EXAM OBJECTIVES

Professional ▶

Exam 70-210

- Monitor, manage, and troubleshoot access to files and folders.
  - Configure, manage, and troubleshoot file compression.
  - Control access to files and folders by using permissions.
  - Optimize access to files and folders.
- Manage and troubleshoot access to shared folders.
  - Create and remove shared folders.
  - Control access to shared folders by using permissions.
- Connect to shared resources on a Microsoft network.
- Encrypt data on a hard disk by using Encrypting File System (EFS).

Server ▶

Exam 70-215

- Monitor, configure, troubleshoot, and control access to files, folders, and shared folders.
  - Configure, manage, and troubleshoot a stand-alone Distributed file system (Dfs).
  - Configure, manage, and troubleshoot a domain-based Distributed file system (Dfs).
  - Monitor, configure, troubleshoot, and control local security on files and folders.
  - Monitor, configure, troubleshoot, and control access to files and folders in a shared folder.
- Configure data compression.
- Monitor and configure disk quotas.
- Encrypt data on a hard disk by using Encrypting File System (EFS).

CHAPTER

11

Sharing, Securing, and Accessing Files and Folders

This chapter focuses on sharing, securing, and accessing network resources. After some introductory information about file and folder attributes, I'll get right to the nitty-gritty of sharing folders, including how to share folders, how to connect to shared folders, and how to work with shared folder permissions. Then I'll explore the Distributed file system (Dfs), and explain how you can use Dfs to make network resources easier for users to find, and accessible even if a server is down. Next, I'll explore NTFS permissions. I'll cover how to assign NTFS permissions to files and folders; how NTFS permissions are applied to new, moved, and copied files and folders; and how NTFS and share permissions interact. Then I'll show you how to take ownership of files and folders, how to configure and monitor disk quotas, and how to optimize access to files and folders. Finally, I'll provide you with some troubleshooting tips for common resource access and permission problems. In short, if it has to do with shared files and folders, you'll find it in this chapter.

Chapter Pre-Test

1. List the seven Windows 2000 file and folder attributes.
2. How does a shared folder appear in Windows Explorer?
3. User and group share permissions are _____ , and normally the _____ restrictive permission is the user's effective permission.
4. When NTFS and share permissions differ, the _____ restrictive permission becomes the user's effective permission to the file or folder in the share.
5. What volume management mechanism can you use to automatically track disk space usage on a user-by-user basis, and to prevent individual users from exceeding the disk space limitations they have been assigned by an Administrator?

Managing File and Folder Attributes

Windows 2000 files and folders have various properties, called *attributes*, some of which the administrator can use to provide a limited amount of data protection. Administrators or users assign many attributes to protect files and folders. Other file and folder attributes are automatically applied to system files during the installation of Windows 2000.

Windows 2000 File and Folder Attributes

There are seven Windows 2000 file and folder attributes. These file and folder attributes can be used on FAT, FAT32, and NTFS volumes, with the exception of the Compress, Encrypt, and Index attributes, which are available only on NTFS volumes.

Table 11-1 lists and describes the Windows 2000 file and folder attributes.

TABLE 11-1 Windows 2000 File and Folder Attributes

Attribute	Description
Archive	Indicates that the file or folder has been modified since the last backup. Is applied by the operating system when a file or folder is saved or created, and is commonly removed by backup programs after the file or folder has been backed up.
Compress	Indicates that Windows 2000 has compressed the file or folder. Is only available on NTFS volumes. Can be set by using Windows Explorer and by using the `compress` command-line utility. Can't be used in conjunction with the Encrypt attribute. In other words, a file can be encrypted or compressed, but not both. Is applied by administrators to control which files and folders will be compressed.
Encrypt	Indicates that Windows 2000 has encrypted the file or folder. Is only available on NTFS volumes. Can be set by using Windows Explorer and by using the `cipher` command-line utility. Can't be used in conjunction with the Compress attribute. Is applied by users and administrator to control which files and folders will be encrypted. Once a file or folder has been encrypted, only the user who encrypted the file or folder (or the Administrator) can open the file or folder and view its contents.

Continued

TABLE 11-1 *(continued)*

Attribute	Description
Hidden	Indicates that the file or folder can't be seen in a normal directory scan. Files or folders with this attribute can't be copied or deleted. Is automatically applied to various files and folders by Windows 2000 during installation. In addition, this attribute can be applied by administrators or users to hide and protect files and folders.
Index	Indicates that the file or folder is indexed by the Indexing Service. Is only available on NTFS volumes. Can be applied by administrators or users. Once this attribute has been applied to a file, users can use Windows Explorer to locate this file by searching for words or phrases contained in the file.
Read-only	Indicates that the file or folder can only be read—it can't be written to or deleted. Is often applied by administrators to prevent accidental deletion of application files.
System	Indicates that the file or folder is used by the operating system. Files or folders with this attribute can't be seen in a normal directory scan, and can't be copied or deleted. Can't be set by using Windows Explorer. You must use the `attrib` command-line utility to view or change this attribute. Is automatically applied to various files and folders by Windows 2000 during installation.

EXAM TIP

Both the Professional and Server exams have objectives on configuring file compression and data encryption. Pay special attention to both the Compress and Encrypt attributes.

Using the Compress Attribute

The Compress attribute is typically used to conserve disk space. You should only use this attribute on files or folders that are infrequently accessed because accessing a compressed file or folder uses more processor time (on the server that contains the file) than accessing an uncompressed file or folder. If a large number of users access compressed files on a server, that server's performance may be degraded. You can only compress files and folders on NTFS volumes.

Using the Encrypt Attribute

The Windows 2000 feature that provides the capability of the Encrypt attribute is called the *Encrypting File System (EFS)*. You don't need to install EFS—it's installed by default and is transparent to users. When users assign

the Encrypt attribute, that's all there is to it. EFS does all the work. As stated previously, the Encrypt attribute is only available for files and folders on NTFS volumes.

The Encrypt attribute is normally applied by a user to protect sensitive data that should be accessed only by that user. It is typically applied at the folder level, because when applied to a folder, Windows 2000 encrypts all of the files in the folder. When applied to an individual file, this attribute must be reapplied each time the file is modified.

As stated previously, in a Windows 2000 domain environment, only the user who encrypted the file and the domain's Administrator account can open the file. On a local Windows 2000 computer that is not a member of a domain, only the local user who encrypted the file and the local Administrator account can open the file. The Administrator account, in both of these situations, is called the *recovery agent* because this account is assigned a special key that permits it to unencrypt (that is, recover) all encrypted files on the computer. If you want to designate additional recovery agents, you can use Group Policy to specify additional users (on the local computer, in an OU, or in an entire domain) who can open all encrypted files and folders.

The Encrypt and Compress attributes are mutually exclusive — you can use one or the other, but not both, on a file or folder.

Using the Read-only Attribute

The Read-only attribute is frequently used to prevent the accidental deletion of application files. When a user has the Write NTFS permission to a Read-only file or folder on an NTFS volume, the Read-only attribute takes precedence. The Read-only attribute must be removed before the file or folder can be modified or deleted. (I'll cover NTFS permissions a little later in this chapter.)

Assigning Attributes to Files or Folders

Any user who can access a file or folder on a FAT or FAT32 volume can modify that file or folder's attributes. Any user who has the Write NTFS permission (or any permission that includes the functionality of the Write permission) to a file or folder on an NTFS volume can modify that file or folder's attributes.

Most file and folder attributes can be changed or assigned by using Windows Explorer, as the following steps explain.

STEP BY STEP

ASSIGNING FILE OR FOLDER ATTRIBUTES

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, expand folders as necessary until the file or folder to which you want to assign attributes is displayed in the right pane. In the right pane, highlight that file or folder. Select File ➪ Properties. (Or, right-click the file or folder, and select Properties from the menu that appears.)
3. The file or folder's Properties dialog box appears, as shown in Figure 11-1. Notice the attributes that you can assign on the General tab.

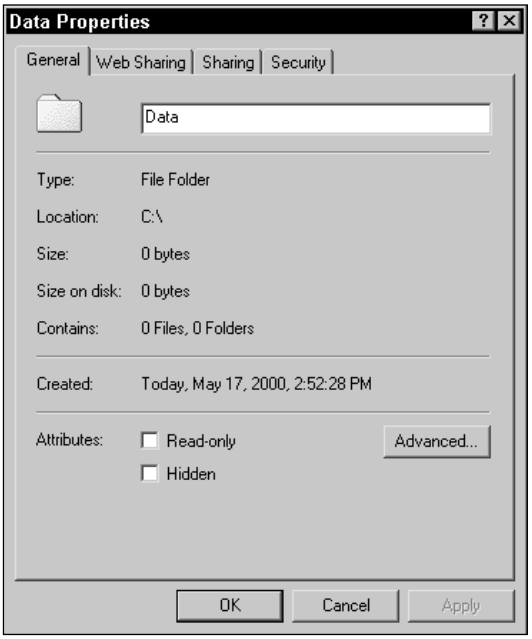

FIGURE 11-1 Setting file or folder attributes

If you want to assign the Read-only or Hidden attributes, select the check box next to the attribute you want to assign. To assign all other attributes, click Advanced.

TIP

Files and folders on FAT or FAT32 volumes don't have the Advanced command button, but do have an additional check box for the Archive attribute.

STEP BY STEP *Continued*

4. The Advanced Attributes dialog box appears, as shown in Figure 11-2. Notice that the Index attribute is selected by default. This dialog box (and the attributes it contains) is available only for files or folders on NTFS volumes.

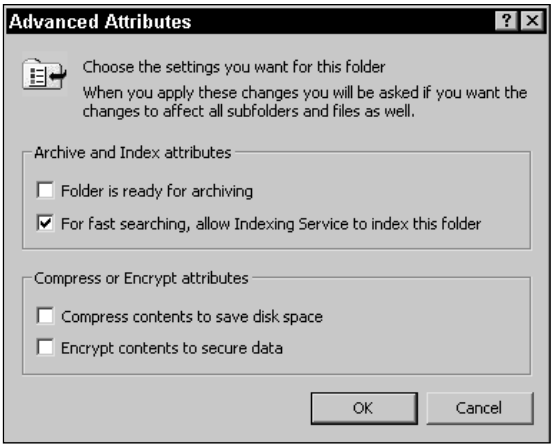

FIGURE 11-2 Setting advanced attributes

Select the check boxes next to the attributes you want to assign. (Or, clear the check boxes next to attributes you want to remove.) The user interface in this dialog box will not permit you to select both the Compress and Encrypt attributes—you can select one or the other, but not both. Click OK.

5. In the file or folder's Properties dialog box, click OK.
6. If you have modified the attributes of a folder that contains other files or folders, a Confirm Attribute Changes dialog box appears. Choose whether to apply your changes to this folder only, or to apply your changes to this folder and all of its subfolders and files. Click OK.
7. Windows 2000 applies attributes. Close Windows Explorer.

Managing Shared Folders

In Windows 2000, folders are *shared* to enable users to access network resources. A folder can't be accessed by users across the network until it is shared or placed within another folder that is shared. Once a folder is shared, users with the appropriate permissions can access the shared folder (and all folders and files that the shared folder contains) over the network.

A shared folder appears in Windows Explorer as a folder with a hand under it. A shared folder is often referred to as a *share*.

Sharing a Folder

Only certain users can share folders:

- Members of the Administrators and Server Operators built-in local groups on domain controllers can share folders on any Windows 2000 domain controller in the domain.
- Members of the Administrators and Power Users built-in local groups on nondomain controllers (whether or not they are members of the domain) can share folders on the local computer.
- Members of the Domain Admins built-in global group on domain controllers can share folders on any Windows 2000 computer that is a member of the domain. This is due to the fact that the Domain Admins group is, by default, a member of the Administrators built-in local group on domain controllers *and* a member of the Administrators built-in local group on all nondomain controllers that are members of the domain.

When a folder is shared, its *entire contents* (including all files and subfolders) are available to users who have the appropriate permissions to the share. Because all files and subfolders are accessible when a folder is shared, you should consider which users and groups need access to folders when you design your server's folder structure.

When sharing a folder, it's a good idea to assign it a share name that is easily recognized by users, and one that appropriately describes the resources contained in the folder. Otherwise, users can become frustrated trying to locate the specific network resources they need.

Additionally, keep in mind when you assign a name to a shared folder that a long share name may not be readable by all client computers on your network. MS-DOS computers, for example, can only read share names of up to 8 characters (plus a 3-character extension) in length, and Windows 95 and Windows 98 computers can only read share names of up to 12 characters in length. Share names on Windows 2000 and Windows NT computers can be up to 80 characters long.

You can use Windows Explorer or Computer Management to share folders on the local Windows 2000 computer. To share folders on remote computers, use Computer Management.

STEP BY STEP

USING WINDOWS EXPLORER TO SHARE A FOLDER ON THE LOCAL COMPUTER

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, expand folders as necessary until the folder you want to share is displayed in the right pane. In the right pane, highlight that folder. Select File ➪ Sharing. (Or, right-click the folder, and select Sharing from the menu that appears.)
3. The folder's Properties dialog box appears with the Sharing tab displayed. To share this folder, select the "Share this folder" option, as shown in Figure 11-3.

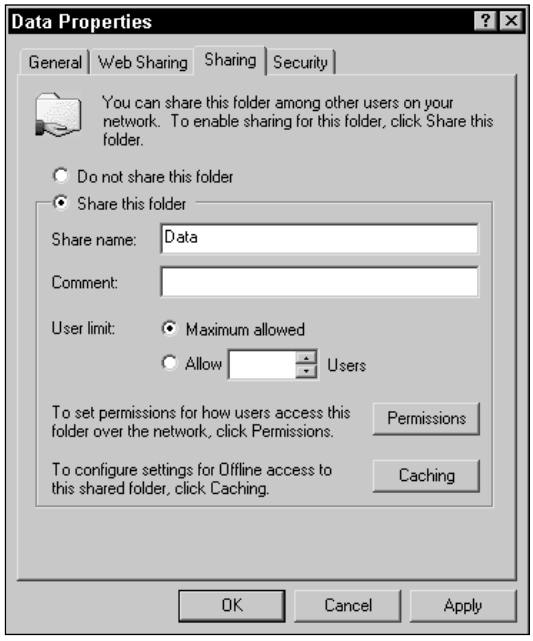

FIGURE 11-3 Sharing a folder in Windows Explorer

There are several configurable options on this tab:

Share name: Either accept the default name in the "Share name" text box or type in the name you want to use for the share.

Comment: You can add a descriptive comment about the share in the Comment text box if you want to. (This is an optional entry.)

User limit: If you want to limit the number of users who can connect to this share simultaneously (because of licensing limitations or for other reasons), you can configure the "User limit" section on this tab. The default "User limit" is "Maximum allowed."

STEP BY STEP *Continued*

Permissions: If you want to assign or change share permissions for this shared folder, click Permissions. (I'll cover share permissions later in this chapter.)

Caching: If you want to modify offline file settings for this shared folder, click Caching. Then, in the Caching Settings dialog box, select from the following options:

Allow caching of files in this shared folder: This check box is selected by default. If you want to prevent users from viewing this folder offline, clear this check box. If you want users to be able to configure this folder for offline use, accept the default setting, and select one of the following three options in the Setting drop-down list box:

- **Manual Caching for Documents:** Select this option if you want users to manually configure individual files in this folder for offline use. This is the default setting.
- **Automatic Caching for Documents:** Select this option if you want the files in this shared folder to be automatically downloaded to a user's local computer and cached on the local hard disk as the user opens each file in the shared folder. The entire folder is not cached on the user's computer—just the individual files the user has opened. If this option is selected, users don't have to manually configure the files in this folder for offline use. In addition, the cached files are automatically synchronized with the server when the user logs on and logs off his or her computer. This setting is not r ecommended when multiple users access and change the same file(s) in the shared folder.
- **Automatic Caching for Programs:** Select this option if this folder contains application files, and you want these application files to be cached on the user's local computer. Selecting this option can increase access speed for the user and decrease network traffic because the application is executed from the user's local computer instead of over the network. If application files in this shared folder are updated on the server, Windows 2000 will update the cached files on the user's local computer the next time the user logs on or logs off.

CROSS-REFERENCE

For more information on working with offline files, see the "Folder Options" section in Chapter 5.

Click OK.

4. In the folder's Properties dialog box, click OK.
5. Close Windows Explorer.

STEP BY STEP *Continued*

USING COMPUTER MANAGEMENT TO SHARE A FOLDER

1. Start Computer Management. (Right-click My Computer, and select Manage from the menu that appears.)
2. If you want to share a folder on this computer, skip to Step 4.

   If you want to share a folder on a remote computer, in the left pane of the Computer Management dialog box, right-click Computer Management (Local), and select "Connect to another computer" from the menu that appears.
3. In the Select Computer dialog box, double-click the name of the computer on which you want to share a folder.
4. In the left pane of the Computer Management dialog box, click the + next to System Tools (if System Tools is not already expanded). Click the + next to Shared Folders. Highlight Shares. Select Action➪New File Share.
5. The Create Shared Folder dialog box appears, as shown in Figure 11-4.

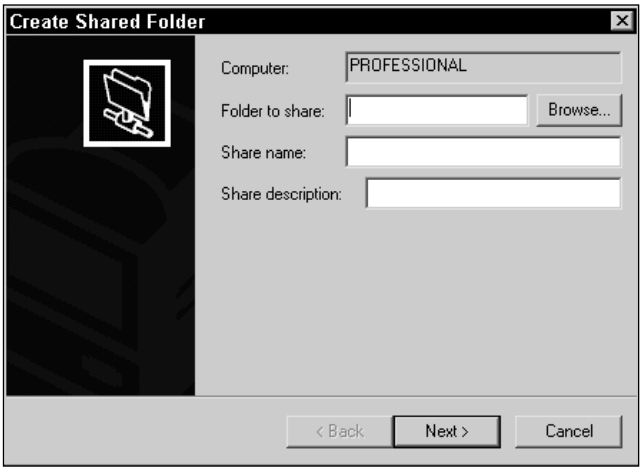

FIGURE 11-4 Sharing a folder in Computer Management

   In this dialog box, enter the full path to the folder you want to share (such as `C:\Data`). You can browse for this folder if you don't know its path.

   Enter a share name for the share. You can also enter a description for the share if you want to. Click Next.
6. In the next dialog box, configure the appropriate share permissions for this shared folder. (I'll cover share permissions a little later in this chapter.) Click Finish.
7. A dialog box appears, indicating that the folder has been successfully shared. Click Yes if you want to create another shared folder. Otherwise, click No.

STEP BY STEP *Continued*

8. The folder you just shared appears in the right pane of the Computer Management dialog box. Close Computer Management.

Connecting to Shared Folders

Users must connect to shared folders before they can access the resources they contain. In the next sections, I'll discuss how to connect to shared folders, including how to use common naming conventions, Windows Explorer, and the command line to connect to shared network resources.

Naming Conventions

A *naming convention* is an accepted method of identifying individual computers and their resources on the network.

The two common naming conventions used in Windows 2000 are the *universal naming convention (UNC)* and *fully qualified domain names (FQDNs)*.

A UNC name consists of a server name and a shared resource name in the following format:

```
\\Server_name\Share_name
```

In this format, *Server_name* represents the name of the server that the shared folder is located on, and *Share_name* represents the name of the shared folder.You can use a UNC name in this format to connect to a network share. For example, a shared folder named `Public` located on a server named SERVER1 would have the following UNC name:

```
\\SERVER1\Public
```

A UNC name can also specify the name of a subfolder within the share, the name of a file within the share, or the name of a file within a subfolder in the share using the following format:

```
\\Server_name\Share_name\Subfolder_name\File_name
```

You can use a UNC name in this format to access a specific folder or file, such as a data file on a remote server. For example, a data file named `Salaries.doc` in the `Payroll` folder located in a share named `HR` on a server named CORP would have the following UNC name:

```
\\CORP\HR\Payroll\Salaries.doc
```

An FQDN is a fancy term for the way computers are named and referenced on the Internet. FQDNs are often used on networks that use TCP/IP and DNS servers. The format of an FQDN is:

```
server_name.domain_name.root_domain_name
```

For example, the FQDN of a server named WOLF in a domain named `AlanCarter` in the `com` root domain would be: `wolf.alancarter.com`.

On Windows 2000 networks, you can replace the *Server_name* in a UNC with an FQDN. For example, to specify a share named `Books` on a server with an FQDN of `wolf.alancarter.com`, you could use: `\\wolf.alancarter.com\Books`. In addition, you can also replace the *Server_name* in a UNC with the IP address of the server.

Both UNC names and FQDNs can be used to connect to shared network resources in Windows Explorer and from the command line.

Using Windows Explorer

Assuming that you have the appropriate permissions, you can connect to any shared folder by using Windows Explorer.

STEP BY STEP

USING WINDOWS EXPLORER TO CONNECT TO A SHARED FOLDER

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. Select Tools ➪ Map Network Drive.
3. In the Map Network Drive dialog box, either accept the default drive letter or select a drive letter from the Drive drop-down list box. Then, in the Folder drop-down list box, type in the UNC name of the shared folder you want to connect to. If you don't know the UNC name, click Browse.

STEP BY STEP *Continued*

4. The Browse For Folder dialog box appears, as shown in Figure 11-5.

   Click the + next to any domain or workgroup (or double-click the domain or workgroup) to view a list of available network servers in that domain or workgroup. Then, click the + next to any server in the list (or double-click the server) to view a list of shared folders on that server. Highlight the shared folder you want to connect to, and click OK.

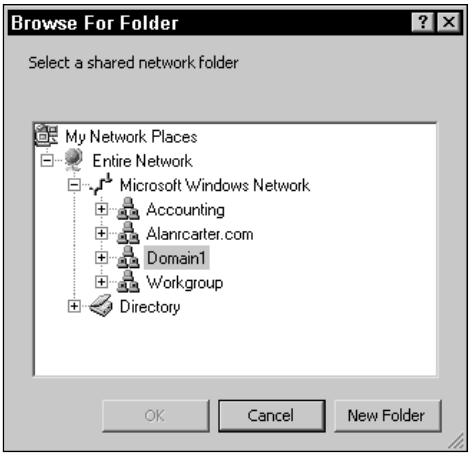

FIGURE 11-5 Browsing for a shared network folder

5. In the Map Network Drive dialog box, the UNC name for the shared folder you selected appears in the Folder drop-down list box. Click Finish.
6. Windows Explorer connects to the shared folder and opens a new dialog box for the shared folder. You can now access the contents of the shared folder. In addition, the shared folder appears, along with its drive letter, in the left pane.

Once you have connected to a shared folder, the new drive letter appears in Windows Explorer, My Computer, and the Open dialog box in standard Windows applications. You can then access the files and folders within the share in the same manner that you access files and folders on your local computer.

Connecting to Shared Folders from the Command Line

You can use the `Net.exe` utility to browse the network, and, assuming you have the appropriate permissions, to connect to a shared folder from the command line.

STEP BY STEP

USING NET.EXE TO BROWSE THE NETWORK FROM THE COMMAND LINE

1. Select Start➪Programs➪Accessories➪Command Prompt.
2. To obtain a list of available servers in your domain or workgroup, at the `C:\>` command prompt, type **net view** and press Enter.
3. To obtain a list of all domains and workgroups on the network, type **net view /domain** and press Enter.
4. To obtain a list of available servers in another domain (or workgroup), type **net view /domain:*domain_name*** and press Enter. (For example, to obtain a list of available servers in the LAB domain, type **net view /domain:lab** and press Enter.)
5. To obtain a list of available shares on a network server, type **net view *server_name*** and press Enter. (For example, to obtain a list of available shares on a server named SERVER01, type **net view \\server01** and press Enter.)
6. To exit the Command Prompt dialog box at any time, type **exit** at the command prompt and press Enter.

USING NET.EXE TO CONNECT TO A SHARE FROM THE COMMAND LINE

1. Select Start➪Programs➪Accessories➪Command Prompt.
2. At the `C:\>` command prompt type **net use *drive_letter*: *server_name**share_name*** and press Enter. For example, to connect a drive letter, such as `X:`, to a share named `Data` on a server named `INSPIRON`, type **net use x: \\inspiron\data** and press Enter.
3. Windows 2000 displays a message indicating that the command completed successfully.
4. Exit the Command Prompt dialog box by typing **exit** at the command prompt and pressing Enter.

Shared Folder Permissions

Shared folder permissions control user access to shared folders. Shared folder permissions only apply when users connect to the folder over the network—they do not apply when users access the folder on the local computer.

Shared folder permissions (commonly called *share permissions*) apply to the shared folder, its files, and subfolders (in other words, to the entire directory tree under the shared folder).

Share permissions are the only folder and file security available on a FAT or FAT32 volume (with the exception of file attributes), and only control over-the-network access to the share — local access is totally unrestricted on a FAT or FAT32 volume.

Table 11-2 lists and describes the Windows 2000 share permissions, from most restrictive to least restrictive.

TABLE 11-2 Windows 2000 Share Permissions

Permission	Description
Read	Permits a user to view a list of the share's contents (names of files and subfolders), to change the current folder to a subfolder of the share (sometimes called *traversing to subfolders*), to view data in files, and to run application files.
Change	Permits a user to perform all tasks included in the Read permission. In addition, permits a user to create files and subfolders within the share, to edit data files and save changes, and to delete files and subfolders within the share.
Full Control	Permits a user to perform all tasks included in the Change permission. In addition, permits a user to change NTFS permissions and to take ownership of files and folders (on shares located on NTFS volumes).

Share permissions are assigned by adding a user or group to the permissions list for the share. From an administrative standpoint, it's more efficient to add groups to the permissions list for a particular share than to add individual users. By default, the Everyone group is granted the Full Control permission to all newly created shared folders.

When assigning permissions to a share, you should consider assigning the most restrictive permission that still permits users to accomplish the tasks they need to perform. For example, on shares that contain applications, consider assigning the Read permission so that users can't accidentally delete application files.

You can use Windows Explorer or Computer Management to assign share permissions to shared folders on the local Windows 2000 computer. To assign share permissions to shared folders on remote computers, use Computer Management.

STEP BY STEP

USING WINDOWS EXPLORER TO ASSIGN SHARE PERMISSIONS

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, expand folders as necessary until the shared folder to which you want to assign share permissions is displayed in the right pane. In the right pane, highlight that folder. Select File ➪ Sharing. (Or, right-click the folder and select Sharing from the menu that appears.)
3. The folder's Properties dialog box appears with the Sharing tab displayed. Click Permissions.
4. The Permissions dialog box for the shared folder appears, as shown in Figure 11-6. Notice that by default the Everyone group is allowed the Full Control, Change, and Read permissions.

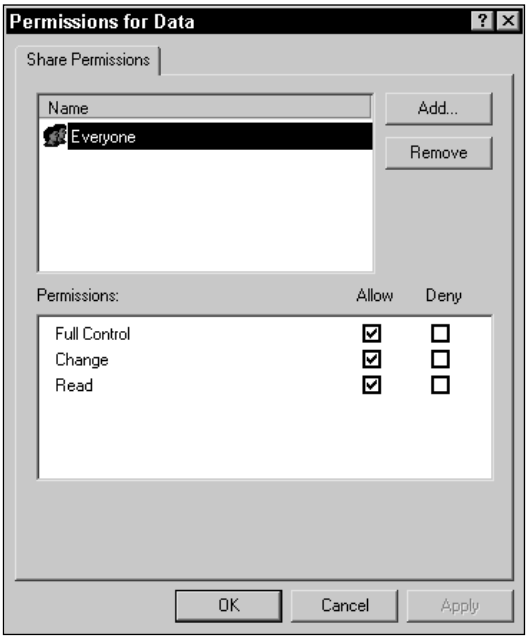

FIGURE 11-6 Assigning share permissions

Also notice the Allow and Deny check boxes.

- **Allow:** When the Allow check box next to a specific permission is selected for a user or group, the user or group is granted the selected permission to the share.

STEP BY STEP *Continued*

- **Deny:** When the Deny check box next to a specific permission is selected for a user or group, the user or group is specifically denied that permission to the share, even if the user or group is allowed that permission through membership in another group.

TIP

A denied permission always overrides an allowed permission.

- **Neither:** When neither the Allow or Deny check box next to a specific permission is selected for a user or group, the user or group is not assigned that permission to the share.

When a user or group is not listed in the Name box, the user or group has no permissions (and no access) to the share unless the user or group is a member of a group that *is* listed in the Name box.

To change the permissions currently assigned to a user or group listed in the Name box, highlight the user or group, then select or clear the appropriate check boxes in the Permissions box.

To remove a user or group from the permissions list for the share, highlight the user or group in the Name box, and click Remove.

To add a user or group to the Name box, click Add.

5. In the Select Users, Computers, or Groups dialog box, double-click each user and group you want to add. (You can also highlight each user or group and then click Add, but double-clicking is faster and easier.) As you double-click each user or group, the user or group appears in the bottom portion of the dialog box. Click OK.
6. In the Permissions dialog box for the share, each user or group that you added is automatically assigned the Read permission to the share. To change the permissions of a user or group you added, highlight the user or group in the Name box, then select or clear the appropriate check boxes in the Permissions box. Click OK.
7. In the shared folder's Properties dialog box, click OK.
8. Close Windows Explorer.

How User and Group Permissions Combine

It is not uncommon for a user to have permissions to a share and to be a member of multiple groups that have different permissions to that share. When this occurs, the user and group permissions are additive, and normally the *least restrictive* permission is the user's effective permission. For

example, suppose a user is allowed the Read permission to a share, and a group that the user is a member of is allowed the Change permission to the share. The user's effective share permission is Change.

An exception to this rule occurs when a user is specifically *denied* a permission. Remember the Allow and Deny check boxes in the permissions list to the share? *A denied permission always overrides an allowed permission.* Whenever a user is specifically denied a permission, or is a member of a group that is specifically denied a permission, the user is denied that permission. If a user is allowed the Full Control permission, but is a member of a group that is denied the Full Control permission, the user is denied the Full Control permission to the share — in other words the user is denied all access to the share. For this reason, you should exercise care in denying a specific share permission to a user or group.

EXAM TIP

When taking the Professional and Server exams, watch out for denied permissions. A denied permission is a big red flag. Remember that a denied permission always overrides an allowed permission.

Here are two examples that illustrate how user and group share permissions combine.

Example 1

A user, RomanB, manages a shared folder named `SalesData` that contains Sales department data. RomanB is a member of three groups. Table 11-3 shows the `SalesData` share permissions assigned to RomanB and to the three groups of which he is a member.

TABLE 11-3 RomanB's Group Memberships and Share Permissions

User or Group	SalesData Share Permissions Assigned
RomanB	Allow – Full Control
Sales	Allow – Change
Everyone	Allow – Read
Domain Users	Allow – Read

Because share permissions are additive, RomanB's effective permission to the `SalesData` share is Full Control.

Example 2

Until recently, a user, PennyL, was a design analyst in the Marketing department. She has just been promoted to a management position in the Human Resources department. PennyL's network has a shared folder named `HRData` that contains Human Resources department data, including employee performance reviews. PennyL is a member of three groups. Table 11-4 shows the `HRData` share permissions assigned to the three groups of which PennyL is a member.

TABLE 11-4 PennyL's Group Memberships and Their HRData Share Permissions

Group	HRData Share Permissions Assigned
Managers	Allow – Read
HR	Allow – Change
Marketing	Deny – Full Control, Change, and Read

Because a denied permission always overrides an allowed permission, PennyL's effective permission to the `HRData` share is Deny – Full Control, Change, and Read. In effect, PennyL is specifically denied all access to the `HRData` share. The administrator should remove PennyL from the Marketing group so she can access the `HRData` share. Once PennyL is removed from the Marketing group, her effective permission to the `HRData` share will be Change.

Modifying a Share

After a share is created, you may want to modify its properties. You can assign multiple share names to a share, change the name of a share, or stop sharing a share.

Assigning Multiple Share Names to a Share

To assist different users in locating or recognizing a share, you can assign multiple names to the same share.

For example, a group of technical support engineers might routinely access a share called `CIM` (CompuServe Information Manager), and less technical personnel at a help desk might access this same share using the name `CompuServe`.

When you assign an additional name to a share, what you actually end up doing is creating a new share for the *same* network resource. When you create the new share *you must manually assign a new set of share permissions that apply only to new share*. The permissions from the original share are *not* automatically applied to the new share.

STEP BY STEP

ASSIGNING AN ADDITIONAL NAME TO A SHARE

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, expand folders as necessary until the shared folder to which you want to assign an additional name is displayed in the right pane. In the right pane, highlight that folder. Select File ➪ Sharing. (Or, right-click the folder, and select Sharing from the menu that appears.)
3. The folder's Properties dialog box appears with the Sharing tab displayed. Click New Share.
4. In the New Share dialog box, enter the new name you want to assign to the share in the Share Name text box. Enter a comment if you want to. Configure the User Limit if necessary. Click Permissions to assign share permissions to the new share.
5. In the Permissions dialog box, configure permissions for the new share. Click OK.
6. In the New Share dialog box, click OK.
7. In the shared folder's Properties dialog box, the "Share name" drop-down list box now contains two names for the share: the original share name, and the name you just added. Click OK.
8. Close Windows Explorer.

Changing a Share Name

Occasionally you may need to change a share name. Perhaps you want to assign a more intuitive share name for users, or you might need to comply with a newly established set of naming conventions. To change a share name, you must create a new share that uses the new name, configure permissions for the new share, and then remove the original share.

STEP BY STEP

CHANGING A SHARE NAME AND REMOVING THE ORIGINAL SHARE

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, expand folders as necessary until the shared folder you want to rename is displayed in the right pane. In the right pane, highlight that folder. Select File ➪ Sharing. (Or, right-click the folder, and select Sharing from the menu that appears.)
3. The folder's Properties dialog box appears with the Sharing tab displayed. Click New Share.
4. In the New Share dialog box, enter the new name you want to assign to the share in the Share Name text box. Enter a comment if you want to. Configure the User Limit if necessary. Click Permissions to assign share permissions to the new share.
5. In the Permissions dialog box, configure permissions for the new share. Click OK.
6. In the New Share dialog box, click OK.
7. In the shared folder's Properties dialog box, select the original share name in the "Share name" drop-down list box. Click Remove Share to remove the original share. The folder is now shared using only the new name you assigned—the original share name has been removed. Click OK.
8. Close Windows Explorer.

How to Stop Sharing a Folder

You might decide to stop sharing a folder because it is no longer needed, or for other reasons.

STEP BY STEP

TO STOP SHARING A FOLDER

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, expand folders as necessary until the shared folder you want to stop sharing is displayed in the right pane. In the right pane, highlight that folder. Select File ➪ Sharing. (Or, right-click the folder, and select Sharing from the menu that appears.)

STEP BY STEP *Continued*

3. The folder's Properties dialog box appears with the Sharing tab displayed. Select the "Do not share this folder" option. Click OK.
4. Close Windows Explorer.

Administrative Shares

Every time you start Windows 2000 on a computer, Windows 2000 automatically creates several hidden shares that only members of the Administrators group (on the local computer) have permissions to access. These shared are referred to as *administrative shares* because they are used by Administrators to perform administrative tasks.

The Windows 2000 administrative shares are: `C$`, `D$`, `E$`, and so on (one share for the root of each hard disk volume on the computer); and a share named `Admin$`, which corresponds to the folder in which Windows 2000 is installed (*SystemRoot*). The `$` at the end of each administrative share causes the share to be hidden from users when they browse the network. If users are not specifically aware the share exists, they will not be able to connect to the hidden share. To connect to a hidden share, you have to type in the server name and share name in the Map Network Drive dialog box in Windows Explorer. You can't browse for hidden shares.

Administrative shares make it possible for an Administrator to connect to any hard disk on a computer and to access all of its files and folders, regardless of whether regular shares exist on that hard disk. In this way an Administrator can perform backup, restore, and other administrative functions on a Windows 2000 computer.

Any share can be configured as a hidden share by placing a `$` at the end of its share name. However, hiding a share by appending a `$` to the share name does *not* limit user access to the share. The hidden share retains it assigned share permissions. Only access to the hidden *administrative* shares is restricted, by default, to Administrators only.

If you don't want administrative shares available on a Windows 2000 computer, you can configure Windows 2000 to prevent the creation of administrative shares. To accomplish this, you can edit the registry. You can

edit the registry directly by using `Regedt32.exe`, or you can use the System Policy Editor to disable the creation of the hidden administrative shares. System Policy editor was covered in chapter 10.

CAUTION

If you configure a Windows 2000 computer to prevent the creation of administrative shares, some administrative tools such as the Distributed File System tool may not function correctly on that computer.

STEP BY STEP

USING REGEDT32.EXE TO PREVENT THE CREATION OF ADMINISTRATIVE SHARES

1. From the desktop, select Start ➪ Run.
2. In the Open text box, type **Regedt32** and click OK.
3. In the Registry Editor dialog box, select Window ➪ HKEY_LOCAL_MACHINE on Local Machine.
4. In the left pane of the Registry Editor dialog box, double-click the `SYSTEM` folder under HKEY_LOCAL_MACHINE. Double-click the `CurrentControlSet` folder. Double-click the `Services` folder. Double-click the `lanmanserver` folder, then click the `parameters` folder.
5. In the right pane of the Registry Editor dialog box, double-click AutoShareServer. (Or, if this value is not present, select Edit ➪ Add Value. In the Add Value dialog box, type **AutoShareServer** in the Value Name text box. Then, in the Data Type drop-down list box, select REG_DWORD. Click OK.)

   (If you are configuring a Windows 2000 Professional computer, the value is named AutoShareWks. If this value is not present, select Edit ➪ Add Value. In the Add Value dialog box, type **AutoShareWks** in the Value Name text box. Then, in the Data Type drop-down list box, select REG_DWORD. Click OK.)
6. In the DWORD Editor dialog box, edit the Data text box so that it has a value of **0** (zero). Click OK.
7. Close Registry Editor. The next time the computer is started, the hidden administrative shares will not be created.

If you configure a Windows 2000 computer to prevent the creation of administrative shares and later change your mind and want to enable the creation of administrative shares, follow the preceding steps, except assign a value of 1 to AutoShareServer or AutoShareWks (instead of 0) in Step 6.

Configuring and Managing the Distributed File System

The *Distributed file system* (*Dfs*) is a file system that enables an administrator to make shares that are stored on various servers on the network appear to users as though they are stored within a single share on a single server. The use of Dfs makes finding network resources easier for users because users don't have to know which server physically contains the shared resource they are trying to access.

There are two specific components used in the implementation of Dfs: Dfs roots and Dfs links. A *Dfs root* is a special type of shared folder that can contain files, folders, Dfs links, and other Dfs roots. To the user, a Dfs root appears in a browse list just like any other shared folder. A *Dfs link* is a special type of subfolder in a Dfs root that acts as a pointer to a specific shared folder on the network.

Here's an example of how Dfs might be used on a typical network. Suppose that you're the administrator of a Windows 2000 network and you want to organize all of the shared folders for the Sales department. Currently, the shared folders for this department are stored on multiple servers across your network. First, you create a Dfs root called `Sales` on one of your Windows 2000 Server network servers. Then, in the `Sales` Dfs root, you create a Dfs link for each shared network folder used by the members of the Sales department. Now, users in the Sales department can map a single network drive to the `Sales` Dfs root instead of searching various network servers for the shared folders they need to access. When users view the contents of the `Sales` Dfs root, each shared folder for the Sales department appears as a subfolder of the `Sales` Dfs root. Users can access these subfolders in the same manner they would normally access subfolders on their local computers.

There are a few general Dfs facts you should know before I get down to the nuts and bolts of working with Dfs:

- You can use the Distributed File System tool in Administrative Tools to create and configure Dfs roots and Dfs links.
- Only Windows 2000 Server computers can host Dfs roots — Windows 2000 Professional computers can't.
- A Windows 2000 Server computer can host only *one* Dfs root (or *one* replica of a Dfs root).

Creating and Configuring a Dfs Root

When you create a Dfs root, you choose whether the Dfs root will be a stand-alone or domain Dfs root.

A *stand-alone Dfs root* is a type of Dfs root that can be hosted on any individual Windows 2000 Server computer. A stand-alone Dfs root is not published in Active Directory. In addition, you can't create a replica of a stand-alone Dfs root for load balancing or fault tolerance purposes. If the server that hosts a stand-alone Dfs root isn't available, the Dfs root is not available to users. Users with the appropriate permissions can access a stand-alone Dfs root by using a UNC path in the following format: *Server_name**Dfs_root_name*.

A *domain Dfs root* is another type of Dfs root that can be hosted on any Windows 2000 Server computer in the domain. In addition, an object representing the Dfs root is published in Active Directory. You can create a replica of a domain Dfs root on one or more Windows 2000 Server computers on your network to provide load balancing and fault tolerance. If one of the servers that hosts the Dfs root (or its replica) is not available, users can still access the Dfs root on one of the other servers. Users with the appropriate permissions can access a domain DFS root by using a UNC path in the following format: *Domain_name**Dfs_root_name*. The user does not need to know the name of the server that physically hosts the domain Dfs root in order to access it.

In general, if you require fault tolerance or load balancing, or if a shared resource must always be available to users, you would probably choose to use a domain Dfs root. If you don't require fault tolerance or load balancing, but simply want to organize shared resources for your users, you'd probably choose to use a stand-alone Dfs root.

STEP BY STEP

CREATING AND CONFIGURING A STAND-ALONE OR DOMAIN DFS ROOT

1. Start the Distributed File System tool. (Select Start ➪ Programs ➪ Administrative Tools ➪ Distributed File System.) (This tool is available on all Windows 2000 Server computers, and is available on Windows 2000 Professional computers on which the ADMINPAK has been installed.)
2. In the Distributed File System dialog box, select Action ➪ New Dfs Root.

STEP BY STEP *Continued*

3. The New Dfs Root Wizard starts. Click Next.
4. The Select the Dfs Root Type screen appears.

   To create a stand-alone Dfs root, select the "Create a standalone Dfs root" option. Click Next, and skip to Step 6.

   To create a domain Dfs root, select the "Create a domain Dfs root" option. Click Next.
5. In the Select the Host Domain for the Dfs Root screen, select, from the "Trusting domains" list box, the Windows 2000 domain that will host the domain Dfs root you're creating. The selected domain appears in the "Domain name" text box. Click Next.
6. In the Specify the Host Server for the Dfs Root screen, type in the FQDN of the Windows 2000 Server computer you want to host this Dfs root. For example, `server01.domain1.mcse`. If you don't know the FQDN of the server, you can click Browse to browse for it. Click Next.
7. In the Specify the Dfs Root Share screen, choose whether to use an existing share on the host server as your new Dfs root or to create a new share to use as your new Dfs root.

   If you have an existing shared folder that is a logical place to organize other shared network resources, or if you already created a shared folder for the specific purpose of becoming your new Dfs root, select the "Use an existing share" option and select the shared folder from the drop-down list box.

   Otherwise, select the "Create a new share" option. Then, in the "Path to share" text box, type in the drive letter and path to the share you want to create, for example, `C:\Dfs`. (This can be the path to an existing or non-existing folder. If the folder doesn't yet exist, Windows 2000 will create it for you.) Finally, in the "Share name" text box, type in the share name for the new Dfs root.

   Figure 11-7 shows this screen configured to create a new share named `Dfs` in the `C:\Dfsroot` folder.

   Click Next.
8. If you chose to create a new share in Step 7, and the folder you specified does not exist, Windows 2000 asks if you want to create the folder. Click Yes.
9. The Name the Dfs Root screen appears. If you chose to use an existing share in Step 7, enter a name for the Dfs root in the "Dfs root name" text box, or accept the default name displayed. (If you chose to create a new share, this text box is grayed out.)

   Enter a comment for the Dfs root if appropriate. Click Next.

STEP BY STEP *Continued*

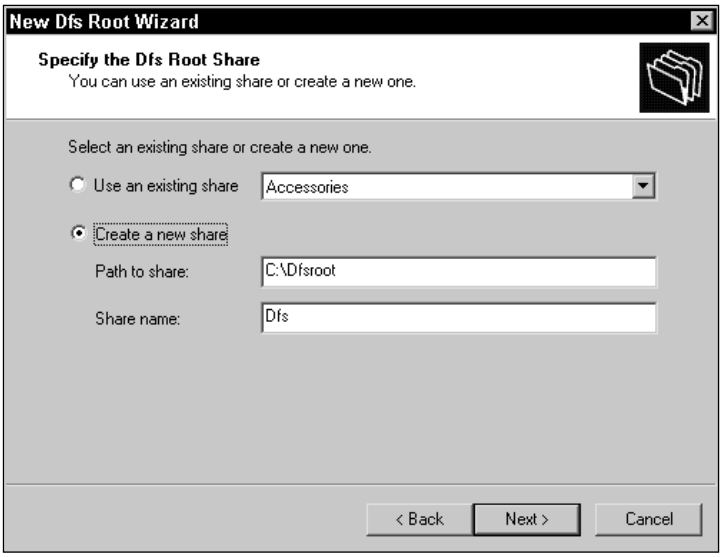

FIGURE 11-7 Creating a new share for the Dfs root

10. In the Completing the New Dfs Root Wizard screen, click Finish.
11. Windows 2000 creates the new Dfs root. It appears in the left pane in the Distributed File System dialog box.

Creating and Configuring a Domain Dfs Root Replica

A *domain Dfs root replica* is a shared folder that is a copy of a domain Dfs root that is stored on a different Windows 2000 Server computer than the original Dfs root. The primary purpose of a domain Dfs root replica is to provide load balancing and fault tolerance, so that if the server that hosts the original domain Dfs root is not available, users can still access the domain Dfs root.

When a domain Dfs root replica is created, Windows 2000 automatically copies all Dfs links in the original domain Dfs root to the replica. However, Windows 2000 does *not* automatically copy files and folders in the original domain Dfs root to the replica — you must either manually copy these items to the replica, or configure Windows 2000 to automatically replicate them for you. If you enable automatic replication between the domain Dfs

root and its replica(s), Windows 2000 will synchronize files and folders between the replica(s) and the original domain Dfs root every 15 minutes.

TIP

You can only configure automatic replication between a domain Dfs root and its replica when both shares are located on NTFS volumes.

You can create up to 31 replicas of an original domain Dfs root, plus the original domain Dfs root, for a total of 32 instances of a domain Dfs root (assuming that you have 32 Windows 2000 Server computers, one computer for each instance).

In the steps that follow I'll explain how to create a domain Dfs root replica, and then how to configure automatic replication between the domain Dfs root and its replica.

STEP BY STEP

CREATING AND CONFIGURING A DOMAIN DFS ROOT REPLICA

1. Start the Distributed File System tool. (Select Start ➪ Programs ➪ Administrative Tools ➪ Distributed File System.)
2. If the domain Dfs root you want to create a replica of is not displayed in the left pane of the Distributed File System dialog box, select Action ➪ Display an Existing Dfs Root.

   Then, in the Display an Existing Dfs Root dialog box, expand the domains in the Trusting Domains list box until the domain Dfs root you want to create a replica of is displayed. Highlight this Dfs root (when you do, it appears in the "Dfs root or host server" text box). Click OK.
3. In the left pane of the Distributed File System dialog box, right-click the domain Dfs root you want to create a replica of, and select New Root Replica from the menu that appears.
4. The New Dfs Root Wizard dialog box appears. Type in the FQDN of the Windows 2000 Server computer on which you want to create the replica, for example, `server02.domain1.mcse`. If you don't know the FQDN of the server, you can click Browse to browse for it. Click Next.
5. In the Specify the Dfs Root Share screen, choose whether to use an existing share for the replica or to create a new share to use for the replica.

   If you have an existing shared folder that you want to use for the replica, select the "Use an existing share" option and select the shared folder from the drop-down list box.

STEP BY STEP *Continued*

Otherwise, select the "Create a new share" option. Then, in the "Path to share" text box, type in the drive letter and path to the share you want to create for the replica, for example, `C:\Dfsreplica`. (This can be the path to an existing or nonexisting folder. If the folder doesn't yet exist, Windows 2000 will create it for you.) Finally, in the "Share name" text box, type in the share name for the replica.

Click Finish.

6. If you chose to create a new share in Step 5, and the folder you specified does not exist, Windows 2000 asks if you want to create the folder. Click Yes.
7. Windows 2000 creates the Dfs root replica. It is displayed in the right pane of the Distributed File System dialog box.

   If you want to manually copy data between the domain Dfs root and its replica, stop here. Otherwise, continue on to Step 8 to configure automatic replication.
8. In the left pane of the Distributed File System dialog box, right-click the domain Dfs root, and select Replication Policy from the menu that appears.
9. The Replication Policy dialog box appears, as shown in Figure 11-8. Notice the "No" entries in the Replication column. Automatic replication is not enabled by default.

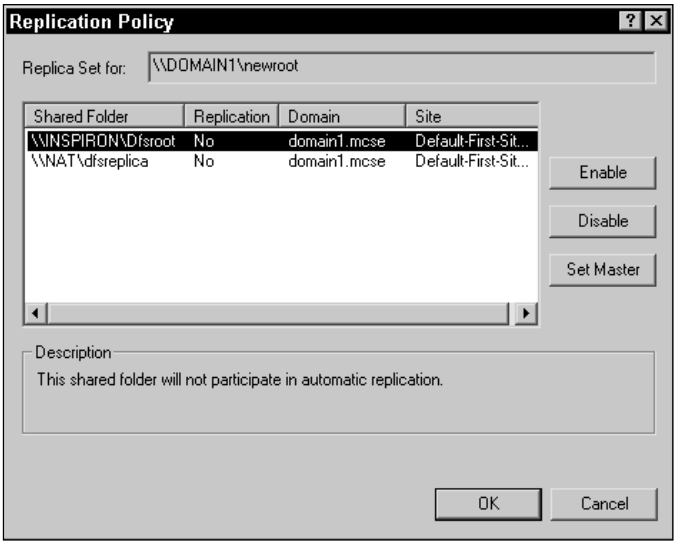

FIGURE 11-8 Configuring automatic replication

Highlight the shared folder that contains the original domain Dfs root. Click Enable. The entry in the Replication column changes from No to Yes (Primary).

Then, highlight the shared folder that contains the replica, and click Enable. The entry in the Replication column changes from No to Yes. Click OK.

STEP BY STEP *Continued*

TIP

When configuring automatic replication, it's important to configure the domain Dfs root *first*, and then the replica, to ensure that the contents of the Dfs root are correctly copied to the replica.

Creating and Configuring a Dfs Link and a Dfs Link Replica

As I said before, a Dfs link is a special type of subfolder in a Dfs root that acts as a pointer to a specific shared folder on the network. A Dfs link can point to a shared folder on any computer on the network, including Windows NT computers, Windows 95/98 computers, and even NetWare servers.

STEP BY STEP

CREATING AND CONFIGURING A DFS LINK

1. Start the Distributed File System tool. (Select Start ➪ Programs ➪ Administrative Tools ➪ Distributed File System.)
2. If the Dfs root in which you want to create a Dfs link is not displayed in the left pane of the Distributed File System dialog box, select Action ➪ Display an Existing Dfs Root.

   Then, in the Display an Existing Dfs Root dialog box, expand the domains in the Trusting Domains list box until the Dfs root in which you want to create a Dfs link is displayed. Highlight this Dfs root (when you do, it appears in the "Dfs root or host server" text box). Click OK.
3. In the left pane of the Distributed File System dialog box, right-click the Dfs root in which you want to create a Dfs link, and select New Dfs Link from the menu that appears.
4. The Create a New Dfs Link dialog box appears, as shown in Figure 11-9.

   In the "Link name" text box, type a name for the Dfs link. Because this is the name that users will see, it should clearly indicate the shared folder that it points to, the shared folder's contents, or both. The Dfs link name can even be the same as the name of the shared folder it points to.

STEP BY STEP *Continued*

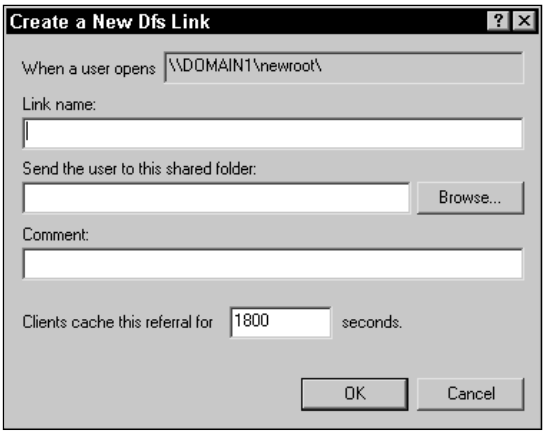

FIGURE 11-9 Creating a new Dfs link

In the "Send the user to this shared folder" text box, type the full UNC name to the shared folder that this Dfs link points to, for example, `\\Server03\Applications`. You can browse for the UNC name if you don't know it.

Enter a comment in the Comment text box if appropriate.

Configure the length of time client computers will cache the pointer if necessary. The default setting is 1800 seconds (30 minutes).

Click OK.

5. Windows 2000 creates the Dfs link. It appears in the left pane of the Distributed File System dialog box, under its Dfs root.

A *Dfs link replica* is an additional pointer attached to a Dfs link. This pointer points to an alternate location where a user can access a copy of the shared folder (that the Dfs link points to) if the server hosting the original shared folder is unavailable. This feature provides load balancing and fault tolerance for the Dfs link.

You can create up to 31 replicas of an original Dfs link, plus the original Dfs link, for a total of 32 instances of a Dfs link. A Windows 2000 Server computer can host multiple Dfs links.

Just as you can configure automatic replication between a domain Dfs root and its replica, you can also configure automatic replication between the original shared folder (that the Dfs link points to) and the copy of the shared folder (that the Dfs link replica points to). In order to do this, however, both

the original shared folder and the copy of the shared folder must both be located on NTFS volumes on Windows 2000 Server computers.

STEP BY STEP

CREATING AND CONFIGURING A DFS LINK REPLICA

1. Start the Distributed File System tool. (Select Start ➪ Programs ➪ Administrative Tools ➪ Distributed File System.)
2. If the Dfs root that contains the Dfs link for which you want to create a replica is not displayed in the left pane of the Distributed File System dialog box, select Action ➪ Display an Existing Dfs Root.

   Then, in the Display an Existing Dfs Root dialog box, expand the domains in the Trusting Domains list box until the Dfs root that contains the Dfs link for which you want to create a replica is displayed. Highlight this Dfs root (when you do, it appears in the "Dfs root or host server" text box). Click OK.
3. In the left pane of the Distributed File System dialog box, click the + next to the Dfs root that contains the Dfs link for which you want to create a replica (if the Dfs root is not already expanded). Right-click the Dfs link, and select New Replica from the menu that appears.
4. The Add a New Replica dialog box appears, as shown in Figure 11-10. Notice that by default, automatic replication of Dfs link replicas is not enabled.

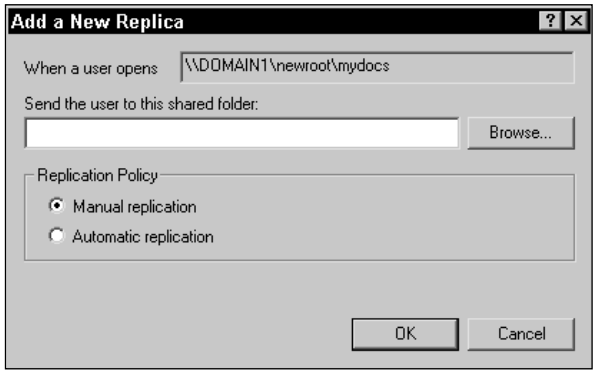

FIGURE 11-10 Creating a Dfs link replica

In the "Send the user to this shared folder" text box, type the full UNC name to the shared folder that this Dfs link replica points to, for example, `\\Server05\Applications`. You can browse for the UNC name if you don't know it.

STEP BY STEP *Continued*

If you want to manually copy data between the original shared folder and its alternate copy, accept the default setting of "Manual replication."

Otherwise, select the "Automatic replication" option. Click OK.

5. If you selected the "Automatic replication" option, the Replication Policy dialog box appears.

   Highlight the original shared folder to which the Dfs link points. Click Enable. The entry in the Replication column changes from No to Yes (Primary).

   Then, highlight the copy of the shared folder to which the Dfs link replica points, and click Enable. The entry in the Replication column changes from No to Yes. Click OK.

   Figure 11-11 shows the Replication Policy dialog box after automatic replication has been configured.

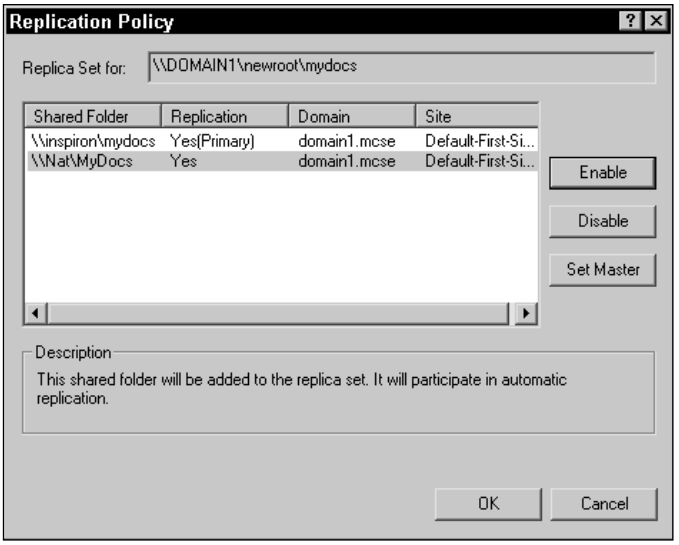

FIGURE 11-11 Replication configured between shared folders

6. The Dfs link replica appears in the right pane of the Distributed File System dialog box.

Configuring Client Computers to Use Dfs

All Windows 2000 client computers (Professional and Server) and all Windows NT 4.0 client computers (Workstation and Server) with Service Pack 3 or later installed can access Dfs roots on Windows 2000 Server computers on the network. No special configuration or software is required.

However, Windows 95 and Windows 98 client computers need to have Dfs client software installed before they can access Dfs roots. Once Dfs client software is installed, Windows 95 and Windows 98 computers can access Dfs links to shared folders on any Windows-based computer on the network. However, Windows 95 and Windows 98 computers can't access Dfs links to NetWare servers, even with Dfs client software installed.

Managing NTFS File and Folder Security

When files and folders are stored on an NTFS volume on a Windows 2000 computer, NTFS permissions can be assigned to provide a greater level of security than share permissions, because:

- NTFS permissions, unlike share permissions, can be assigned to individual files as well as folders. This gives an administrator a much finer level of control over shared files and folders than is possible by using only share permissions.
- NTFS permissions apply to local users as well as to users who connect to a shared folder over the network. This fills the large security loophole left when files and folders on FAT partitions are secured only by share permissions.

The following sections discuss NTFS permissions, including how they are assigned to files and folders, how NTFS permissions are applied, and how NTFS and share permissions interact.

NTFS Permissions

NTFS permissions, which can only be assigned to files and folders on NTFS volumes, protect data from unauthorized access when users connect to the share locally or over the network.

The standard Windows 2000 NTFS permissions that can be assigned to files and folders are listed and described in Table 11-5.

TABLE 11-5 Windows 2000 Standard NTFS Permissions

Permission	When Applied to a File, a User Is Able to . . .	When Applied to a Folder, a User Is Able To . . .
Read	View the file's contents, attributes, extended attributes, and permissions; and synchronize the file.	View a list of the folder's contents (names of files and subfolders), attributes, extended attributes, and permissions; and synchronize the folder.
Read & Execute	Perform all actions included in the Read permission. In addition, the user can execute the file (if it is an executable).	Perform all actions included in the Read permission. In addition, the user can change the current folder to a subfolder (traverse to subfolders).
List Folder Contents	This permission is not available on files.	Perform all actions included in the Read & Execute permission. This permission is not inheritable by files in a folder—it applies to the folder only.
Write	View the file's permissions and synchronize the file. In addition, the user can write data to the file, append data to the file, and change the file's attributes and extended attributes.	View the folder's permissions and synchronize the folder. In addition, the user can create files and subfolders in the folder, and can change the folder's attributes and extended attributes.
Modify	Perform all actions included in the Read & Execute and Write permissions. In addition, the user can delete the file.	Perform all actions included in the Read & Execute and Write permissions. In addition, the user can delete the folder.
Full Control	Perform all actions included in the Modify permission. In addition, the user can change the file's permissions and can take ownership of the file.	Perform all actions included in the Modify permission. In addition, the user can change the folder's permissions, take ownership of the folder, and delete files and subfolders within the folder.

Assigning NTFS Permissions to Files and Folders

NTFS permissions are assigned by adding a user or group to the access control list (ACL) for the file or folder. From an administrative standpoint, it's more efficient to add groups to the ACL for a particular file or folder than to add individual users. By default, the Everyone group is granted the Full Control NTFS permission to the root of all newly created NTFS volumes.

When assigning NTFS permissions, you should consider assigning the most restrictive permission that still permits users to accomplish the tasks they need to perform. For example, on a folder that contains applications, consider assigning the Read & Execute permission so that users can't accidentally delete application files.

Like share permissions, NTFS permissions are specifically allowed or denied to a specific user or group.

Another important concept to keep in mind when assigning NTFS permissions is *inheritance*. By default, when NTFS permissions are assigned to a folder, those permissions extend to (that is, are inherited by) all of the files and subfolders in that folder. However, when you assign NTFS permissions to a folder, you can choose whether or not the NTFS permissions you assign will be inherited by the files and subfolders contained in that folder. In addition, when you assign NTFS permissions to a file or folder, you can configure whether that file or folder will inherit NTFS permissions from its parent folder (that is, the folder that contains the file or folder you're configuring).

TIP

You can think of a volume as a parent folder for all of the files and folders it contains. You can assign NTFS permissions to a volume in the same way you can assign them to a folder. A volume is just a big folder that doesn't have a parent folder.

You can use Windows Explorer or the `Cacls.exe` command-line utility to assign NTFS permissions. You can assign NTFS permissions to a file or folder only if you are the owner of the file or folder, or you have the Full Control or Change Permissions NTFS permission to the file or folder.

STEP BY STEP

ASSIGNING NTFS PERMISSIONS TO A FILE OR FOLDER

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, expand folders as necessary until the file or folder to which you want to assign NTFS permissions is displayed in the right pane. In the right pane, highlight that file or folder. Select File ➪ Properties. (Or, right-click the file or folder, and select Properties from the menu that appears.)
3. In the file or folder's Properties dialog box, click the Security tab.
4. The Security tab appears, as shown in Figure 11-12. Notice that by default the Everyone group is allowed the Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write NTFS permissions. Also notice that these permissions are each displayed by the use of a gray box with a check in it. This indicates that the permission has been inherited from a parent folder, rather than specifically assigned to the file or folder.

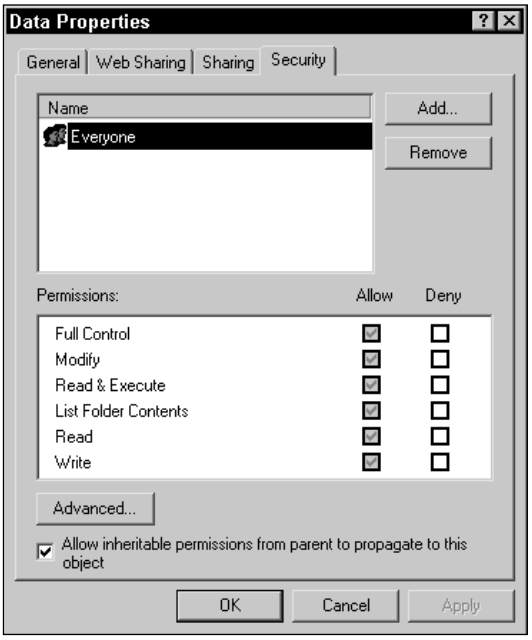

FIGURE 11-12 Assigning NTFS permissions to a file

Also notice the Allow and Deny check boxes.

- **Allow:** When the Allow check box next to a specific NTFS permission is selected for a user or group, the user or group has the selected NTFS permission to the file or folder.

STEP BY STEP *Continued*

- **Deny:** When the Deny check box next to a specific NTFS permission is selected for a user or group, the user or group is specifically denied that NTFS permission to the file or folder, even if the user or group is allowed that permission through membership in another group.

TIP

A denied permission always overrides an allowed permission.

- **Neither:** When neither the Allow or Deny check box next to a specific NTFS permission is selected for a user or group, the user or group is not assigned that permission to the file or folder.

When a user or group is not listed in the Name box, the user or group has no NTFS permissions (and no access) to the file or folder unless the user or group is a member of a group that *is* listed in the Name box.

To change the NTFS permissions currently assigned to a user or group listed in the Name box, highlight the user or group, then select or clear the appropriate check boxes in the Permissions box.

TIP

You can't change inherited NTFS permissions at this level. If the permissions shown in this dialog box are inherited (that is, a gray box with a check in it is displayed), you must change these permissions on the parent folder where the NTFS permissions were originally assigned.

To remove a user or group from the permissions list for the file or folder, highlight the user or group in the Name box, and click Remove.

To add a user or group to the Name box, click Add.

5. In the Select Users, Computers, or Groups dialog box, double-click each user and group you want to add. (You can also highlight each user or group and then click Add, but double-clicking is faster and easier.) As you double-click each user or group, the user or group appears in the bottom portion of the dialog box. Click OK.
6. In the file or folder's Properties dialog box, each user or group you added is automatically assigned the Read and Read & Execute NTFS permissions to a file, or the Read, Read & Execute, and List Folder Contents NTFS permissions to a folder.

   To change the NTFS permissions of a user or group you added, highlight the user or group in the Name box, then select or clear the appropriate check boxes in the Permissions box.

   If you want this file or folder to inherit NTFS permissions from its parent folder, accept the default setting of "Allow inheritable permissions from parent to propagate to this object."

STEP BY STEP *Continued*

If you want to block inheritance of NTFS permissions from this file or folder's parent folder, clear the check box next to "Allow inheritable permissions from parent to propagate to this object."

CAUTION

Exercise care when blocking inheritance—you could end up denying yourself permission to access or assign permissions to the file or folder. If you intend to block inheritance, make sure you specifically assign yourself the Allow – Full Control NTFS permission to the file or folder *before* you block inheritance.

7. If you selected the check box next to "Allow inheritable permissions from parent to propagate to this object" in Step 6, the Security dialog box shown in Figure 11-13 appears.

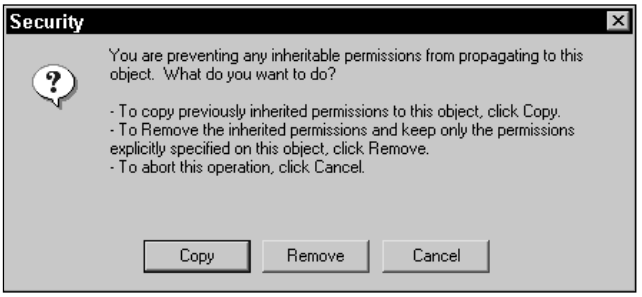

FIGURE 11-13 Copying or removing inherited permissions

If you want to keep all of this file or folder's inherited permissions, but convert them to explicit permissions instead of inherited permissions, click Copy.

If you want to delete all of this file or folder's inherited permissions, so that only the users and groups that you explicitly assign permissions to this file or folder remain, click Remove.

If you've changed your mind after all of this and decide you don't want to block inheritance after all, click Cancel.

8. In the file or folder's Properties dialog box, click OK.
9. Exit Windows Explorer.

The standard NTFS file and folder permissions I've talked about so far are used in most situations. The standard permissions actually consist of the most commonly used combinations of *special permissions*, which are sometimes called *advanced permissions*.

For example, the Read NTFS permission consists of the List Folder/Read Data, Read Attributes, and Read Extended Attributes special permissions. You might encounter a situation where assigning a special permission to a user or group for a file or folder would better accomplish your security goals than assigning a standard permission.

Special NTFS permissions are assigned by clicking the Advanced command button on the Security tab in a file or folder's Properties dialog box. Like regular NTFS permissions, special permissions are specifically allowed or denied to a specific user or group.

STEP BY STEP

CONFIGURING ADVANCED NTFS PERMISSIONS

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, expand folders as necessary until the file or folder to which you want to assign advanced NTFS permissions is displayed in the right pane. In the right pane, highlight that file or folder. Select File ➪ Properties. (Or, right-click the file or folder, and select Properties from the menu that appears.)
3. In the file or folder's Properties dialog box, click the Security tab.
4. On the Security tab, click Advanced.
5. The Access Control Settings dialog box for the file or folder appears, as shown in Figure 11-14. Notice the "Reset permissions on all child objects . . ." check box at the bottom of the dialog box. This check box is only available on folders—it is not available when configuring files.

CAUTION

Think twice before selecting the "Reset permissions on all child objects . . ." check box. If you select this check box, you will reset NTFS permissions on *all* subfolders and files of this folder to match the users, groups, and NTFS permissions set in the Permission Entries list box for *this* folder.

STEP BY STEP *Continued*

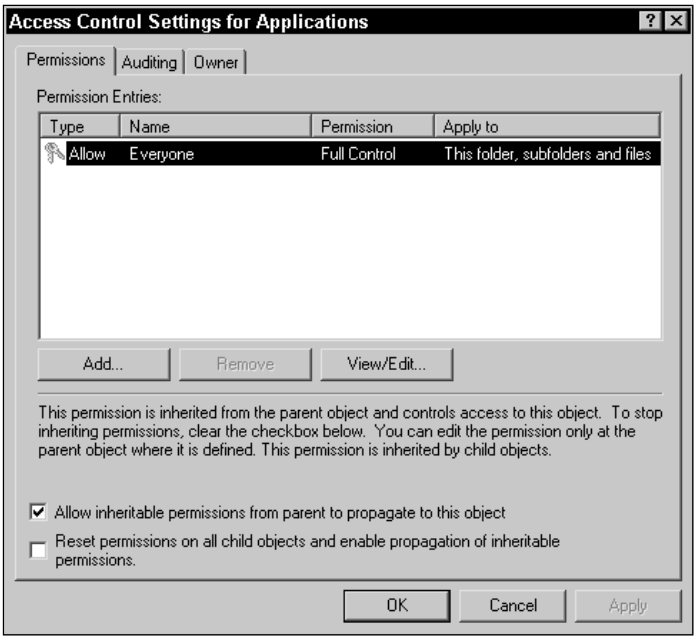

FIGURE 11-14 Configuring NTFS permissions and inheritance

When this check box is selected, permissions will even be reset on files and subfolders that are currently configured to block inheritance, and inheritance will be enabled on those files and subfolders.

To remove a user or group from the Permission Entries list box, highlight the user or group and click Remove.

To view or edit current NTFS permissions for a user or group, highlight the user or group and click View/Edit. Assign advanced permissions as appropriate. Click OK.

To add a user or group to the Permission Entries list box, click Add.

6. In the Select User, Computer, or Group dialog box, double-click the user or group you want to add.
7. The Permission Entry dialog box for the folder appears, as shown in Figure 11-15. Notice the long list of permissions in the Permissions list box—these are the special (or advanced) NTFS permissions.

   Assign special permissions to the user or group you added by selecting the appropriate Allow or Deny check boxes.

STEP BY STEP *Continued*

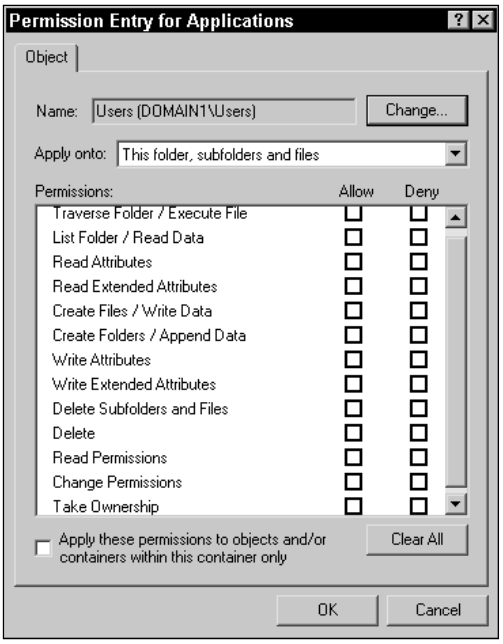

FIGURE 11-15 Setting special NTFS permissions

Then, select the appropriate option from the "Apply onto" drop-down list box. This setting determines how the permissions you set in this dialog box will be inherited. The possible selections are:

- This folder, subfolders and files—this is the default setting
- This folder only
- This folder and subfolders
- This folder and files
- Subfolders and files only
- Subfolders only
- Files only

The selection you make in this drop-down list box works in conjunction with the "Apply these permissions to objects and/or containers within this container only" check box at the bottom of the dialog box. If you select this check box (and any option in the "Apply onto" box that includes subfolders), the permissions you set will be applied to the subfolder, but *will not be applied to any files or folders within the subfolder*.

Click OK.

STEP BY STEP *Continued*

8. In the Access Control Settings dialog box for the file or folder, click OK.
9. In the file or folder's Properties dialog box, click OK.

How User and Group NTFS Permissions Combine

As with share permissions, it is not uncommon for a user to have one set of NTFS permissions to a file or folder, and to be a member of multiple groups that have different NTFS permissions to the file or folder. When this occurs, the user and group permissions are additive, and normally the *least restrictive* combination of permissions applies.

An exception to this rule occurs when a user is specifically *denied* an NTFS permission. *A denied permission always overrides an allowed permission*. Whenever a user is specifically denied a permission to a file or folder, or is a member of a group that is specifically denied a permission to a file or folder, the user is denied that permission to the file or folder. For example, if a user is allowed the Full Control NTFS permission to a file or folder, but is a member of a group that is denied the Full Control NTFS permission to that file or folder, the user is denied all access to the file or folder. For this reason, you should exercise care in denying a specific NTFS permission.

How NTFS Permissions Are Applied to New, Moved, and Copied Files and Folders

When new files or subfolders are created in a folder on an NTFS volume, the new files or subfolders inherit all of the inheritable NTFS permissions from the folder in which they are created. For example, if you create a new file in the `Public` folder, and the Everyone group is allowed the Modify NTFS permission to the `Public` folder, the new file inherits the NTFS permissions from the `Public` folder, and the Everyone group is allowed the Modify permission to the file.

When files or folders are moved or copied, their NTFS permissions often change. Normally, when files or folders are moved or copied, they inherit the inheritable NTFS permissions from the destination folder.

The only exception to this rule is when the moved files or folders are *moved to a new folder on the* same *NTFS volume* — in this case, the moved files or folders retain their original NTFS permissions, even if these permissions were inherited from the folder in which they were originally contained. In this situation, the moved files or folders do *not* inherit the NTFS permissions from the destination folder.

The following examples illustrate how NTFS permissions are applied to moved or copied files. The same rules apply to moved or copied folders.

Example 1: Moving a File to a Folder on a Different Volume

You move the `D:\Public\Readme.txt` file (to which the Everyone group is allowed the Read NTFS permission) to the `E:\Data` folder (to which the Everyone group is allowed the Full Control NTFS permission). When a file is moved to a folder on a different volume, it inherits the inheritable NTFS permissions from the destination folder. In this case, the `Readme.txt` file inherits the NTFS permission from the `E:\Data` folder, so the Everyone group is now allowed the Full Control NTFS permission to the `Readme.txt` file.

Example 2: Copying a File to a Different Folder on the Same Volume

You copy the `D:\Data\Busplan.doc` file (to which the Managers group is allowed the Read NTFS permission) to the `D:\Public` folder (to which the Everyone group is allowed the Modify permission, and the Managers group is not assigned any NTFS permissions). When a file is copied to a different folder on the same NTFS volume, the file inherits the inheritable NTFS permissions from the destination folder. Therefore, after the `Busplan.doc file` is copied to the `D:\Public` folder, the Everyone group is allowed the Modify NTFS permission to the file, and the Managers group is no longer assigned any NTFS permissions to the file.

Example 3: Moving a File to a Different Folder on the Same Volume

You move the `D:\Data\Forecast.doc` file (to which the Managers group is allowed the Read NTFS permission, and the Everyone group is not assigned any NTFS permissions) to the `D:\Public` folder (to which the Everyone group is allowed the Modify NTFS permission). When a file is moved to a folder on the same volume, it retains all of its original NTFS

permissions—it does *not* inherit the inheritable NTFS permissions from the destination folder. In this case, after the `Forecast.doc file` is moved, the Managers group is still allowed the Read NTFS permission to the file, and the Everyone group is not assigned any NTFS permissions to the file.

TIP

Because FAT and FAT32 volumes don't support NTFS permissions, any files or folders that you copy or move to a FAT or FAT32 volume lose all of their NTFS permissions, along with the security that those permissions provided.

How NTFS and Share Permissions Interact

When users access a file or folder (in a share located on an NTFS volume) over the network, *both* NTFS and share permissions are used to determine the user's effective permission to the file or folder in the share.

When NTFS and share permissions differ, the *most restrictive* permission becomes the user's effective permission to the file or folder in the share. This means that if *either* the NTFS or the share permissions deny a user access, access is denied.

The following two examples illustrate how NTFS and share permissions interact.

Example 1

A folder named `Documents` is shared on an NTFS volume. The Everyone group is allowed the Change share permission to the `Documents` share. In addition, the Everyone group is allowed the Full Control NTFS permission to all files and folders in the `Documents` share. Users who access the `Documents` share over the network are only allowed the Change permission to the files and folders in the share, because Change is the most restrictive permission.

Example 2

A folder named `Apps` is shared on an NTFS volume. The Everyone group is allowed the Full Control share permission to the `Apps` share. In addition, the Everyone group is allowed the Read NTFS permission to the files and folders in the `Apps` share. Users who access the `Apps` share over the

network only have the Read permission to the files and folders in this share, because Read is the most restrictive permission.

TIP

Remember, share permissions only apply when users connect to a share *over the network*. NTFS permissions are the only permissions that apply to users who log on locally to the computer that contains the share.

Keep in mind that when you combine share and NTFS permissions, both the share permissions and NTFS permissions must permit a user to perform a task. For example, if a user is allowed the Change share permission to a share, and also is allowed the Read NTFS permission to the shared folder, the user's effective permission to the share is Read, for two reasons. First, Read is the most restrictive permission. Second, the Change share permission includes the functionality of the Read permission, so in effect, both the share permission and NTFS permission grants the user the ability to Read.

Sometimes, however, there isn't any overlap between share and NTFS permissions, and the user ends up not having any effective permissions to a resource. For example, if a user has the Allow – Read share permission to a share, and also has the Allow – Write NTFS permission to the shared folder, the user won't be able to either Read or Write, because there is no overlap in the functionality of these two permissions.

Taking Ownership of Files and Folders

The creator of a file or folder is its *owner* (except that when a member of the Administrators group on the local computer creates a file or folder, the Administrators group — not the user — is the owner of the file or folder). The owner of a file or folder has special status and can always assign or change NTFS permissions to users and groups for that file or folder. Only files and folders on NTFS volumes have owners.

Occasionally you may need to change or assign permissions to a file or folder, but not have the Full Control NTFS permission (or the Change Permissions special NTFS permission) to the file or folder. Without being the owner of the file or folder, or having the Full Control or Change Permissions NTFS permission to the file or folder, the only way you change or assign permissions to the file or folder is to *take ownership* of the file or folder.

A common situation where taking ownership becomes necessary is when a user (who created a folder and was its owner) leaves the company, and no one else has the Full Control or Change Permissions NTFS permission to the folder. To change the permissions on the folder, the Administrator must first take ownership of it.

A user can take ownership of a file or folder only if one or more of the following criteria are met:

- The user is a member of the Administrators group on the local computer on which the file or folder is located. (If the computer is a domain controller, the user must be a member of the Administrators group in the domain.)
- The user has the Full Control or Change Permissions NTFS permission to the file or folder.
- The user has the "Take ownership of files or other objects" user right.

STEP BY STEP

TAKING OWNERSHIP OF A FILE OR FOLDER

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, expand folders as necessary until the file or folder you want to take ownership of is displayed in the right pane. In the right pane, highlight that file or folder. Select File ➪ Properties. (Or, right-click the file or folder, and select Properties from the menu that appears.)
3. In the file or folder's Properties dialog box, click the Security tab.
4. If you currently do not have permission to view or edit permissions to the file or folder, Windows 2000 displays a Security warning dialog box, as shown in Figure 11-16. Notice that the message indicates that you can take ownership. Click OK.

FIGURE 11-16 Security warning message

5. The Security tab in the file or folder's Properties dialog box is displayed. Click Advanced.

STEP BY STEP *Continued*

6. In the Access Control Settings dialog box for the file or folder, click the Owner tab.
7. The Owner tab is displayed, as shown in Figure 11-17. Notice that Windows 2000 is unable to display the current owner (because you don't have permissions to view the ownership information for the file or folder).

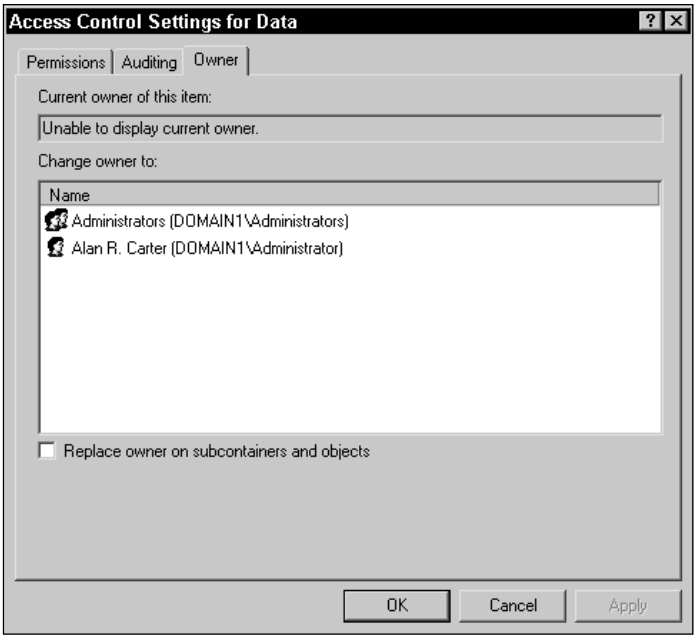

FIGURE 11-17 Taking ownership of a folder

In the "Change owner to" box, highlight the user (or group, if listed) that you want to become the new owner of the file or folder.

If you are taking ownership of a folder, and you also want to become the owner of all subfolders and files in this folder, select the check box next to "Replace owner on subcontainers and objects."

Click OK.

8. If you selected the check box next to "Replace owner on subcontainers and objects" in Step 7, Windows 2000 displays a security warning dialog box, indicating that you don't have permission to read the contents of the folder. The dialog box also asks if you want to grant yourself the Full Control permission to the folder and to all of its contents. Click Yes.
9. The Security tab reappears. Click OK.

Configuring and Monitoring Disk Quotas

Disk quotas are volume management mechanisms that are enabled on a volume-by-volume basis. Disk quotas are disabled by default. Once enabled, disk quotas automatically track disk space usage on a user-by-user basis, and can prevent individual users from exceeding the disk space limitations that an Administrator has assigned.

Disk quotas are normally only used on servers, although they can be used on any Windows 2000 computer. Enabling disk quotas puts an extra strain on the computer's processor. Because of this, you shouldn't enable disk quotas unless you have a need for them.

Disk quotas can only be used on NTFS volumes, because only NTFS volumes maintain ownership information on files and folders.

You can use Windows Explorer to configure and monitor disk quotas. Only members of the Administrators group on the local computer can configure disk quotas. (If the computer is a domain controller, the user must be a member of the Administrators group in the domain.)

STEP BY STEP

CONFIGURING AND MONITORING DISK QUOTAS

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, expand folders as necessary until the volume on which you want to configure disk quotas is displayed. Highlight that volume (such as `C:`, `D:`, and so on). Select File ➪ Properties. (Or, right-click the volume and select Properties from the menu that appears.)
3. In the volume's Properties dialog box, click the Quota tab.
4. On the Quota tab, select the check box next to "Enable quota management," as shown in Figure 11-18. (Remember, disk quotas are disabled by default.)

   There are several configurable options on this tab:

   - **Deny disk space to users exceeding quota limit:** If you select this check box, users are prevented from using more than their assigned amount of disk space. This option is not selected by default.
   - **Do not limit disk usage:** If you select this option, Windows 2000 will track disk space usage of this volume on a user-by-user basis, but it will not limit an individual's disk usage.

STEP BY STEP *Continued*

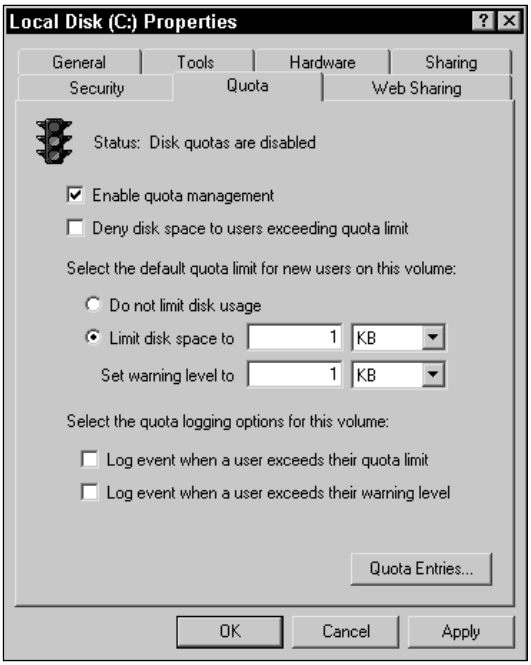

FIGURE 11-18 Enabling disk quotas

TIP

By default, once quotas are enabled, this option is selected, and disk space on this volume is limited to 1K per user. You'll almost certainly want to increase this setting.

- **Limit disk space to:** If you select this option, all users of this volume (that don't have an individual disk quota assigned) will be assigned a disk quota in the amount of disk space specified.

  Enforcement of this quota depends on whether the "Deny disk space to users exceeding quota limit" check box is selected.

  You can configure disk space limit on a user-by-user basis, thus allotting different users different amounts of disk space. I'll show you how to do this when I discuss Quota Entries later in this section.

- **Set warning level to:** This setting determines when Windows 2000 will generate a warning message in the Quota Entries dialog box (and in the System Log in Event Viewer if so configured). Users are not notified when they exceed their warning level. The warning level must be less than or equal to the user's disk space limit.

STEP BY STEP *Continued*

- **Log event when a user exceeds their quota limit:** If this check box is selected, Windows 2000 writes an event to the System Log in Event Viewer when the user exceeds the disk space limit.
- **Log event when a user exceeds their warning level:** If this check box is selected, Windows 2000 writes an event to the System Log in Event Viewer when the user exceeds the warning level limit.

Select and configure the appropriate options on this tab. Click Apply.

5. A Disk Quota warning dialog box is displayed. Click OK to enable the quota system.
6. On the Quota tab, click Quota Entries to view disk quota utilization for this volume and to configure disk space limits for individual users.
7. The Quota Entries dialog box for the volume appears, as shown in Figure 11-19. Notice the three types of indicators in the Status column: Above Limit, Warning, and OK.

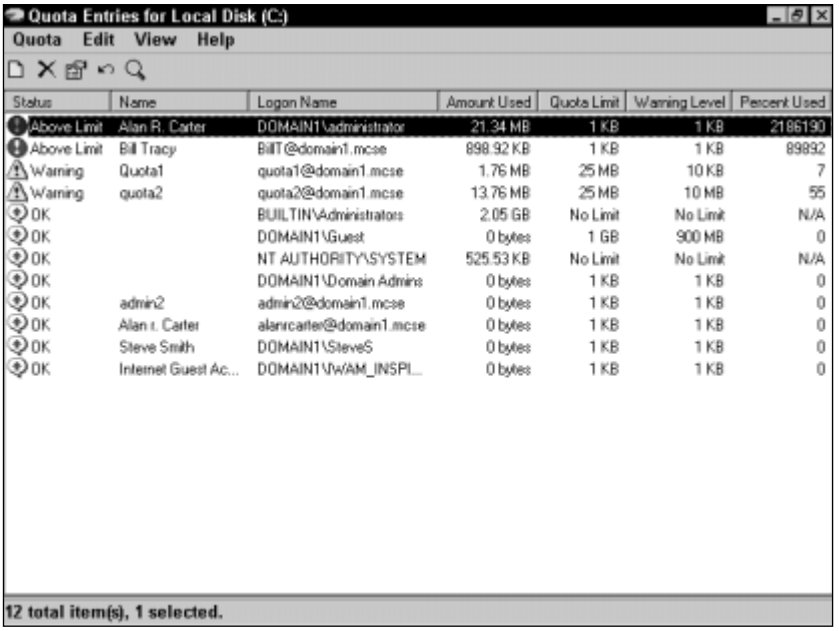

FIGURE 11-19 Monitoring disk quotas

This dialog box is primarily used for monitoring disk quota usage for individual users and groups. You can view the exact amount of disk space currently used by each user, as well as each user's disk quota limit, warning level, and percent of allowed disk space used.

STEP BY STEP *Continued*

In addition, you can modify the disk quota limit and warning level for any user or group listed in the dialog box. You can also add users to the dialog box and assign them disk quota limits.

To modify an individual user's disk quota limit, double-click the entry.

8. The Quota Settings dialog box for the user appears, as shown in Figure 11-20.

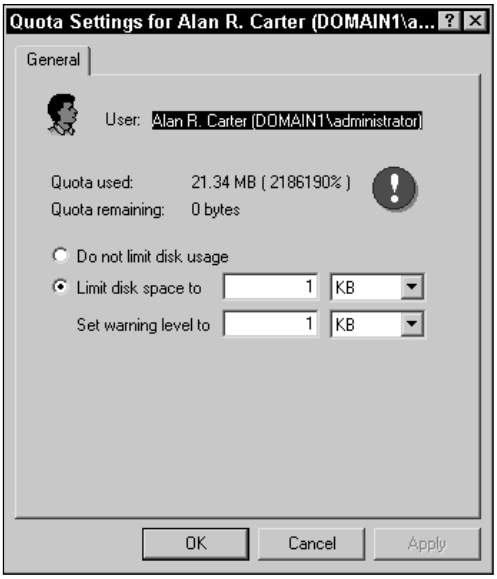

FIGURE 11-20 Configuring a user's disk quota

If you want Windows 2000 to track the user's disk usage, but you don't want to limit the user's disk usage, select the "Do not limit disk usage" option.

If you want to limit the user to a specific amount of disk space, select the "Limit disk space to" option and configure the user's limit. You should also configure the user's warning level—this level can't be greater than the user's disk space limit.

TIP

When an individual user is assigned a disk quota, the user won't be prevented from exceeding his or her assigned disk space limit unless the "Deny disk space to users exceeding quota limit" check box is selected on the Quota tab for the volume.

Click OK.

9. To add a user to the Quota Entries list, select Quota➪New Quota Entry in the Quota Entries dialog box.

STEP BY STEP *Continued*

10. In the Select Users dialog box, double-click the user you want to add. Click OK. (You can select more than one user to add, but if you do, you end up assigning them all identical disk space limits. Unless you want all users to have the same disk quota limit, add the users one at a time.)
11. In the Add New Quota Entry dialog box, make the appropriate disk limit configurations for the user you're adding and click OK.
12. The user is added to the top of the Quota Entries list. When you're finished configuring and monitoring disk quotas, close Quota Entries.
13. In the volume's Properties dialog box, click OK.

If you enable disk quotas on a volume, and configure Windows 2000 to deny disk space to users exceeding their quota limit, when a user takes any action that would exceed this limit, the user is notified that "there is not enough free disk space." This may happen when a user tries to save or copy a file or folder. It may even happen when the user attempts to log on if there is not enough space (in the user's quota) to create the user's profile.

IN THE REAL WORLD

Once, after I configured disk quotas, one of my users (a notorious disk hog) exceeded his disk quota and proceeded to create quite a stir in the office by telling everyone that the server's disk was full. It took me quite a while to calm everyone down and explain the situation.

Disk quotas can create problems if not configured appropriately. If you set disk space limits too low, you can hamper users' ability to perform their day-to-day tasks, because they won't be able to save or copy documents when they need to. You'll also have to deal with users telling you that the server's disk is full, when in fact the server is not full — the user has simply exceeded his or her disk quota limit.

Optimizing Access to Files and Folders

There is no one right way to optimize access to your network resources. However, there are several common-sense practices you can use to optimize access to files and folders. Consider using one or more of the following tips

to optimize security for network resources, to optimize administration of shared files and folders, and to optimize access to files and folders.

To optimize security for network resources:

- Consider making it a practice to always assign the most restrictive permission that still permits a user to accomplish the tasks he or she needs to perform.
- Consider storing important data on NTFS volumes instead of on FAT or FAT32 volumes because of the greater security possible on NTFS volumes.
- When you want to assign permissions to all users in the domain, consider assigning appropriate permissions to the Domain Users group and then removing the Everyone group from the permissions list (or access control list) to the resource. This closes up the security loophole that the Everyone group inherently produces.
- Always store data files and application files in different folders. This helps prevent accidental deletion of application files and simplifies backup and restore procedures.

To optimize administration of shared files and folders:

- When assigning permissions, assign permissions to groups, rather than individual users, when possible.
- When planning a folder structure (on an NTFS volume), keep inheritance in mind, and try to increase the amount of access users are allowed to a resource as you go farther down the tree. In other words, assign the most restrictive permissions at the top of the folder structure, and assign the least restrictive permissions toward the bottom of the tree. If you do this, you won't ever have to block inheritance.
- Consider assigning the Domain Admins global group the Full Control share permission to all shares, with the exception of users' home folders.
- In high-security environments, consider assigning the Domain Users group the Full Control or the Change share permission to shared folders, and using NTFS permissions to control access to individual files and folders within the shared folder. This prevents the administrative nightmare of always having to determine the most restrictive combination of share and NTFS permissions for

a given user or group to a resource. When this strategy is used, the NTFS permission to the file or folder is always the user's effective permission.

- In low-security environments, consider assigning the Domain Users group the Full Control NTFS permission to all files and folders on a volume, and using share permissions to control access to shared folders. This is the simplest way to control access to shared files and folders in a low security environment, because the share permission is always the user's effective permission to all contents of the share.
- Consider storing operating systems on a separate volume from data files, home folders, and applications. This makes backup, restore, and administration easier.

To optimize access to shared files and folders:

- Assign share names that are easily recognized by users, that appropriately describe the resources contained in the share, and that are of appropriate length (so users of *all* client computers can access the share).
- When users routinely log on to more than one Windows 2000 computer on the network, consider using roaming user profiles to optimize users access to their profiles.
- If roaming user profiles are used, consider redirecting the `My Documents` folder within users' profiles to a shared folder on a network server. This prevents the `My Documents` folder from being copied to and from the server each time the user logs on and logs off. If users use laptop computers and you redirect the `My Documents` folder, consider configuring "Automatic Caching for Documents" on the shared folder to which `My Documents` is redirected. (This will ensure that recently accessed documents are cached locally on users' computers, so that users can access the documents when their laptops aren't connected to the network.)
- If you use Dfs, consider making it a policy to use domain Dfs roots (instead of stand-alone Dfs roots) and to create at least one additional replica of each domain Dfs root. This will ensure that even if one of the servers that hosts the domain Dfs root is unavailable, users will still be able to access the Dfs root.

Troubleshooting Common Resource Access and Permission Problems

When a user can't access a resource (that he or she is supposed to be able to access), the administrator must determine why this is happening and correct the problem. Many resource access problems are caused by incorrectly configured or conflicting permissions.

Here are some recommended troubleshooting tips to help you solve various resource access and permission problems.

Problem 1: A User Can't Access Files in a Shared Folder

Ensure that the user (or a group that the user is a member of) is allowed permissions to the shared folder. Also look for conflicting share and NTFS permissions. To do this, you'll need to determine which groups the user is a member of (including groups in other domains), and determine the user's effective share permission and effective NTFS permissions to the shared folder. Finally, look for permissions that have specifically been denied to the user or to any groups to which the user belongs. Remember that a denied permission always overrides an allowed permission.

Problem 2: A New Group Member Can't Access a Share That Other Group Members Can Access

One of the simplest things you can do try to resolve this problem is to have the user log off and then log on again, so that the user's group membership information will be updated. You may also need to examine the new group member's other existing group memberships. It's possible that the user may be a member of another group that is denied access to the share.

Problem 3: A User Is Unable to Access a File After It Has Been Moved

This problem is likely the result of the file being moved to a different NTFS volume. When a file is moved to a different NTFS volume, the file loses all of its original NTFS permissions and inherits the inheritable NTFS permissions from the destination folder it is moved to. You may

need to reassign NTFS permissions to users or groups in order for them to access the moved file.

Problem 4: Users Report Slow Server Response When They Access a Shared Folder That Was Recently Compressed

Using compression places an increased load on the server's processor, thus slowing the server's response to users when they access compressed files and folders. Compression should only be used on files and folders that are accessed infrequently. If files and folders are accessed frequently, choose to add disk space instead of using compression.

Problem 5: Users Report That Their Files Are No Longer Encrypted After You Compress an NTFS Volume

Compression and encryption are mutually exclusive — you can use one or the other, but not both. If users require encryption, uncompress the folders users need to encrypt.

Problem 6: A User Reports That He Can't Locate a File That He Saved to a Domain Dfs Root Yesterday

The most likely cause of this problem is that the file was saved in a Dfs root, the file was *not* automatically replicated to the Dfs root replica(s), and the next day the user accessed a replica instead of the Dfs root. Determine whether automatic replication is configured between the Dfs root and its replica(s). If automatic replication is not configured, either configure automatic replication, or instruct users not to store files in the Dfs root.

Problem 7: Users Report That They Are Unable to Connect to a Stand-alone Dfs Root

The most likely cause of this problem is that the server that hosts the Dfs root is unavailable. Either bring the server back on line or consider using a domain Dfs root with a replica to provide fault tolerance.

KEY POINT SUMMARY

This chapter introduced several important Windows 2000 file and folder topics:

- Windows 2000 files and folders have various attributes, some of which the administrator can use to provide a limited amount of data protection. You can assign or change attributes by using Windows Explorer.
- In Windows 2000, folders are shared to enable users to access network resources. A shared folder appears in Windows Explorer as a folder with a hand under it. A shared folder is often referred to as a share.
- Shared folder permissions (often called share permissions) control user access to shared folders, and only apply when users connect to the folder over the network.
- When user and group permissions conflict, the permissions are additive, and normally the least restrictive permission is the user's effective permission. However, there is an exception: a denied permission always overrides an allowed permission.
- The Distributed file system (Dfs) enables an administrator to make shares that are stored on various servers on the network appear to users as though they are stored within a single share on a single server. This makes finding network resources easier for users.
- A Dfs root is a special type of shared folder that can contain files, folders, Dfs links, and other Dfs roots. A Dfs link is a special type of subfolder in a Dfs root that acts as a pointer to a specific shared folder on the network.
- NTFS permissions, which can only be assigned to files and folders on NTFS volumes, protect data from unauthorized access when users connect to the share locally or over the network. There are standard and special NTFS permissions.
- When NTFS and share permissions differ, the most restrictive permission becomes the user's effective permission to the file or folder in the share. If either the NTFS or the share permissions deny a user access, access is denied.
- If the Administrator needs to change the permissions assigned to a file or folder, but doesn't have the Full Control or Change Permissions NTFS permission to the file or folder, the Administrator must take ownership of the file or folder.

- Disk quotas are volume management mechanisms that, once enabled, automatically track disk space usage on a user-by-user basis, and can prevent individual users from exceeding the disk space limitations they have been assigned by an Administrator.

STUDY GUIDE

This section contains several exercises that are designed to solidify your knowledge about sharing, securing, and accessing files and folders on the network, and to help you prepare for the Windows 2000 Professional and Server exams:

- **Assessment questions:** These questions test your knowledge of the various Windows 2000 file and folder topics covered in this chapter. You'll find the answers to these questions at the end of this chapter.
- **Scenarios:** The situation-based questions in scenarios challenge you to apply your understanding of the material to solve a hypothetical problem. In this chapter's scenario, you are asked to troubleshoot and optimize various situations involving access to shared files and folders. You don't need to be at a computer to do scenarios. Answers to this chapter's scenarios are presented at the end of this chapter.
- **Lab exercises:** These exercises are hands-on practice activities that you perform on a computer. The lab in this chapter gives you an opportunity to practice several common Windows 2000 file and folder tasks.

Assessment Questions

1. You want to protect application files located on an NTFS volume on a Windows 2000 computer so that users can't accidentally delete these files. Which attribute should you assign to the application files?
   A. Hidden
   B. System
   C. Encrypt
   D. Read-only
2. You want to share a folder located on a FAT32 volume on a Windows 2000 computer. Which tool should you use?
   A. System Tools
   B. Folder Options
   C. Windows Explorer

D. Local Security Policy

3. You want to map a network drive on your Windows 2000 client computer to a folder named `Invoices` that is stored in a share named `Accounting` on a Windows 2000 Server computer named Corp02. What UNC name should you specify?

   A. `\\CORP02\Accounting`

   B. `\\CORP02\Accounting\Invoices`

   C. `C:\CORP02\Accounting`

   D. `E:\CORP02\Accounting\Invoices`

4. You want to prevent the creation of administrative shares on a Windows 2000 Server computer. What should you do?

   A. Nothing. You can't prevent the creation of administrative shares.

   B. Configure the Advanced options in Configure Your Server.

   C. Configure the Advanced settings on the View tab in Folder Options.

   D. Use `Regedt32.exe` or the System Policy Editor to edit the registry.

5. JeffB is allowed the Full Control share permission to a folder named `Payroll`. Jeff is a member of three groups, which have the following share permissions to the `Payroll` folder:

Group	Share Permission to the `Payroll` Folder
Domain Users	No permissions assigned
Accounting	Allow – Change
Managers	Allow – Read

   What is JeffB's effective permission to the `Payroll` folder?

   A. Allow – Read

   B. Allow – Change

   C. Allow – Full Control

   D. Deny – Full Control

6. You want to assign NTFS permissions to a shared folder located on an NTFS volume on a Windows 2000 Server computer. Which tool should you use?

A. Windows Explorer

B. Disk Management

C. Folder Options

D. System Tools

7. You move a file from an NTFS volume on a Windows 2000 client computer to a folder on an NTFS volume on a Windows 2000 Server computer. What effect does moving this file have on the NTFS permissions assigned to the file?

   A. The moved file retains all of its original NTFS permissions.

   B. The moved file loses all of its original NTFS permissions, and now has no permissions.

   C. The moved file loses some of its original NTFS permissions, and inherits some of the NTFS permissions from its destination folder.

   D. The moved file loses all of its original NTFS permissions, and inherits all of the inheritable NTFS permissions from its destination folder.

8. BetsyR is a member of one group, Technicians, that is allowed the Full Control share permission to the `Support` share. BetsyR is a member of another group, Managers, that is allowed the Modify NTFS permission to the `Support` share. BetsyR is *not* assigned any specific share or NTFS permissions as an individual user. What is BetsyR's effective permission to the `Support` share?

   A. Allow – Modify

   B. Allow – Full Control

   C. Allow – Read & Execute

   D. Deny – Full Control

Scenarios

The following scenarios provide you with an opportunity to apply the knowledge you've gained in this chapter about working with files and folders in a Windows 2000 environment.

Users can have difficulty accessing shared resources for a number of reasons. For each of the following problems, consider the given situation and facts, and state what course of action you would take to try to resolve the problem or optimize the situation.

1. A user, NancyW, reports that she can't save files to the `AccountingData` share located on an NTFS volume on a Windows 2000 computer. NancyW is a member of the following groups that have various share and NTFS permissions to the `AccountingData` share.

Group	Share Permissions Assigned for AccountingData	NTFS Permissions Assigned for AccountingData
Everyone	Allow – Read	No permissions assigned
Accounting	No permissions assigned	Allow – Full Control
Domain Users	No permissions assigned	Allow – Read

2. A user reports that her personal, sensitive data files are no longer encrypted. You just enabled compression on the NTFS volume on the Windows 2000 Server computer that contains the user's data files.
3. A user, JohnS, has worked at your company as a sales representative for five years. JohnS was recently made a manager of the company. He reports that he can't access the `ManagersData` share located on an NTFS volume on a Windows 2000 computer. John is a member of several groups that have various NTFS permissions to the `ManagersData` share.

Group	NTFS Permissions Assigned for ManagersData
Administrators	Allow – Full Control
Managers	Allow – Modify
Sales	Deny – Full Control

4. Users report that they cannot access the `Data` stand-alone Dfs root that is hosted by a Windows 2000 Server computer named Server03.
5. Yesterday you saved a file in a domain Dfs root. Today, when you map a network drive to the domain Dfs root, the file is not listed in the contents of the Dfs root.
6. Several users in your company report that they are having difficulty locating shared folders that contain documents they need to access to perform their daily tasks.

Lab Exercises

The following lab is designed to give you practical experience working with files and folders in a Windows 2000 environment.

Lab 11-1 Sharing, Securing, and Accessing Files and Folders

- ► Professional
- ► Server

The purpose of this lab is to provide you with an opportunity to practice configuring, managing, sharing, securing, and accessing files and folders on a Windows 2000 computer.

There are five parts to this lab:

- Part 1: Sharing Folders and Configuring Share and NTFS Permissions
- Part 2: Configuring a Dfs Root and Connecting to Shared Resources
- Part 3: Configuring Data Compression
- Part 4: Configuring Data Encryption
- Part 5: Configuring and Monitoring Disk Quotas

Begin this lab by booting your computer to Windows 2000 Server and logging on as Administrator.

Part 1: Sharing Folders and Configuring Share and NTFS Permissions

In this part, you use Windows Explorer to create and share several folders. Then you assign share and NTFS permissions to these folders.

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, click the + next to My Computer. Highlight Local Disk (C:). Select File ➪ Properties.
3. In the Local Disk (C:) Properties dialog box, click the Security tab.
4. On the Security tab, click Add.
5. In the Select Users, Computers, or Groups dialog box, scroll down and double-click the Domain Admins group. Click OK.
6. On the Security tab, highlight the Domain Admins group. Select the Allow check box next to the Full Control permission. Highlight the Everyone group and click Remove. Click OK.
7. In Windows Explorer, select File ➪ New ➪ Folder.
8. In the right pane, type in a new folder name of **SharedData** and press Enter.
9. Double-click the newly created `SharedData` folder. Select File ➪ New ➪ Folder.
10. In the right pane, type in a new folder name of **Managers** and press Enter.
11. Select File ➪ New ➪ Folder.
12. In the right pane, type in a new folder name of **Accounting** and press Enter.
13. Select File ➪ New ➪ Folder.
14. In the right pane, type in a new folder name of **Sales** and press Enter. You should now have three new folders in the right pane, named `Managers`, `Accounting`, and `Sales`.
15. In the right pane, highlight the `Managers` folder. Select File ➪ Sharing.
16. In the Managers Properties dialog box, select the option next to "Share this folder." Type **ManagersData** in the "Share name" text box. Click Permissions.

17. In the Permissions for ManagersData dialog box, notice that the Everyone group is allowed the Full Control share permission to the folder. Click Add.
18. In the Select Users, Computers, or Groups dialog box, scroll down and double-click the Domain Users group. Click OK.
19. In the Permissions for ManagersData dialog box, highlight the Domain Users group, and select the Allow check box for the Full Control permission. Highlight the Everyone group, and click Remove. Click OK.
20. In the Managers Properties dialog box, click the Security tab.
21. On the Security tab, click Add.
22. In the Select Users, Computers, or Groups dialog box, scroll down and double-click the Managers group. Click OK.
23. On the Security tab, highlight the Managers group. Select the Allow check box next to the Full Control NTFS permission. Click OK.
24. In the right pane, highlight the `Accounting` folder. Select File➪ Sharing.
25. In the Accounting Properties dialog box, select the option next to "Share this folder." Type **AccountingData** in the "Share name" text box. Click Permissions.
26. In the Permissions for AccountingData dialog box, click Add.
27. In the Select Users, Computers, or Groups dialog box, scroll down and double-click the Domain Users group. Click OK.
28. In the Permissions for AccountingData dialog box, highlight the Domain Users group, and select the Allow check box for the Full Control permission. Highlight the Everyone group, and click Remove. Click OK.
29. In the Accounting Properties dialog box, click the Security tab.
30. On the Security tab, click Add.
31. In the Select Users, Computers, or Groups dialog box, scroll down and double-click the Accountants group. Then double-click the Managers group. Click OK.
32. On the Security tab, highlight the Managers group. Select the Allow check box next to the Full Control NTFS permission. Then highlight the Accountants group. Select the Allow check box next to the Modify NTFS permission. Click OK.

33. In the right pane, highlight the `Sales` folder. Select File ➪ Sharing.
34. In the Sales Properties dialog box, select the option next to "Share this folder." Type **SalesData** in the "Share name" text box. Click Permissions.
35. In the Permissions for SalesData dialog box, click Add.
36. In the Select Users, Computers, or Groups dialog box, scroll down and double-click the Domain Users group. Click OK.
37. In the Permissions for SalesData dialog box, highlight the Domain Users group, and select the Allow check box for the Full Control permission. Highlight the Everyone group, and click Remove. Click OK.
38. In the Sales Properties dialog box, click the Security tab.
39. On the Security tab, click Add.
40. In the Select Users, Computers, or Groups dialog box, scroll down and double-click the Managers group. Then double-click the Sales group. Click OK.
41. On the Security tab, highlight the Managers group. Select the Allow check box next to the Full Control NTFS permission. Then highlight the Sales group. Select the Allow check box next to the Modify NTFS permission. Click OK.

    You've now shared the three new folders, and assigned both share and NTFS permissions to these shared folders. Close Windows Explorer.

Part 2: Configuring a Dfs Root and Connecting to Shared Resources

In this part, you use the Distributed File System tool to create and configure a Dfs root and three Dfs links to the shared folders you created in Part 1. Then you map a network drive to connect to the Dfs root.

1. Start the Distributed File System tool. (Select Start ➪ Programs ➪ Administrative Tools ➪ Distributed File System.)
2. In the Distributed File System dialog box, select Action ➪ New Dfs Root.
3. The New Dfs Root Wizard starts. Click Next.
4. In the Select the Dfs Root Type screen, select the "Create a standalone Dfs root" option. Click Next.

5. In the Specify the Host Server for the Dfs Root screen, accept the default Server name of server01.domain1.mcse. Click Next.
6. In the Specify the Dfs Root Share screen, select the "Create a new share" option. In the "Path to share" text box, type **C:\Data**. In the "Share name" text box, type **Data** and click Next.
7. Windows 2000 asks if you want to create the `C:\Data` folder. Click Yes.
8. In the Name the Dfs Root screen, enter a Comment of **Company Shared Data**. Click Next.
9. In the Completing the New Dfs Root Wizard screen, click Finish.
10. Windows 2000 creates the new Dfs root. It appears in the left pane in the Distributed File System dialog box. Highlight the new Dfs root named `\\SERVER01\Data` and select Action ➪ New Dfs Link.
11. In the Create a New Dfs Link dialog box, type in a Link name of **ManagersData**. In the "Send the user to this shared folder" text box, type **\\Server01\ManagersData**. Click OK.
12. The new Dfs link appears in the left pane. Highlight the Dfs root named `\\SERVER01\Data` and select Action ➪ New Dfs Link.
13. In the Create a New Dfs Link dialog box, type in a Link name of **AccountingData**. In the "Send the user to this shared folder" text box, type **\\Server01\AccountingData**. Click OK.
14. The new Dfs link appears in the left pane. Highlight the Dfs root named `\\SERVER01\Data` and select Action ➪ New Dfs Link.
15. In the Create a New Dfs Link dialog box, type in a Link name of **SalesData**. In the "Send the user to this shared folder" text box, type **\\Server01\SalesData**. Click OK.
16. The new Dfs link appears in the left pane.You've now created a Dfs root and three Dfs links. Close the Distributed File System.
17. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
18. In the left pane, click the + next to My Computer. Select Tools ➪ Map Network Drive.
19. In the Map Network Drive dialog box, select a Drive letter of V: (from the Drive drop-down list box) and type in a Folder name of **\\Server01\Data**. Click Finish.

20. Windows 2000 connects you to the Dfs root, and displays the Data on Server01 dialog box. Notice the three folders in the right pane. These folders correspond to the three Dfs links you created. If you open one of these folders, Dfs will automatically open the shared folder associated with the Dfs link. Close both Windows Explorer dialog boxes.

Part 3: Configuring Data Compression

In this part, you use Windows Explorer to assign the Compress attribute to a folder and all of its files. After observing the change in disk space used by the folder, you remove the Compress attribute from the folder and all of its files.

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, click the + next to My Computer. Highlight Local Disk (C:). In the right pane, highlight the `Program Files` folder. Select File ➪ Properties.
3. In the Program Files Properties dialog box, notice the "Size on disk" information. Click Advanced.
4. In the Advanced Attributes dialog box, select the check box next to "Compress contents to save disk space." Click OK.
5. In the Program Files Properties dialog box, click Apply.
6. A Confirm Attribute Changes dialog box appears. Select the "Apply changes to this folder, subfolder and files" option. Click OK.
7. Windows 2000 applies the Compress attribute and compresses all files in the folder. This may take several minutes. If an Error Applying Attributes dialog box appears, click Ignore All.

   In the Program Files Properties dialog box, notice the "Size on disk" entry now. The size should have decreased substantially. Click Advanced.
8. In the Advanced Attributes dialog box, clear the check box next to "Compress contents to save disk space." Click OK.
9. In the Program Files Properties dialog box, click OK.
10. In the Confirm Attribute Changes dialog box, select the "Apply changes to this folder, subfolder and files" option. Click OK.
11. Windows 2000 removes the Compress attribute, and uncompresses all of the files in the folder. Continue on to Part 4.

Part 4: Configuring Data Encryption

In this part, you use Windows Explorer to first create a folder and a file, and then to assign the Encrypt attribute to the folder and its contents. Then you test encryption by trying to access the file while logged on as a different user.

1. In the left pane of Windows Explorer, highlight the `My Documents` folder. Select File ➪ Properties.
2. In the My Documents Properties dialog box, click the General tab.
3. On the General tab, click Advanced.
4. On the Advanced Attributes tab, select the check box next to "Encrypt contents to secure data." Click OK.
5. On the General tab, click OK.
6. In the Confirm Attribute Changes dialog box, select the "Apply changes to this folder, subfolders and files" option. Click OK.
7. Windows 2000 applies the Encrypt attribute and encrypts all of the files in the folder. Select File ➪ New ➪ Text Document.
8. In the right pane, type in a name for the new text document of **Encrypted.txt** and press Enter. Double-click the `Encrypted.txt` file.
9. In the Encrypted.txt - Notepad dialog box, type in the following text:

   This file is encrypted!

   Select File ➪ Save. Select File ➪ Exit.
10. Close Windows Explorer.
11. Select Start ➪ Shut Down.
12. In the Shut Down Windows dialog box, select "Log off administrator" from the drop-down list box. Click OK.
13. Press Ctrl+Alt+Delete.
14. In the Log On to Windows dialog box, type in a User name of **SteveS** and a password of **password**. (Remember that SteveS, a user you created in Chapter 9, is a member of the Domain Admins group. He should have the Full Control NTFS permissions to all files and folders on the local computer.) Click OK.
15. From the desktop, start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)

16. In the left pane, click the + next to My Computer. Highlight Local Disk (C:). Click the Search command button in the toolbar. In the "Search for files or folders named" text box, type **Encrypted.txt** and click Search Now.
17. In the right pane, double-click the `Encrypted.txt` file.
18. A Notepad warning dialog box appears, indicating that access is denied. Even though SteveS has permissions to all files and folder on the local computer, he is unable to open this file because it is encrypted. Click OK.
19. Close the Untitled - Notepad dialog box.
20. Close Windows Explorer.
21. Select Start ➪ Shut Down.
22. In the Shut Down Windows dialog box, select "Log off SteveS" from the drop-down list box. Click OK.
23. Press Ctrl+Alt+Delete.
24. In the Log On to Windows dialog box, type in a User name of **Administrator** and a password of **password**. Click OK.

Part 5: Configuring and Monitoring Disk Quotas

In this part, you use Windows Explorer to configure and monitor disk quotas.

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, click the + next to My Computer. Highlight Local Disk (C:). Select File ➪ Properties.
3. In the Local Disk (C:) Properties dialog box, click the Quota tab.
4. On the Quota tab, select the check box next to "Enable quota management." Accept the default "Limit disk space to" option. Configure this option to 25MB. Set the warning level to 20MB. Click Apply.
5. In the Disk Quota warning dialog box, click OK to enable the quota system now.
6. On the Quota tab, click Quota Entries.
7. In the Quota Entries dialog box for Local Disk (C:), notice the users and groups listed, their respective quota limits, and the percent of their quotas used. Select Quota ➪ New Quota Entry.

8. In the Select Users dialog box, double-click Colleen Green and click OK.
9. In the Add New Quota Entry dialog box, accept the default "Limit disk space to" option and configure a disk space limit of 10MB and a warning level of 1MB. Click OK.
10. Notice the new entry in the Quota Entries dialog box for Local Disk (C:). Close the Quota Entries dialog box.
11. In the Local Disk (C:) Properties dialog box, click OK.
12. Close Windows Explorer.

Answers to Chapter Questions

Chapter Pre-Test

1. The seven Windows 2000 file and folder attributes are: Archive, Compress, Encrypt, Hidden, Index, Read-only, and System.
2. A shared folder appears in Windows Explorer with a hand under it.
3. User and group share permissions are *additive,* and normally the *least* restrictive permission is the user's effective permission.
4. When NTFS and share permissions differ, the *most* restrictive permission becomes the user's effective permission to the file or folder in the share.
5. Disk quotas are used to automatically track disk space usage by users and to prevent individual users from exceeding the disk space limitations assigned to them by an Administrator.

Assessment Questions

1. **D.** Assign the Read-only attribute to application files to protect them from accidental deletion by users.
2. **C.** Windows Explorer is used to share folders on Windows 2000 computers.
3. **B.** UNC names are specified in the format:

   ```
   \\Server_name\Share_name\Subfolder_name\File_name
   ```

4. **D.** Edit the registry to prevent the creation of administrative shares.

5. **C.** User and group share permissions are additive, and the *least restrictive* permission is typically the user's effective permission.
6. **A.** Windows Explorer is used to assign NTFS permissions to files and folders.
7. **D.** When a file or folder is moved to a new folder on a different volume, it inherits all of the inheritable NTFS permissions from the destination folder.
8. **A.** When share and NTFS permissions combine, the most restrictive permission is applied.

Scenarios

1. When share and NTFS permissions combine, the most restrictive permission is applied. In this case, NancyW's effective permission to the `AccountingData` share is Read. To enable NancyW to save files to the share, you could assign the Allow – Full Control share permission to the Accounting group for the `AccountingData` share. This would give the Accounting group the Full Control share permission and the Full Control NTFS permission to the `AccountingData` share (for an effective permission of Full Control).
2. Compression and encryption are mutually exclusive — you can use one or the other, but not both. A possible solution for this case, if the user requires encryption, would be to uncompress the folder that contains the user's sensitive data files.
3. JohnS is unable to access the `ManagersData` share because he is a member of a group that is specifically denied access to this share. To solve the problem, you could remove the Sales group from the access control list to the `ManagersData` folder. Or, you could remove JohnS from the Sales group.
4. Determine whether Server03 is accessible on the network. If not, take the action to bring it back on line. Another possible solution that will prevent this problem from recurring would be to implement a domain Dfs root with a replica to provide fault tolerance.

5. The most likely cause of this problem is that the file was saved in one replica of the domain Dfs root, the file was *not* automatically copied to the Dfs root replicas, and today you accessed a different replica of the Dfs root. To solve the problem, first determine whether automatic replication is configured between the Dfs root and its replicas. If automatic replication is not configured, either configure automatic replication, or discontinue your practice of saving files in the Dfs root.
6. One solution to this problem would be to assign more intuitive names to shared folders so that users can quickly locate the resources they need. Another possible solution is to make shares from multiple servers available in a single Dfs root.