the file and view file attributes, ownership, and permissions

NTFS folder permissions

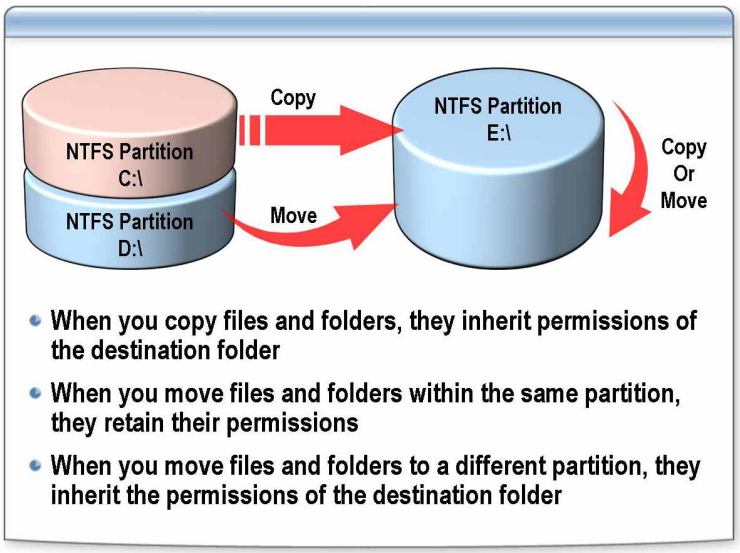
Permissions control access to folders and the files and subfolders that are contained in those folders. The following table lists the standard NTFS folder permissions that you can grant and the type of access that each permission provides.

NTFS folder permission	Allows the user to:
Full Control	Change permissions, take ownership, delete subfolders and files, and perform actions permitted by all other NTFS folder permissions
Modify	Delete the folder and perform actions permitted by the Write permission and the Read & Execute permission
Read & Execute	Traverse folders and perform actions permitted by the Read permission and the List Folder Contents permission
Write	Create new files and subfolders in the folder, change folder attributes, and view folder ownership and permissions
Read	View files and subfolders in the folder, folder attributes, ownership, and permissions
List Folder Contents	View the names of files and subfolders in the folder

Additional reading

For more information about permissions, see “Permissions” at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_sfmhowworks_13.asp.

Effects on NTFS Permissions When Copying and Moving Files and Folders



Introduction

When you copy or move a file or folder, the permissions may change depending on where you move the file or folder. It is important to understand the changes that the permissions undergo when being copied or moved.

Effects of copying files and folders

When you copy files or folders from one folder to another folder, or from one partition to another partition, permissions for the files or folders may change. Copying a file or folder has the following effects on NTFS permissions:

- When you copy a folder or file within a single NTFS partition, the copy of the folder or file inherits the permissions of the destination folder.
- When you copy a folder or file to a different NTFS partition, the copy of the folder or file inherits the permissions of the destination folder.
- 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.

Effects of moving files and folders

To copy files and folders within a single NTFS partition or between NTFS partitions, you must have Read permission for the source folder and Write permission for the destination folder.

When you move a file or folder, permissions may change, depending on the permissions of the destination folder. Moving a file or folder has the following effects on NTFS permissions:

- When you move a folder or file within an NTFS partition, the folder or file retains its original permissions.
- When you move a folder or file to a different NTFS partition, the folder or file inherits the permissions of the destination folder. When you move a folder or file between partitions, Windows Server 2003 copies the folder or file to the new location and then deletes it from the old location.
- 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.

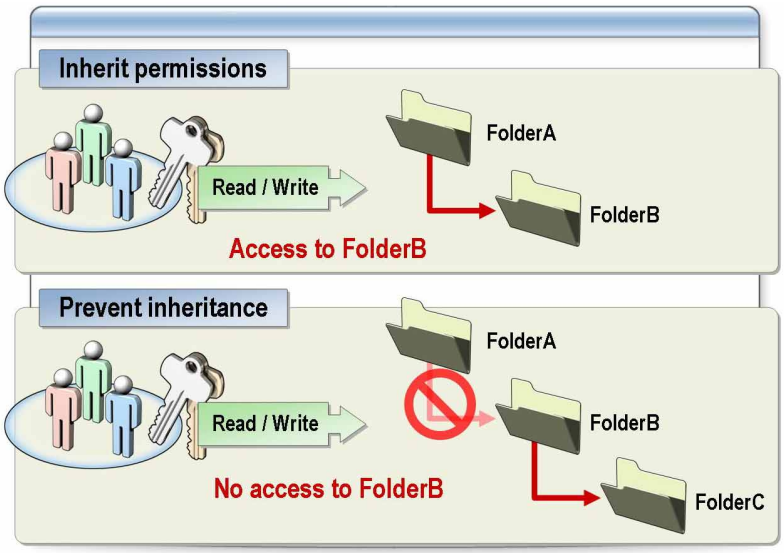
To move files and folders within an NTFS partition or between NTFS partitions, you must have both Write permission for the destination folder and Modify permission for the source folder or file. The Modify permission is required to move a folder or file, because Windows Server 2003 removes the folder or file from the source folder after it copies it to the destination folder.

Effects of copying and moving within volumes

The following table lists the possible copy and move options and describes how Windows Server 2003 treats the compression state of a file or folder.

Action	Result
Copy a file or folder within a volume	Inherits compression state of the destination folder
Move a file or folder within a volume	Retains original compression state of the source
Copy a file or folder between volumes	Inherits compression state of the destination folder
Move a file or folder between volumes	Inherits compression state of source file or folder

What Is NTFS Permissions Inheritance?



Definition

By default, permissions that you grant to a parent folder are inherited by the subfolders and files that are contained in the parent folder. When you create files and folders, and when you format a partition with NTFS, Windows Server 2003 automatically assigns default NTFS permissions.

Controlling permissions inheritance

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.

  - or -

- Remove the inherited permissions and retain only the permissions that were explicitly assigned.

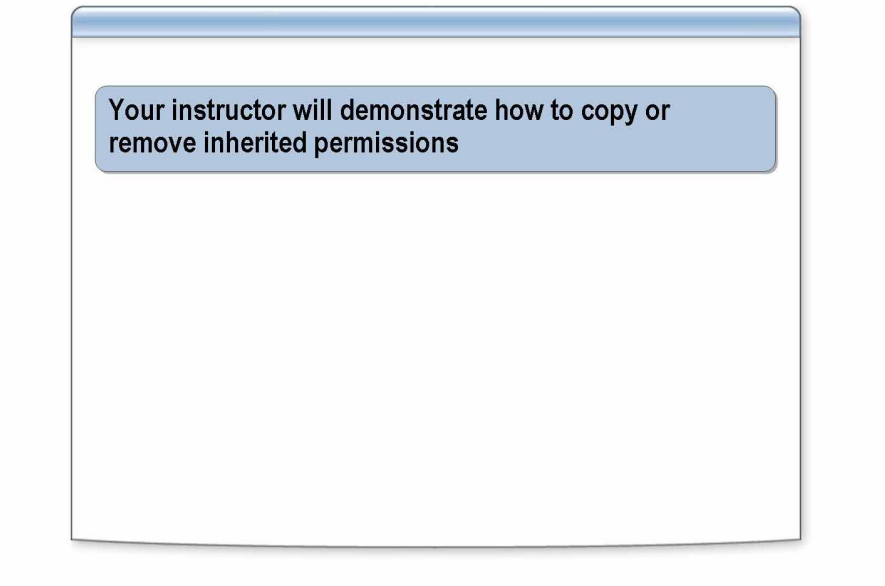
The folder at which you prevent permissions inheritance becomes the new parent folder, and the subfolders and files that are contained in it inherit the permissions assigned to it.

Why prevent propagating permissions?

Permissions inheritance simplifies how permissions for parent folders, subfolders, and resources are assigned. However, you may want to prevent inheritance so that permissions do not propagate from a parent folder to subfolders and files.

For example, you may need to keep all Sales department files in one Sales folder for which everyone in the Sales department has Write permission. However, for a few files in the folder, you may need to limit the permissions to Read. To do so, prevent inheritance so that the Write permission does not propagate to the files contained in the folder.

How to Copy or Remove Inherited Permissions



Introduction

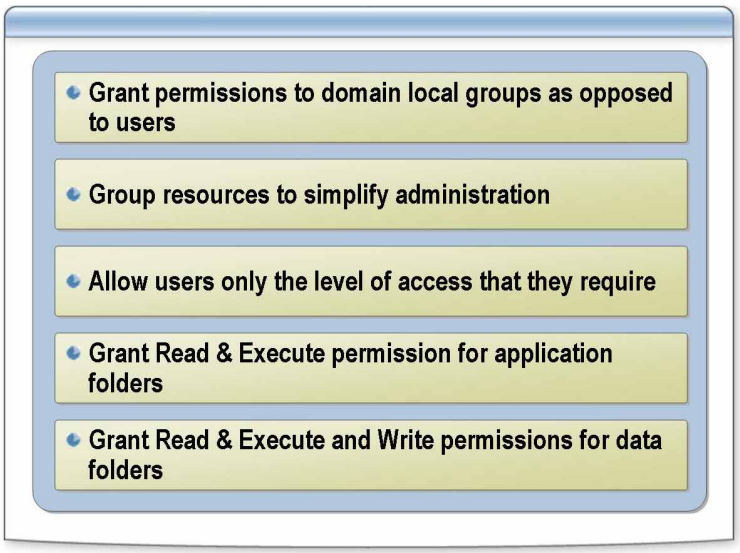
Use the following procedure to copy or remove inherited permissions.

Procedure

To copy or remove inherited permissions:

1. In Windows Explorer, right-click the file or folder you want to change inherited permissions on, and then click **Properties**.
2. In the **Properties** dialog box, on the **Security** tab, click **Advanced**.
3. In the **Advanced Security Settings** dialog box, clear the check box labeled **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here**.
4. In the **Security** dialog box, click one of the following:
   - Click **Copy** to copy the permission entries that were previously applied from the parent to this object.
   - Click **Remove** to remove permission entries that were previously applied from the parent and keep only those permissions explicitly assigned.
5. In the **Advanced Security Settings** dialog box, click **OK**.
6. In the **Properties** dialog box, click **OK**.

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



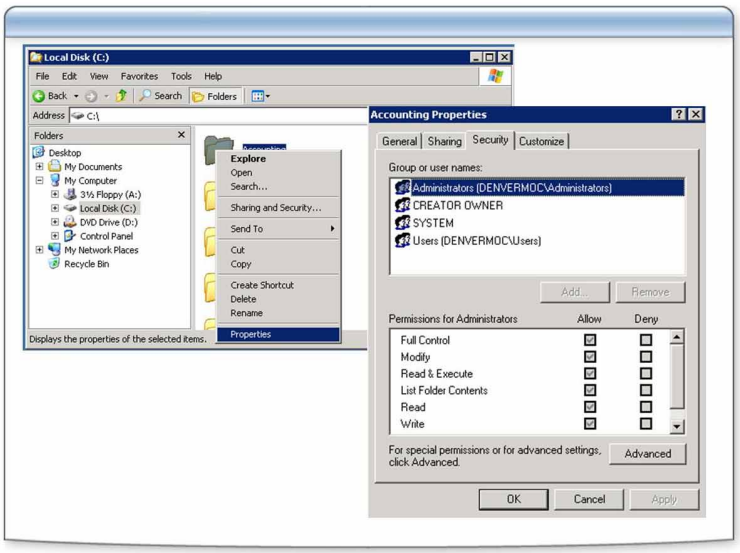
Best practices

When managing access to files and folders, consider the following best practices when granting NTFS permissions:

- Grant permissions to groups instead of users. Because it is inefficient to maintain user accounts directly, avoid granting permissions to individual users.
- Use Deny permissions in the following situations:
  - To exclude a subset of a group that has Allow permissions
  - To exclude one permission when you have already granted Full Control permissions to a user or group
- If possible, do not change the default permission entries for file system objects, particularly on system folders and root folders. Changing default permissions can cause unexpected access problems or reduce security.
- Never deny the Everyone group access to an object. If you deny everyone access to an object, you deny administrators access. Instead, it is recommended that you remove the Everyone group, as long as you grant permissions for the object to other users, groups, or computers.
- Grant permissions to an object that is as high on the tree as possible so that the security settings are propagated throughout the tree. You can quickly and effectively grant permissions to all children or a subtree of a parent object. By doing this, you affect the most objects with the least effort. Grant permissions that are adequate for the majority of users, groups, and computers.

- To simplify administration, group files according to function, for example:
  - Group program files into folders where commonly used applications are kept.
  - Group data folders containing home folders into one folder.
  - Group data files that are shared by multiple users into one folder.
- Grant the Read & Execute permission to the Users and Administrators groups for application folders. This prevents users or viruses from accidentally deleting or damaging data and application files.
- Only allow users the level of access that they require. For example, if a user only needs to read a file, grant the Read permission for the file to the user or group to which the user belongs.
- Grant the Read & Execute and Write permissions to the Users group and the Modify permission to the Creator Owner group for data folders. This enables users to read and modify documents that other users create and to read, modify, and delete the files and folders that they themselves create.

How to Manage Access to Files and Folders Using NTFS Permissions



Introduction

Use the follow procedure to change standard and special permissions for files and folders.

Procedure for changing standard permissions

To change standard permissions:

1. In Windows Explorer, right-click the file or folder for which you want to grant permissions, and then click **Properties**.
2. In the **Properties** dialog box, on the **Security** tab, do one of the following:
   - To grant permissions to a group or user that does not appear in the **Group or user names** box, click **Add**. In the **Select users, computers, or groups** dialog box, in the **Enter object names to select** box, type the name of the group or user you want to grant permissions to, and then click **OK**.
   - To change or remove permissions from an existing group or user, in the **Group or user names** box, click the name of the group or user, and then do one of the following:
     - To allow or deny permission, in the **Permissions for** box, select the **Allow** or **Deny** check box.
     - To remove the group or user from the **Group or user names** box, click **Remove**.

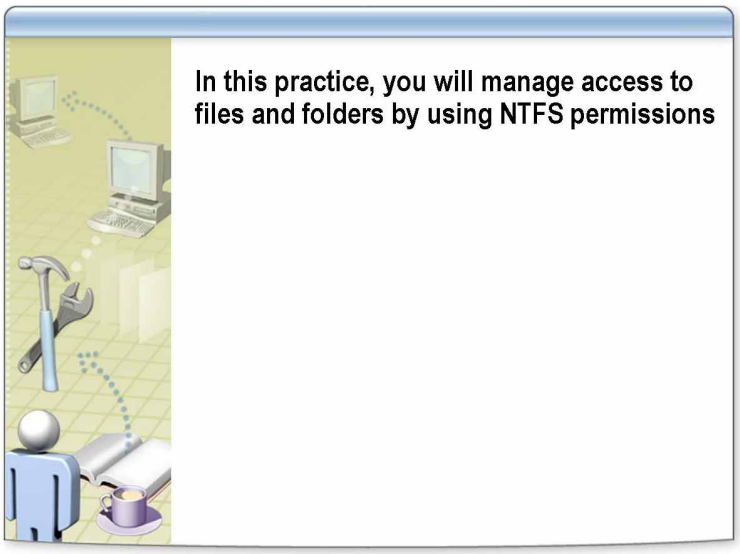
Procedure for changing special permissions

To change special permissions:

1. In Windows Explorer, right-click the object for which you want to grant special permissions, and then click **Properties**.
2. In the **Properties** dialog box, on the **Security** tab, click **Advanced**.
3. In the **Advanced Security Settings** dialog box, do one of the following:
   - To grant special permissions to an additional group or user, click **Add**. In the **Select user, computer, or group** dialog box, in the **Enter object name to select** box, type the name of the user or group, and then click **OK**.
   - To view or change special permissions for an existing group or user, click the name of the group or user, and then click **Edit**.
4. In the **Permissions Entry** dialog box, select or clear the appropriate **Allow** or **Deny** check box.
5. In the **Apply onto** drop down list, click the folders or subfolders you want these permissions to be applied to.
6. To configure security so that the subfolders and files do not inherit these permissions, clear the **Apply these permissions to objects and/or containers within this container only** check box.
7. Click **OK** and then, in the **Advanced Security Settings** dialog box, click **OK**.

Note To remove an existing group or user and its special permissions, click the name of the group or user, and then click **Remove**. If the **Remove** button is unavailable, clear the **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here** check box, and then click **Copy** or **Remove**.

Practice: Managing Access to Files and Folders Using NTFS Permissions



Objective

In this practice, you will manage access to files and folders by using NTFS permissions.

Instructions

Before you begin this practice:

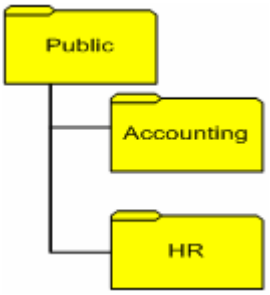
- Log on to the domain as *ComputerName*Admin.

> **Note** You cannot use the **Run as** command with Windows Explorer, so you must log on as *ComputerName*Admin to have the permissions that you need to complete this practice.

- Review the procedures in this lesson that describe how to perform this task.

Scenario

Northwind Traders wants you to create a shared folder called Public that is accessible to the Accounting department and the Human Resources 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

► **Share the Public folder**

1. Create and share the folder D:\Public.
2. Configure the Authenticated Users group to have Change permission for the D:\Public folder.
3. Remove the Everyone group.

► **Create folders according to the diagram**

1. Create the folder D:\Public\Accounting.
2. Create the folder D:\Public\HR.

► Configure NTFS permissions

- Remove all inherited permissions in the following folders and apply the permissions only to the folder. Do not let subfolders inherit 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

► Test the NTFS permissions

1. Log on as **HRUser** with a password of **P@ssw0rd**.
2. Attempt to access *ComputerName*\Public\Accounting.

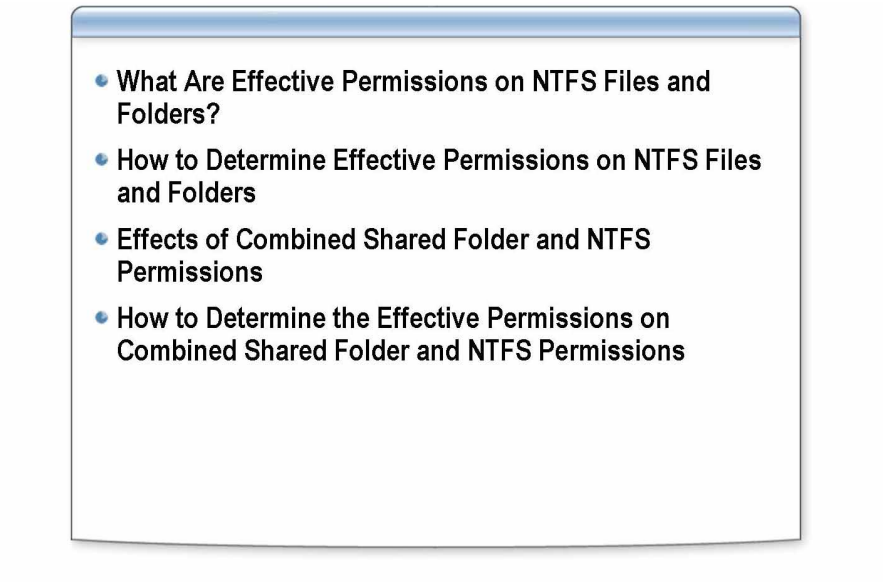
   You should *not* be able to access the Accounting folder. If you can access the folder, check that there are no NTFS permissions granted to Authenticated Users for the Accounting folder.
3. Attempt to Connect to D:\Public\Accounting.

   You should *not* be able to access the Accounting folder. If you can access the folder, check that there are no NTFS permissions granted to Authenticated Users for the Accounting folder.
4. Connect to *ComputerName*\Public\HR.

   You *should* be able to access the HR folder. If you cannot access the folder, check that the DL NWTraders HR Personnel Full Control group has NTFS Full Control permissions granted to the HR folder.
5. Connect to D:\Public\HR.

   You *should* be able to access the HR folder. If you cannot access the folder, check that the DL NWTraders HR Personnel Full Control group has NTFS Full Control permissions granted to the HR folder.

Lesson: Determining Effective Permissions



Introduction

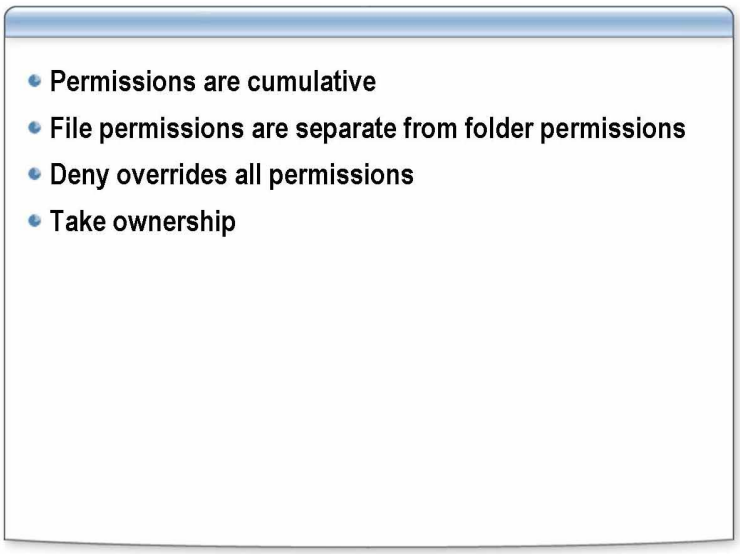
If you grant NTFS permissions to an individual user account and a group to which the user belongs, then you grant multiple permissions to the user. There are rules for how NTFS combines these multiple permissions to produce the user's effective permissions.

Lesson objectives

After completing this lesson, you will be able to:

- 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?



Introduction

Windows Server 2003 provides a tool that shows effective permissions, which are cumulative permissions based on group membership. The information is calculated from the existing permissions entries and is displayed in a read-only format.

Characteristics

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.

Important An administrator who needs to repair or change permissions on a file must take ownership of the file.

Ownership

By default, in the Windows Server 2003 family, the owner is the Administrators group. The owner can always change permissions on an object, even when denied all access to the object.

Ownership can be taken by:

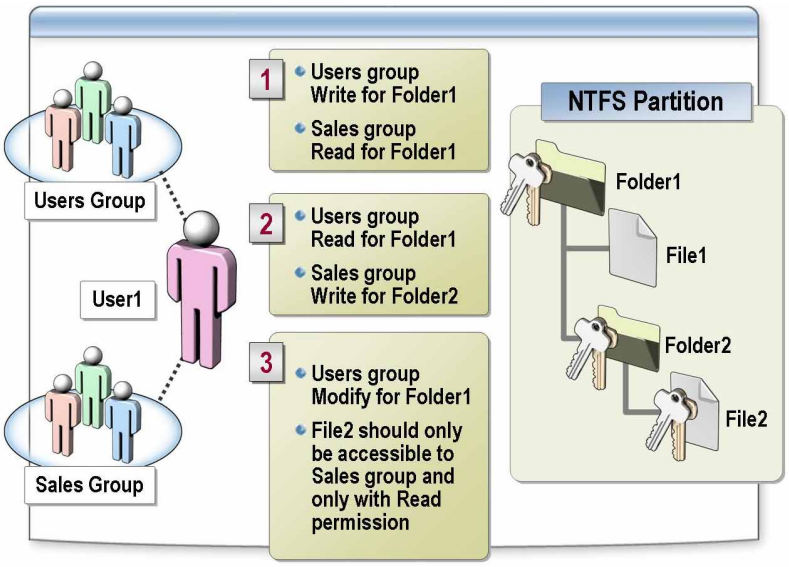
- An administrator. By default, the Administrators group is given the **Take ownership of files or other objects** user right.
- Anyone or any group who has the **Take ownership** permission for the object in question.
- A user who has the **Restore files and directories** privilege.

Ownership can be transferred in the following ways:

- The current owner can grant the **Take ownership** permission to another user. The user must actually take ownership to complete the transfer.
- An administrator can take ownership.
- A user who has the **Restore files and directories** privilege can double-click **Other users and groups** and choose any user or group to assign ownership to.

Important Permissions on a shared folder are not part of the effective permissions calculation. Access to shared folders can be denied though shared folder permissions even when access is allowed through NTFS permissions.

Class Discussion: Applying NTFS Permissions



Introduction

In this exercise, you are presented with a scenario where you are asked to apply NTFS permissions. You and your classmates will discuss possible solutions to the scenario.

Discussion

User1 is a member of the Users group and the Sales group.

1. The Users group has Write permission and the Sales group has Read permission for Folder1. What permissions does User1 have for Folder1?

   _____

   _____

2. The Users group has Read permission for Folder1. The Sales group has Write permission for Folder2. What permissions does User1 have for File2?

   _____

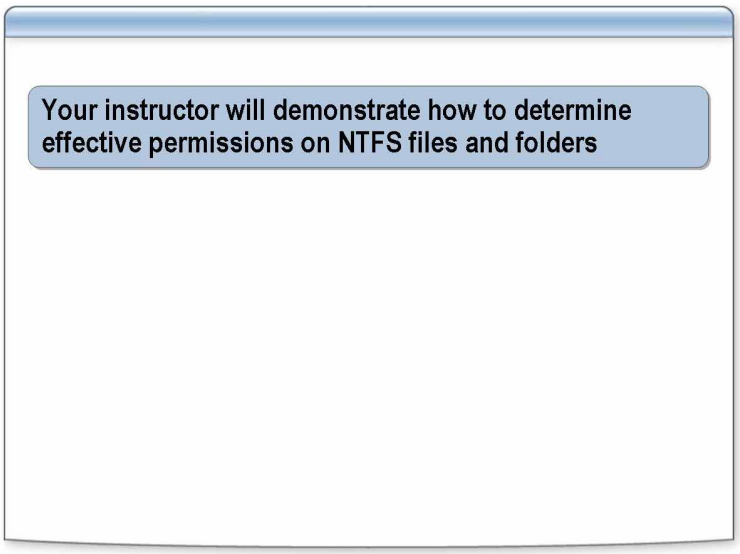
   _____

3. The Users group has Modify permission for Folder1. File2 should only be accessible to the Sales group, and they should only be able to read File2. What do you do to ensure that the Sales group has only Read permission for File2?

_____

_____

How to Determine Effective Permissions on NTFS Files and Folders



Introduction

Use the following procedure to view the effective permissions for files and folders.

Procedure

To view the effective permissions for files and folders:

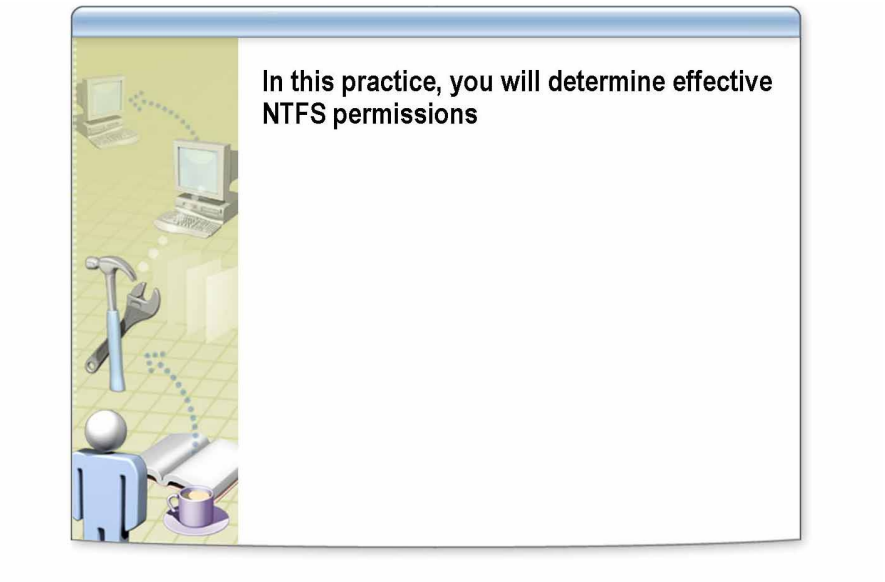
1. In Windows Explorer, right-click the file or folder for which you want to view effective permissions, and then click **Properties**.
2. In the **Properties** dialog box, on the **Security** tab, click **Advanced**.
3. In the **Advanced Security Settings** dialog box, on the **Effective Permissions** tab, click **Select**.
4. 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, and then click **OK**.

   The selected check boxes in the **Advanced Security Settings** dialog box indicate the effective permissions of the user or group for that file or folder.

Additional reading

For more information about effective permissions, see “Effective Permission tool” at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/acl_effective_perm.asp.

Practice: Determining Effective Permissions on NTFS Files and Folders



Objective

In this practice, you will determine the effective NTFS permissions.

Instructions

Before you begin this practice:

- Log on to the domain as *ComputerName*Admin.

> **Note** You cannot use the **Run as** command with Windows Explorer, so you must log on as *ComputerName*Admin to have the permissions that you need to complete this practice.

- Review the procedures in this lesson that describe how to perform this task.

Scenario

The HR Manager for your city calls you and wants to know if they have the permissions to create documents in the *ComputerName*\Public\HR folder and what permissions a user called TelemarketingUser has for the HR folder.

Practice

► **Determine effective permissions for HRManager**

1. Navigate to *ComputerName*\Public\HR.
2. Determine effective permissions for the HRManager user account.
3. Write the highest permissions granted to HRManager

_____

_____

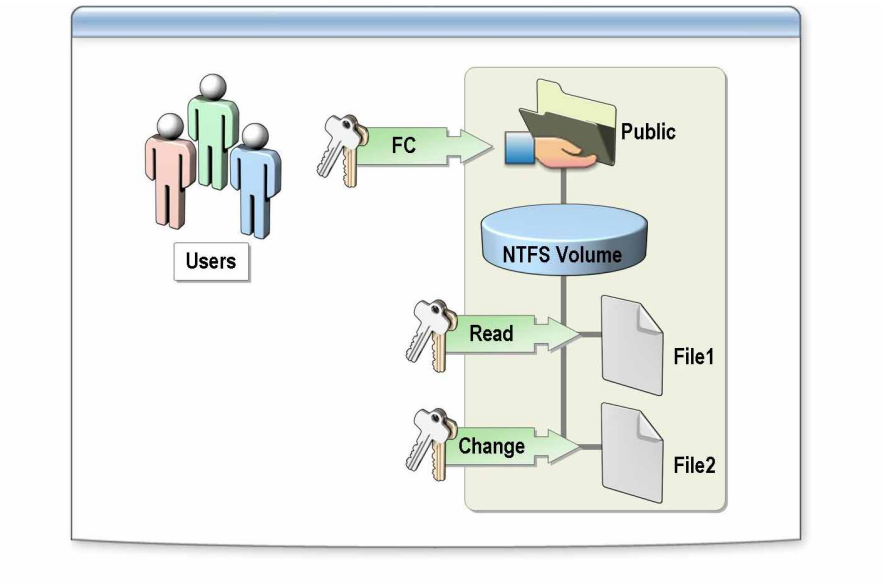
► **Determine effective permissions for TelemarketingUser**

1. Navigate to *ComputerName*\Public\HR.
2. Determine effective permissions for the Telemarketing user account.
3. Write the highest permissions granted to TelemarketingUser.

_____

_____

Effects of Combined Shared Folder and NTFS Permissions



Introduction

When allowing access to network resources on an NTFS volume, it is recommended that you use the most restrictive NTFS permissions to control access to folders and files, combined with the most restrictive shared folder permissions that control network access.

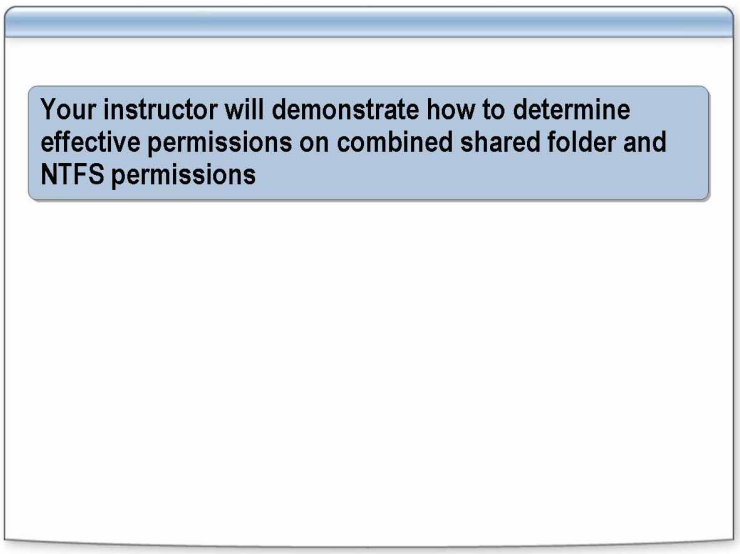
What are combined permissions?

When you create a shared folder on a partition formatted with NTFS, both the shared folder permissions and the NTFS permissions combine to secure file resources. NTFS permissions apply whether the resource is accessed locally or over a network.

When you grant shared folder permissions on an NTFS volume, the following rules apply:

- NTFS permissions are required on NTFS volumes. By default, the Everyone groups has Read permission.
- Users must have the appropriate NTFS permissions for each file and subfolder in a shared folder, in addition to the appropriate shared folder permissions, to access those resources.
- When you combine NTFS permissions and shared folder permissions, the resulting permission is the most restrictive permission of the combined shared folder permissions or the combined NTFS permissions.

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



Introduction

Use Windows Explorer to view effective permissions on shared folders. To determine effective permissions, you need to first determine the maximum NTFS and the shared folder permissions and then compare the permissions.

Procedure for determining maximum NTFS permissions

To determine the maximum permissions a user has for a file on an NTFS volume:

1. In Windows Explorer, locate the file or folder for which you want to view effective permissions.
2. Right-click the file or folder, and then click **Properties**.
3. In the **Properties** dialog box, on the **Security** tab, click **Advanced**.
4. In the **Advanced Security Settings** dialog box, on the **Effective Permissions** tab, click **Select**.
5. In the **Select User, Computer, or Group** dialog box, in the **Enter the object name to select (examples)** box, enter the name of a user or group, and then click **OK**.

   The selected check boxes indicate the maximum NTFS permissions that a user or group has for a file or folder.

Procedure for determining maximum shared folder permissions

To determine the maximum permissions a user has for a shared folder:

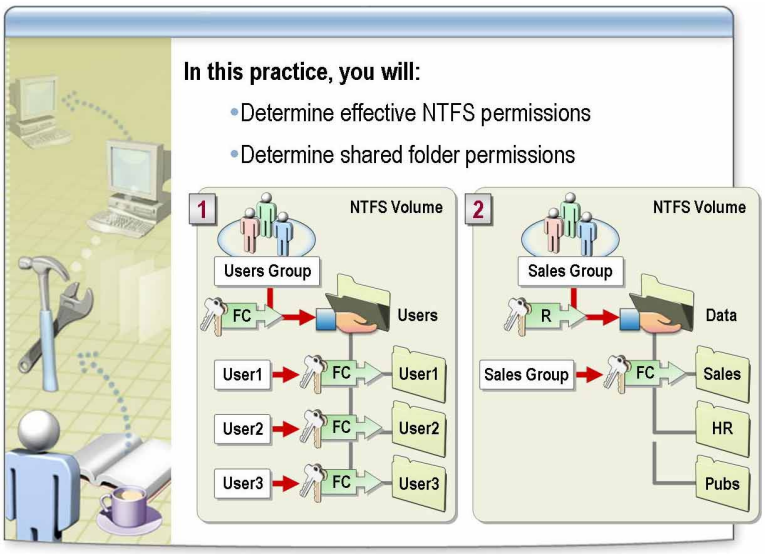
1. Open the **Properties** dialog box for the shared folder.
2. Find the maximum permissions the user has to the share by determining what groups the user belongs to.

Procedure for determining effective permissions

To determine the effective permissions for a shared folder:

1. Compare the maximum NTFS permissions with the maximum shared folder permissions.
2. 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



Objective

In this practice, you will determine the effective NTFS and shared folder permissions.

Class discussion

The graphic on this page illustrates two shared folders that contain folders or files that have been assigned NTFS permissions. Look at each example and determine a user's *effective* permissions.

1. In the first example, the Users folder has been shared, and the Users group has the shared folder permission Full Control. User1, User2, and User3 have been granted the NTFS permission Full Control to *only* their folder. These users are all members of the Users group.

   Do members of the Users group have Full Control to *all* home folders in the Users folder once they connect to the Users shared folder?

   _____

   _____

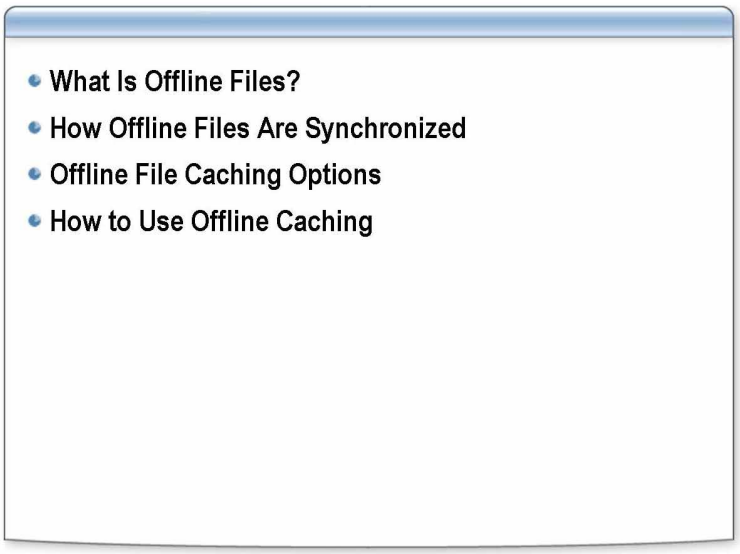
2. In the second example, the Data folder has been shared. The Sales group has been granted the shared folder permission Read for the Data shared folder and the NTFS permission Full Control for the Sales folder.

   What are the Sales group's effective permissions when they access the Sales folder by connecting to the Data shared folder?

   _____

   _____

Lesson: Managing Access to Shared Files Using Offline Caching



Introduction

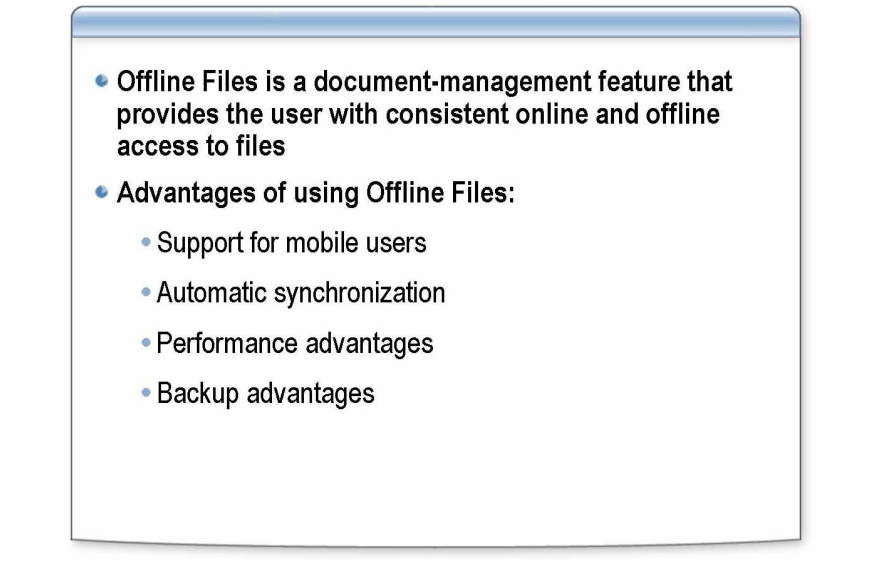
The information in this lesson presents the skills and knowledge that you need to manage access to shared files by using offline caching.

Lesson objectives

After completing this lesson, you will be able to:

- Explain what Offline Files is.
- Explain how offline files are synchronized.
- Explain the offline file caching modes.
- Use offline caching.

What Is Offline Files?



Definition

Offline Files is an important document-management feature that provides the user with consistent online and offline access to files. When the client disconnects from the network, anything that has been downloaded to the local cache remains available. Users can continue working as though they were still connected to the network. They can continue editing, copying, deleting, and so forth.

From the user's perspective, the workspaces appear identical, whether they are on or off the network. Visual cues, such as icons, menus, and Active Directory, remain the same, including the view of the mapped network drives. Network files appear in the same network drive directory and can be accessed, copied, edited, printed, or deleted precisely as they are when they are online. When you reconnect to the network, client and server files are automatically resynchronized.

Advantages of using Offline Files

Using Offline Files has the following advantages:

- Support for mobile users

  When a mobile user views the shared folder while disconnected, the user can still browse, read, and edit files, because they have been cached on the client computer. When the user later connects to the server, the system reconciles the changes with the server.

- Automatic synchronization

  You can configure synchronization policy and behavior based on the time of day and network connection type by using Synchronization Manager. For example, you can configure synchronization so that it occurs automatically when the user logs on to a direct local area network (LAN) connection, but only at a user's request when he or she uses a dial-up connection.

- Performance advantages

  Offline Files provides performance advantages for networks. While connected to the network, clients can still read files from the local cache, reducing the amount of data transferred over the network.

- Backup advantages

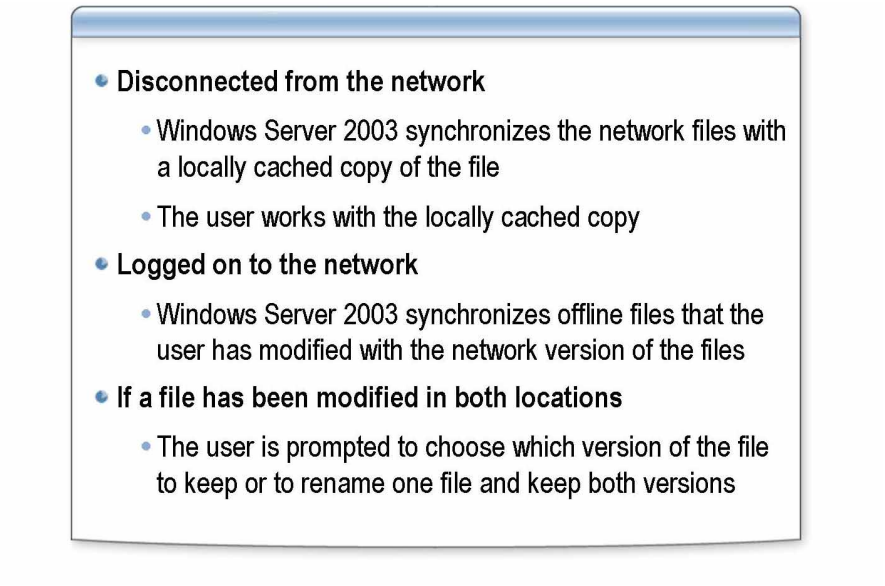
  Offline Files solves a dilemma facing most enterprise organizations today. Many organizations implement a backup policy that requires all user data to be stored on managed servers. The organization's IT department often does not back up data stored on local disks. This becomes a problem for mobile users of portable computers.

  If you want to access data when offline, a mechanism is needed to replicate data between the portable computer and the servers. Some organizations use the Briefcase tool. Others use batch files or replicate data manually. With Windows Server 2003, replication between client and server is managed automatically. Files can be accessed while offline and are automatically synchronized with the managed server.

Additional reading

For more information about offline file security, see "Securing Offline Files" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prdc_mcc_lvvu.asp.

How Offline Files Are Synchronized



Introduction

A user can configure a file on a network to be available offline, provided that Offline Files is enabled for the folder in which the file resides. When users configure files to be available offline, the users work with the network version of the files while they are connected to the network and then with a locally cached version of the files when they are not connected to the network.

Synchronization events

When a user configures a file to be available offline, the following synchronization events occur when the user disconnects from the network:

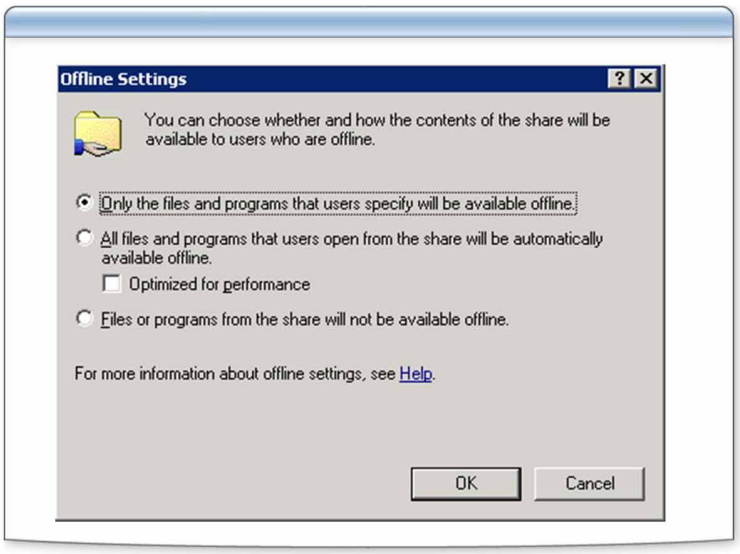
- When the user logs off the network, the Windows client operating system synchronizes the network files with a locally cached copy of the file.
- While the computer is disconnected from the network, the user works with the locally cached copy of the file.
- When the user again logs on to the network, the Windows client operating system synchronizes any offline file that the user has modified with the network version of the file. If the file has been modified on both the network and the user's computer, the Windows client operating system prompts the user to choose which version of the file to keep, or the user can rename one file and keep both versions.

Important Using offline files is not a substitute for document version control. If two users work with the same offline file at the same time, and then synchronize the file with the network version, one of the versions may be lost.

Additional reading

For more information about how clients synchronize offline files, see "Offline Files overview" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/csc_overview.asp.

Offline File Caching Options



Introduction

Offline Files caches files that are often accessed from a shared folder. This is similar to the way in which a Web browser keeps a cache of recently visited Web sites. When you create shared folders on the network, you can specify the caching option for the files and programs in that folder. There are three different caching options.

Manual caching of documents

Manual caching of documents provides offline access for only the files and programs that the user specifies will be available. This caching option is ideal for a shared network folder containing files that several people will access and modify. This is the default option when you configure a shared folder to be available offline.

Automatic caching of documents

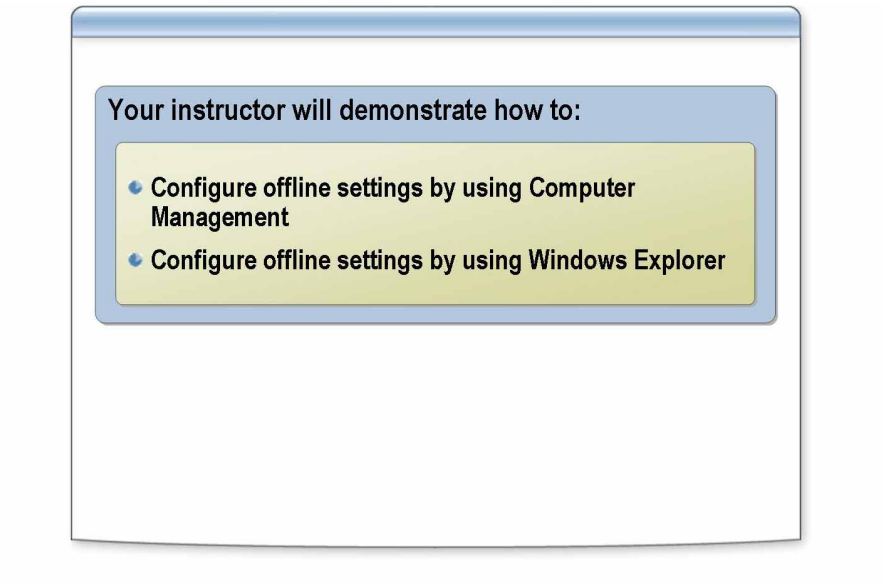
With automatic caching of documents, all files and programs that users open from the shared folder are automatically available offline. Files that the user does not open are not available offline. Older copies are automatically overwritten by newer versions of files.

Automatic caching of programs

When the **Optimized for performance** check box is selected, it provides automatic caching of programs, which provides offline access to shared folders containing files that are not to be changed. Automatic caching of programs reduces network traffic, because offline files are opened directly. The network versions are not accessed in any way, and the offline files generally start and run faster than the network versions.

When you use automatic caching of programs, be sure to restrict permissions for the files contained in the shared folders to Read access.

How to Use Offline Caching



Introduction

Use the following procedures to manage access to shared files by using offline caching.

Procedure using Computer Management

To configure offline settings by using Computer Management:

1. In Computer Management, in the console tree, expand **Shared Folders**, and then click **Shares**.
2. In the details pane, right-click the shared resource for which you want to configure offline settings, and then click **Properties**.
3. In the **Properties** dialog box, on the **General** tab, click **Offline Settings**.
4. In the **Offline Settings** dialog box, select the option that you want, and then click **OK**.

Procedure using Windows Explorer

To configure offline settings by using Windows Explorer:

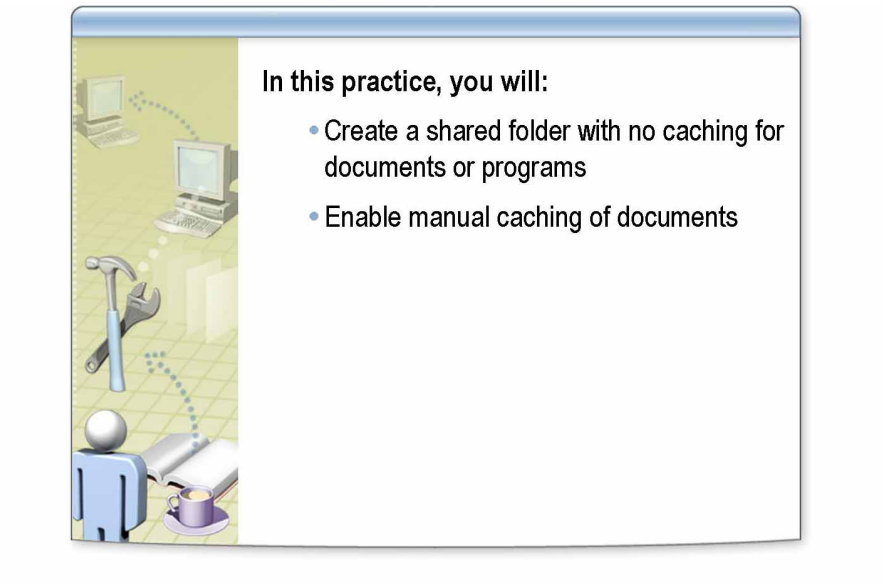
1. In Windows Explorer, right-click the shared folder or drive for which you want to configure offline access, and then click **Sharing and Security**.
2. In the **Properties** dialog box, on the **Sharing** tab, click **Offline Settings**.
3. In the **Offline Settings** dialog box, select the option that you want, and then click **OK**.

Using a command line

To configure offline settings by using **net share**:

1. Open a command prompt.
2. To configure manual caching, type
   net share *SharedFolderName* **/cache:manual**
3. To configure caching of documents, type
   net share *SharedFolderName* **/cache:documents**
4. To configure caching of programs, type
   net share *SharedFolderName* **/cache:programs**
5. To configure a shared folder to not cache, type
   net share *SharedFolderName* **/cache:none**

Practice: Using Offline Caching



Objective

In this practice, you will create a shared folder and use different caching options.

Instructions

Before you begin this practice:

- Log on to the domain as *ComputerName*Admin.

> **Note** You cannot use the **Run as** command with Windows Explorer, so you must log on as *ComputerName*Admin to have the permissions that you need to complete this practice.

- Review the procedures in this lesson that describe how to perform this task.

Scenario

The Human Resources department wants you to configure a shared folder that contains sensitive human resources data. Northwind Traders does not want this data to be cached on any desktop and laptop computer of Human Resources personnel.

Practice: Creating a shared folder with no caching

► **Create a shared folder with no caching for documents of programs**

1. Create a shared folder on the your student computer by using the following parameters:
   - Folder location: D:\
   - Folder name: **HR Confidential**
   - Share name: **HR Confidential**
2. Configure shared folder permissions as follows:
   - Grant Full Control permissions to DL NWTraders HR Personnel Full Control.
   - Remove the Everyone group.
3. Configure NTFS permissions as follows:
   - Remove all inherited NTFS permissions.
   - Grant Full Control permission to DL NWTraders HR Personnel Full Control.
   - Grant Full Control permission to *ComputerName*\Administrators.
4. Set the offline settings to **Files or programs from the share will not be available offline**.

Scenario

Corporate policy has changed and now states that all desktop and laptop computers must have only NTFS partitions, and all laptops of Human Resources personnel must use the EFS feature of NTFS. Your IT security team notifies the Human Resources department that they are now allowed to copy all sensitive Human Resources information for offline use.

Practice: Enabling manual caching of documents

► **Enable manual caching of documents**

- Enable manual caching of documents in the HR Confidential folder by changing the offline settings to **Only the files and programs that users specify will be available offline**.

Scenario

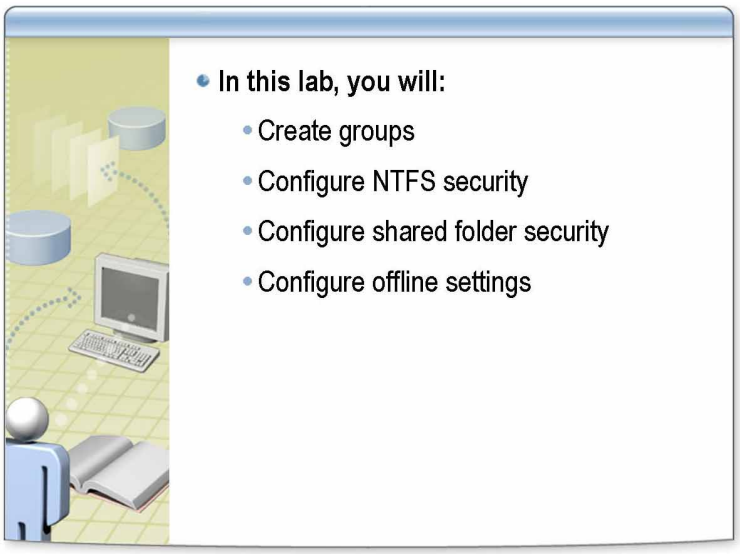
The Human Resources department uses a custom application based on Microsoft Visual Basic® that has a single executable file. For performance reasons, you want this file to run from the local hard drive. However, sometimes this application is updated, and you want this application to be automatically redeployed after it is updated. You decide to put this application on the server in your city organizational unit and use automatic caching for programs that is optimized for performance.

Practice: Enabling automatic caching of programs

► **Create a shared folder for the Human Resources department**

1. Create a share by using the following parameters:
   - Folder location: D:\
   - Folder name: **HR App**
   - Share name: **HR App**
2. Configure shared folder permissions as follows:
   - Grant Change permission to DL NWTraders HR Personnel Change.
   - Remove the Everyone group.
3. Configure NTFS permissions as follows:
   - Grant Change permission to DL NWTraders HR Personnel Change.
   - Grant Full Control permission to *ComputerName*\Administrators.
4. Set offline settings to **All files and programs that users open from the share will be automatically available offline** and **Optimized for performance**.

Lab A: Managing Access to Resources



Objectives

After completing this lab, you will be able to:

- Create groups.
- Configure NTFS security.
- Configure shared folder security.
- Configure offline settings.

Instructions

Before you begin this practice:

- Log on to the domain as *ComputerName*Admin.

> **Note** You cannot use the **Run as** command with Windows Explorer, so you must log on as *ComputerName*Admin to have the permissions that you need to complete this practice.

- Ensure that CustomMMC contains Computer Management (Glasgow).
- Review the procedures in this lesson that describe how to perform this task.

Estimated time to complete this lab: 30 minutes

Exercise 1
Configuring Access for Manufacturing Personnel

In this exercise, you will configure access for Manufacturing personnel.

Scenario

The Manufacturing managers in your city organizational unit need a shared folder for thousands of specification documents. These documents do not often change, but the managers need to be able to add, change, and delete documents. They want the Manufacturing personnel to only read the documents, without changing or deleting the files, and they want to have Change permission. Manufacturing personnel do not have any laptops and do require offline access to the documents. You must configure security, offline settings, and permissions for the Manufacturing personnel.

Tasks	Detailed Information
1. Create a shared folder.	▪ Tool: Computer Management (Glasgow) ▪ Server name: Glasgow ▪ Folder path: D:*ComputerName* Manufacturing ▪ Share name: *ComputerName* Manufacturing ▪ Shared folder permissions: • 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.	▪ 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
3. Set the offline caching settings.	▪ Clear the offline caching settings

Exercise 2
Configuring Access for Marketing Personnel

In this exercise, you will configure access for Marketing personnel.

Scenario

The Marketing department at Northwind Traders needs you to create a shared folder that will contain electronic catalog files. There will be hundreds of electronic catalog files that change quarterly, and the Marketing personnel need offline access to all catalog files. You must create a shared folder, configure security, offline settings, and permissions for Marketing personnel.

Tasks	Detailed Information
1. Create a shared folder.	▪ Tool: Computer Management (Glasgow) ▪ Server name: Glasgow ▪ Folder path: D:*ComputerName* Marketing ▪ Share name: *ComputerName* Marketing ▪ Shared folder permissions: • Grant Full Control to DL NWTraders Marketing Personnel Full Control • Grant Full Control GLASGOW\Administrators
2. Set the NTFS permissions.	▪ Grant Modify to DL Marketing Personnel Full Control ▪ Grant Full Control to GLASGOW\Administrators ▪ Copy all NTFS permissions inheritance
3. Set the offline caching settings.	▪ Enable automatic caching for documents

Exercise 3
Configure Access for Accounting Personnel

In this exercise, you will configure access for Accounting personnel.

Scenario

The Accounting department at Northwind Traders needs a shared folder for accounting policies and procedures so that everyone in the department can change the shared documents. Most of the Accounting personnel use laptops. They only need offline access to the policy and procedures that they open from the shared folder. You must create groups and configure security, offline settings, and permissions for the Accounting personnel.

Tasks	Detailed Information
1. Create a shared folder.	▪ Tool: Computer Management (Glasgow) ▪ Server name: Glasgow ▪ Folder path: D:\ComputerName Accounting ▪ Share name: ComputerName Accounting ▪ Shared folder permissions: • Grant Full Control to DL NWTraders Accounting Personnel Full Control • Grant Full Control to GLASGOW\Administrators
2. Set NTFS permissions.	▪ Grant Modify to DL ComputerName Accounting Personnel Full Control ▪ Grant Full Control to GLASGOW\Administrators ▪ Copy all NTFS permissions inheritance
3. Set the offline caching settings.	▪ Enable caching for files that the users opens from the shared folder