Workstation
Server
Enterprise

CHAPTER

Sharing and Securing File Systems

12

About Chapter 12

This chapter focuses on sharing and securing files and folders on a network. After some introductory information about file and folder attributes, we'll get right to the nitty-gritty of sharing folders. You'll learn how to share a folder and how to modify a share. Share permissions are explained, including how to assign them, and how user and group permissions combine.

Next, we explore NTFS permissions. You'll learn 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 this chapter presents tips for planning a strategy for sharing and securing your network resources. Finally, we discuss auditing files and folders on NTFS partitions, and tips for troubleshooting common resource access and permission problems.

This chapter includes three hands-on labs. In the first lab, you'll plan a strategy for sharing and securing resources, and then actually implement that strategy. In the second, you'll establish file and folder auditing. In the third, you'll troubleshoot some common resource access and permission problems.

Chapter 12 is a "must read" no matter which of the three Windows NT 4.0 Microsoft Certified Professional exams you're preparing for. This chapter covers shared resource objectives in the Planning, Managing Resources, and Troubleshooting sections in these exams' objectives.

Managing File and Folder Attributes

Windows NT files and folders have various *attributes*, some of which the administrator can use to provide a limited amount of data protection. For example, administrators often use the read-only file attribute to prevent accidental deletion of files, such as application files. Other file and folder attributes are applied by Windows NT system files automatically during installation.

File attributes can be used on both FAT and NTFS partitions, with the exception of the Compress attribute, which is only available on NTFS partitions.

Table 12-1 lists and describes the five Windows NT file and folder attributes.

TABLE 12-1 WINDOWS NT 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. Is normally not changed by the administrator.
Compress	Indicates that Windows NT has compressed the file or folder. Is only available on NTFS partitions. Uses the same compression algorithm as the MS-DOS 6.0 DoubleSpace utility. Can be set on individual files. Is applied by administrators to control which files and folders will be compressed.
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 applied to various files and folders by NT automatically during installation.
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. Files or folders with this attribute can't be copied or deleted. Is applied to various files and folders by NT automatically during installation.

Any user who can access a file or folder on a FAT partition can modify that file or folder's attributes. Any user who has the Write (W) NTFS permission (or any permission that includes the Write (W) permission) to a file or folder on an NTFS partition can modify that file or folder's attributes. (NTFS permissions are covered later in this chapter.)

On NTFS volumes, when a file or folder has the Read-only attribute, and the file or folder also has the Write (W) NTFS permission for a user or group, the

Read-only attribute takes precedence. The Read-only attribute must be removed before the file can be modified or deleted. The next section describes how to change file or folder attributes, and how to assign file or folder attributes.

TO CHANGE OR ASSIGN FILE OR FOLDER ATTRIBUTES, FOLLOW THESE STEPS:

1. Select Start➢Programs➢Windows NT Explorer.
2. In the Exploring dialog box, highlight the file or folder on which you want to change attributes or to which you want to assign attributes.
3. Select File➢Properties. (Or, you can right-click the file or folder, and select Properties from the menu that appears.)
4. The *File_name* or *Folder_name* Properties dialog box appears, as shown in Figure 12-1. Notice the System attribute is grayed out and can't be changed using this interface. Also notice the four attributes that are available: Read-only, Archive, Compress, and Hidden.

FIGURE 12-1 **Setting file or folder attributes**

5. Select the check boxes next to the attributes you want to assign. (Or, clear the check boxes next to attributes you want to remove.) Click OK.
6. Exit Windows NT Explorer.

Managing Shared Folders

In Windows NT, 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 NT Explorer and My Computer as a folder with a hand under it. A shared folder is often referred to as a *share*.

Only members of the Administrators, Server Operators, and Power Users built-in local groups can share folders.

The following sections discuss how to share a folder, shared folder permissions and how to assign them, how to modify a share, how to stop sharing a folder, and administrative shares and how to prevent their automatic creation by Windows NT.

Sharing a Folder

Only certain users can share folders. Members of the Administrators local group can share folders on any Windows NT computer; members of the Server Operators group can share folders on all Windows NT domain controllers; and members of the Power Users group can share folders on all Windows NT non-domain controllers, including Windows NT Workstation computers.

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 groups and users 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 find 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 up to eight characters (plus a three-character extension), and Windows 95 computers can only read share names up to twelve characters. Share names in Windows NT can be as long as eighty characters.

You can use either Windows NT Explorer or Server Manager to share folders.

The next sections explain the steps involved in sharing a folder, first by using Windows NT Explorer, and then by using Server Manager.

You can use Windows NT Explorer to share folders only on the local computer; however, you can use Server Manager to share folders both locally and on remote computers.

TO SHARE A FOLDER USING WINDOWS NT EXPLORER, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Windows NT Explorer.
2. In the Exploring dialog box, highlight the folder you want to share. Select File ➢ Properties. (Or, right-click the folder and select Sharing from the menu that appears. Skip to Step 4.)
3. In the *Folder_name* Properties dialog box, click the Sharing tab.
4. On the Sharing tab, select the radio button next to Shared As. Either accept the default name in the Share Name text box or type in the name you want to use for the share. Figure 12-2 shows the Sharing tab in the Data Properties dialog box. Note that the radio button next to Shared As is selected.

   You can add a descriptive comment about the share in the Comment text box if you so choose. (This is an optional setting.)

   If you want to limit the number of users who can connect to this share simultaneously (because of licensing limitations and such) you can configure the User Limit section on the Sharing tab. The default User Limit setting is Maximum Allowed.

   Click OK.

FIGURE 12-2 **Using Windows NT Explorer to share a folder**

5. The Exploring dialog box reappears. A hand appears under the folder you shared, indicating that it is a shared folder. Exit Windows NT Explorer.

TO SHARE A FOLDER USING SERVER MANAGER, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Administrative Tools (Common) ➢ Server Manager.
2. In the Server Manager dialog box, highlight the computer that contains the folder you want to share. Select Computer ➢ Shared Directories.
3. In the Shared Directories dialog box, click the New Share command button.
4. The New Share dialog box appears, as shown in Figure 12-3. Notice the various configuration options in the dialog box.

FIGURE 12-3 **Using Server Manager to share a folder**

In the Share Name text box, type in the name you want to assign to the new share. Then, in the Path text box, type in the full path to the share, in the form of *`Drive_letter:\Folder\subfolder\...`* For example, to share the CD-ROM drive on a remote Windows NT computer that uses E: as the drive letter, you would type **E:\** in the Path text box.

You can enter a descriptive comment about the share in the Comment text box if you so choose. If you want to limit the number of users that can connect to this share simultaneously you can configure the User Limit section.

Click OK.

5. The new share appears (with a hand under it) in the Shared Directories dialog box. Click the Close command button.
6. Exit Server Manager.

If you want to restrict user access to the folders that you have shared, you can assign shared folder permissions.

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 from 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 partition (with the exception of file attributes), and control only over-the-network access to the share—local access is totally unrestricted on a FAT partition.

Table 12-2 lists and describes the Windows NT share permissions, from the most restrictive to the least restrictive.

TABLE 12-2 WINDOWS NT SHARE PERMISSIONS

PERMISSION	DESCRIPTION
No Access	Permits a user to connect to a share only, but prevents a user from accessing the shared folder and its contents.
Read	Permits a user to view file and folder names.
	Permits a user to change current folder to a subfolder of the share.
	Permits a user to view data in files; and to run application files.
Change	Permits a user to perform all tasks included in the Read permission.
	Permits a user to create files and folders within the share; to edit data files and save changes; and to delete files and folders within the share.
Full Control	Permits a user to perform all tasks included in the Change permission.
	Permits a user to change NTFS permissions (discussed later in this chapter)—this only applies to shares on NTFS partitions; and
	Permits a user to take ownership of files and folders—this only applies to shares on NTFS partitions.

Share permissions are assigned by adding a user or group to the permissions list for the share. From an administrative standpoint, it's much 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 allows 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 assign share permissions by using Windows NT Explorer or Server Manager. The next section explains how to assign share permissions using Windows NT Explorer.

TO ASSIGN SHARE PERMISSIONS BY USING WINDOWS NT EXPLORER, FOLLOW THESE STEPS:

1. Select Start ⋗ Programs ⋗ Windows NT Explorer.
2. In the Exploring dialog box, highlight the shared folder to which you want to assign permissions. Select File ⋗ Properties.
3. In the *Folder_name* Properties dialog box, click the Sharing tab.
4. On the Sharing tab, click the Permissions command button.
5. The Access Through Share Permissions dialog box appears, as shown in Figure 12-4. Notice that, by default, the Everyone group has Full Control.

   Click the Add command button.

FIGURE 12-4 **Assigning share permissions**

6. The Add Users and Groups dialog box appears, as shown in Figure 12-5. Notice that only group names from the WEST domain appear in the Names list box.

   If you want to add global groups and users from other trusted domains, click the arrow in the List Names From drop-down list box and select the domain you want. If you want to add individual users, click the Show Users command button. Double-click the group or user you want to add to the permissions list for the share. Then select the appropriate permission from the Type of Access drop-down list box. Click OK.

FIGURE 12-5 **Adding users and groups to the permissions list for the share**

7. In the Access Through Share Permissions dialog box, highlight any users or groups you want to remove from the permissions list for the share. Click the Remove command button.

   (Once you have assigned the appropriate user and groups to the permissions list for the share, I recommend you remove the Everyone group from the list, so that only authorized users can access the share.)

   Click OK.
8. Click OK in the *Folder_name* Properties dialog box.
9. Exit Windows NT Explorer.

If you share folders on a FAT partition, I recommend you assign appropriate share permissions. However, if you share folders on an NTFS partition, I recommend you assign the Domain Users group the Full Control share permission, delete the Everyone group's Full Control share permission, and then manage security by assigning the appropriate NTFS permissions (covered later in this chapter).

How user and group permissions combine

It is not uncommon for a user to have permission 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 the *least* restrictive permission is the user's effective permission. For example, a user has the Read permission to a share, and a group that the user is a member of has the Change permission to the share. The user's effective share permission is Change.

The exception to this rule is the No Access permission. *No Access always overrides all other share permissions.* If a user has the Full Control permission, but is a member of a group that has the No Access permission, the user's effective permission is No Access. *No Access always means no access.*

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 12-3 shows the `SalesData` share permissions assigned to RomanB and to the three groups of which he is a member.

TABLE 12-3 ROMANB'S GROUP MEMBERSHIPS AND SHARE PERMISSIONS

USER OR GROUP	*SALESDATA SHARE PERMISSION ASSIGNED*
RomanB	Full Control
Sales	Change
Everyone	Read
Domain Users	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 12-4 shows the `HRData` share permissions assigned to the three groups of which PennyL is a member.

TABLE 12-4 PENNYL'S GROUP MEMBERSHIPS AND THEIR HRDATA SHARE PERMISSIONS

GROUP	*HRDATA SHARE PERMISSION ASSIGNED*
Managers	Read
HR	Change
Marketing	No Access

Because the No Access permission always overrides all other share permissions, PennyL's effective permission to the `HRData` share is No Access. The administrator should remove PennyL from the Marketing group so that she can access the `HRData` share.

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 aid 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, you can assign a new set of share permissions that apply only to the new share name.

TO ASSIGN AN ADDITIONAL NAME TO A SHARE, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Windows NT Explorer.
2. In the Exploring dialog box, highlight the share to which you want to assign an additional name. Select File ➢ Properties.
3. In the *Folder_name* Properties dialog box, click the Sharing tab.
4. On the Sharing tab, click the New Share command button.
5. In the New Share dialog box, type in the additional name you want to assign to the share. Type in a descriptive comment if you so choose. Configure the share permissions and user limit as desired. Click OK.
6. In the *Folder_name* Properties dialog box, click OK.
7. Exit Windows NT 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, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Windows NT Explorer.
2. In the Exploring dialog box, highlight the share with the name you want to change. Select File ➢ Properties.
3. In the *Folder_name* Properties dialog box, click the Sharing tab.
4. On the Sharing tab, click the New Share command button.
5. In the New Share dialog box, type a new name for the share in the Share Name text box. You should configure the share permissions and user limit to match those assigned to the original share name (assuming no permission or user limit changes are desired). Click OK when you are finished.
6. The *Folder_name* Properties dialog box reappears. Click the arrow in the Share Name drop-down list box to display all names assigned to the share. Figure 12-6 shows the Sharing tab in the Data Properties dialog box. Notice that two names are assigned to the `Data` folder: Data and

Spreadsheets. (In this example, the `Data` share is being renamed as Spreadsheets because it is a more intuitive name for users to recognize.)

FIGURE 12-6 Changing the name of a share

Select the original name (not the new name) of the share in the Share Name drop-down list box. Click the Remove Share command button. (This deletes the original share.) Click OK.

7. Exit Windows NT 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.

TO STOP SHARING A FOLDER, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Windows NT Explorer.
2. In the Exploring dialog box, highlight the share you want to stop sharing. Select File ➢ Properties.
3. In the *Folder_name* Properties dialog box, click the Sharing tab.
4. On the Sharing tab, select the radio button next to Not Shared. Then click OK.
5. Exit Windows NT Explorer.

Administrative Shares

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

The Windows NT administrative shares are: `C$`, `D$`, `E$`, and so on (one share for the root of each hard disk partition on the computer); and a share named `Admin$`, which corresponds to the folder in which NT is installed (<*`winntroot`*>). The $ at the end of each administrative share causes the share to be hidden from users when they browse the network.

Administrative shares make it possible for an Administrator to connect to any hard drive on a computer and access all of its files and folders, regardless of whether regular shares exist on that hard drive. In this way an Administrator can perform backup, restore, and other administrative functions on a Windows NT 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 its assigned share permissions. Only access to the hidden *administrative* shares is restricted, by default, to Administrators only.

If you do not want administrative shares available on a Windows NT computer, you can configure NT to prevent the creation of administrative shares.

Preventing the creation of administrative shares

To configure Windows NT so it does not automatically create administrative shares each time it is started, you can edit the Registry. You can edit the Registry directly using `regedt32.exe`, or you can use the System Policy Editor to turn off the default administrative shares. The steps below explain how to turn off administrative shares by using the Registry editor, `regedt32.exe`.

TO PREVENT THE AUTOMATIC CREATION OF ADMINISTRATIVE SHARES, FOLLOW THESE STEPS:

1. Select Start ➢ Run.
2. In the Open text box, type **Regedt32**. (Don’t type the period at the end.)
3. In the Registry Editor dialog box, select Window ➢ HKEY_LOCAL_MACHINE on Local Machine.

4. 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 window on the right-hand side of the dialog box, double-click AutoShareServer. (If this value is not present, select Edit⪢Add Value. In the Add Value dialog box, type **AutoShareServer** in the Value Name text box. In the Data Type drop-down list box, select REG_DWORD. Click OK.)

   (If you are configuring a Windows NT Workstation 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. 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. The Registry Editor dialog box reappears. The AutoShareServer REG_DWORD setting (or the AutoShareWks REG_DWORD setting) is changed to 0. Exit Registry Editor.

Managing NTFS File and Folder Security

When files and folders are stored on an NTFS volume, 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 authorized access when users connect to the share locally or over the network.

The NTFS permissions that can be assigned, and how each permission applies to folders and files, are shown in Table 12-5.

TABLE 12-5 WINDOWS NT NTFS PERMISSIONS

PERMISSION	WHEN APPLIED TO A FOLDER, A USER IS ABLE TO . . .	WHEN APPLIED TO A FILE, A USER IS ABLE TO . . .
Read (R)	View folder attributes, permissions, and owner; view names of files and subfolders.	View file attributes, permissions, owner, and file contents.
Write (W)	View folder attributes, permissions, and owner; change folder attributes; add files and subfolders.	View file attributes, permissions, and owner; change file attributes; change file contents.
Execute (X)	View folder attributes, permissions, and owner; change the current folder to a subfolder.	View file attributes, permissions, and owner; run the file if it is an executable program.
Delete (D)	Delete the folder.	Delete the file.
Change Permissions (P)	Assign NTFS permissions to the folder.	Assign NTFS permissions to the file.
Take Ownership (O)	Take ownership of the folder.	Take ownership of the file.

To make the assignment of NTFS permissions easier, Microsoft has created a set of standard directory (folder) permissions, and a set of standard file permissions. These *standard permissions* consist of the most commonly used combinations of NTFS permissions.

Standard permissions are used in most situations. Individual NTFS permissions are typically only used when a unique combination of permissions must be assigned. The individual NTFS permissions are sometimes referred to as *Special Access Directory permissions* and *Special Access File permissions*.

Table 12-6 shows the standard NTFS directory permissions. The permissions specified within the first set of parentheses following the permission name apply to the *folder*, and the permissions specified within the second set of parentheses following the permission name apply to *files* within the folder.

Table 12-7 shows the standard NTFS file permissions. NTFS file permissions apply only to the individual file they are assigned to. Other files in the same folder are *not* affected.

TABLE 12-6 STANDARD NTFS DIRECTORY (FOLDER) PERMISSIONS

STANDARD PERMISSION	*DESCRIPTION*
No Access (None) (None)	Prevents access to the folder, and to any file in the folder. When the permission is initially assigned, the administrator can choose whether to apply the permission to existing files and subfolders.
List (RX) (Not Specified)	Assigns the Read and Execute permissions to the folder, but no permissions are assigned to any files in the folder.
Read (RX) (RX)	Assigns the Read and Execute permissions to the folder and to *new* files created in the folder. When the permission is initially assigned, the administrator can choose whether to apply the permission to all *existing* files and subfolders.
Add (WX) (Not Specified)	Assigns the Write and Execute permissions to the folder, but no permissions are assigned to any files in the folder.
Add & Read (RWX) (RX)	Assigns the Read, Write, and Execute permissions to the folder, and assigns the Read and Execute permissions to *new* files created in the folder. When the permission is initially assigned, the administrator can choose whether to apply the permission to all *existing* files and subfolders.
Change (RWXD) (RWXD)	Assigns the Read, Write, Execute, and Delete permissions to the folder and to *new* files created in the folder. When the permission is initially assigned, the administrator can choose whether to apply the permission to all *existing* files and subfolders.

STANDARD PERMISSION	**DESCRIPTION**
Full Control (All) (All)	Assigns all NTFS permissions (Read, Write, Execute, Delete, Change Permissions, and Take Ownership) to the folder and to *new* files created in the folder. When the permission is initially assigned, the administrator can choose whether to apply the permission to all *existing* files and subfolders.

TABLE 12-7 STANDARD NTFS FILE PERMISSIONS

STANDARD FILE PERMISSION	**DESCRIPTION**
No Access (None)	Prevents access to the file.
Read (RX)	Assigns the Read and Execute permissions to the file.
Change (RWXD)	Assigns the Read, Write, Execute, and Delete permissions to the file.
Full Control (All)	Assigns all NTFS permissions (Read, Write, Execute, Delete, Change Permissions, and Take Ownership) to the file.

Sometimes a user has a different set of NTFS permissions to a file than to the folder that contains the file. When the user wants to access a file, and the NTFS file and folder permissions conflict, the file permissions are applied. *File permissions take precedence over folder permissions.* For example, if a user has the Change (RWXD) (RWXD) permission to the folder, and has the Read (RX) permission to the file, the user's effective permission to the file is Read (RX).

If a user has permission to access a file, but does *not* have permission to access the folder that contains the file, the user can access the file by typing the file's full path name (in an application, in the Run dialog box, or at the command prompt). The user can't see the file when browsing in Windows NT Explorer.

The Full Control (All) (All) standard directory permission has a feature that you should be aware of. Because it is designed to support POSIX applications, the Full Control (All) (All) permission allows a user to delete any file in the folder, *even if the user has the No Access (None) standard file permission to the file.* (This is the only exception to the rule that file permissions take precedence over

folder permissions.) To prevent this, I recommend that you assign all of the individual (Special Access) NTFS permissions instead of the Full Control (All) (All) standard directory permission.

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 the *least* restrictive combination of permissions applies. The exception to this rule is the No Access permission. *No Access always overrides all other NTFS permissions.*

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 much 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 (All) (All) NTFS permission to the root of all newly created NTFS volumes.

Assigning NTFS Permissions to Files and Folders

A user can assign NTFS permissions to a file or folder only if one or more of the following criteria are met:

- The user is the owner of the file or folder.
- The user has the Change Permissions NTFS permission to the file or folder.
- The user has the Full Control NTFS permission to the file or folder. (The Full Control permission includes the Change Permissions NTFS permission.)

The following sections explain how to assign NTFS permissions — first to a file, and second, to a folder.

TO ASSIGN NTFS PERMISSIONS TO A FILE, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Windows NT Explorer.
2. In the Exploring dialog box, highlight the file to which you want to assign NTFS permissions. (To assign identical permissions to multiple files, highlight more than one file.) Select File ➢ Properties.

3. The *File_name* Properties dialog box appears. Click the Security tab. On the Security tab, click the Permissions command button.
4. The File Permissions dialog box appears, as shown in Figure 12-7. Notice the complete path to the file and the owner of the file are listed.

   Click the Add command button.

FIGURE 12-7 **Assigning NTFS permissions to the** `Networks.txt` **file**

5. The Add Users and Groups dialog box appears.

   To add users or groups from trusted domains, click the arrow in the List Names From drop-down list box, and select the appropriate domain from the list.

   To add individual users, click the Show Users command button to display individual users, as well as groups, in the Names list box.

   Double-click each user and/or group you want to add to the ACL (permissions list) for the file. Select the NTFS file permission you want to assign from the Type of Access drop-down list box. Click OK.
6. The File Permissions dialog box reappears. If you want to assign individual (Special Access) NTFS file permissions (as opposed to the standard NTFS permissions):

a. Highlight the user(s) or group(s) to which you want to assign the individual NTFS permissions. Select Special Access from the Type of Access drop-down list box.

b. The Special Access dialog box appears, as shown in Figure 12-8. Notice the individual NTFS permissions that can be assigned.

FIGURE 12-8 **Assigning individual (Special Access) NTFS permissions**

Select the radio button next to Other. Check the check box next to the individual NTFS permission(s) you want to assign. Click OK. The File Permissions dialog box reappears.

If you want to remove any users or groups from the ACL for the file (such as the Everyone group), highlight the user or group and click the Remove command button.

Figure 12-9 shows the File Permissions dialog box after NTFS permissions have been assigned. Notice the various NTFS permissions assigned, and how they appear in the Name list box. Click OK.

FIGURE 12-9 **NTFS permissions assigned to the** `Networks.txt` **file**

7. In the *File_name* Properties dialog box, click OK.
8. Exit Windows NT Explorer.

TO ASSIGN NTFS PERMISSIONS TO A FOLDER, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Windows NT Explorer.
2. In the Exploring dialog box, highlight the folder to which you want to assign NTFS permissions. (To assign identical permissions to multiple folders, highlight more than one folder.) Select File ➢ Properties.
3. The *Folder_name* Properties dialog box appears. Click the Security tab. On the Security tab, click the Permissions command button.
4. The Directory Permissions dialog box appears, as shown in Figure 12-10. Note the two check boxes available. Also note that the check box next to Replace Permissions on Existing Files is selected by default.

   Click the Add command button.

FIGURE 12-10 **Assigning NTFS permissions to the** `D:\Data` **folder**

5. The Add Users and Groups dialog box appears. To add users or groups from trusted domains, click the arrow in the List Names From drop-down list box, and select the appropriate domain from the list.

   To add individual users, click the Show Users command button to display individual users, as well as groups, in the Names list box.

   Double-click each user and/or group you want to add to the ACL (permissions list) for the folder. Select the NTFS folder permission you want to assign from the Type of Access drop-down list box. Click OK.

6. The Directory Permissions dialog box reappears. If you want to assign individual (Special Access) NTFS folder permissions (as opposed to the standard NTFS permissions):

a. Highlight the user(s) or group(s) to which you want to assign the individual NTFS permissions. Select Special Directory Access (to assign individual *directory* [folder] permissions) or Special File Access (to assign individual *file* permissions within the folder) from the Type of Access drop-down list box.

b. The Special Directory Access (or Special File Access) dialog box appears. Select the radio button next to Other. Then check the check box next to the individual NTFS permission(s) you want to assign. Click OK. The Directory Permissions dialog box reappears.

   If you want to remove any users or groups from the ACL for the folder (such as the Everyone group), highlight the user or group and click the Remove command button.

7. In the Directory Permissions dialog box, select the check box next to Replace Permissions on Subdirectories if you want these NTFS permissions assigned to all subfolders.

   Clear the check box next to Replace Permissions on Existing Files if you do *not* want these NTFS permissions assigned to each existing file within the folder.

   > The Replace Permissions on Existing Files option is selected by default for a good reason. It can become very cumbersome for an administrator to have to manage individual file permissions. Therefore, it is a good practice to accept the default to Replace Permissions on Existing Files so that all files will have the same permissions as set on the folder. If different permissions are required, a different folder can be created.

   If both check boxes are selected, these NTFS permissions will be assigned to all files within the folder, all subfolders, and their files. If both check boxes are cleared, these NTFS permissions will be assigned only to the folder and to new files created in the folder. Existing subfolders and the files they contain will not be affected.

   Figure 12-11 shows the Directory Permissions dialog box after NTFS permissions have been assigned. Notice that both check boxes are selected.

   Click OK.

FIGURE 12-11 **NTFS permissions assigned to the `D:\Data` folder**

8. If you checked the check box next to Replace Permissions on Subdirectories, a warning message appears, asking if you want to replace the security information on all existing subfolders. Click the Yes command button. (If both check boxes were selected, this could take a while. You might want to consider performing this task during nonbusiness hours.)
9. In the *Folder_name* Properties dialog box, click OK.
10. Exit Windows NT Explorer.

There are a few common administrative practices you should consider when assigning NTFS permissions to files or folders:

- Consider assigning the most restrictive NTFS permission that still makes it possible for users to accomplish necessary tasks.
- After assigning the appropriate NTFS permissions, consider removing the Everyone group, which by default is granted the Full Control permission.
- When you want all users to be able to access a file or folder, consider assigning the NTFS permissions to the Domain Users group instead of to the Everyone group. (The Everyone group includes not only all domain users, but also *anyone* [authorized or not] who can access your network, including those who connect via the Internet.)

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

When files are created in a folder on an NTFS volume, the new files inherit the NTFS permissions of the folder in which they are created. For example, if you create a new file in the `Public` folder, and the `Public` folder has the Change (RWXD) (RWXD) NTFS permission for the Everyone group, the new file inherits the Change (RWXD) permission for the Everyone group.

> **The permissions in the *second* set of parentheses following the NTFS folder permission name are the permissions that are assigned to the new *file*. So, if you create a new file in the `Data` folder, and the `Data` folder has the Add & Read (RWX) (RX) NTFS permission for the Domain Users group, the file inherits the Read (RX) permission for the Domain Users group.**

When new subfolders are created on an NTFS volume, they inherit the NTFS permissions of the folder that contains them. For example, if you create a new subfolder in the `Data` folder, and the `Data` folder has the Add & Read (RWX) (RX) NTFS permission for the Everyone group, the new subfolder inherits the Add & Read (RWX) (RX) permission for the Everyone group.

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 NTFS permissions of the destination folder. The only exception to this rule is when 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.

The following examples illustrate how NTFS permissions are applied to moved or copied files:

Example 1: Moving a file to a folder on a different volume You *move* the `D:\Public\Readme.txt` file (that has the Read (RX) NTFS permissions for the Everyone group) to the `E:\Data` folder (that has the Full Control (All) (All) NTFS permission for the Everyone group). When the file is moved to a folder on a different volume, it inherits the NTFS permissions from the `E:\Data` folder (the destination folder), so the moved file's permissions are now Full Control (All) for the Everyone group.

Example 2: Copying a file to a different folder on the same volume You *copy* the `D:\Data\Busplan.doc` file (that has the Read (RX) NTFS permissions for the Managers group) to the `D:\Public` folder (that has the Change (RWXD) (RWXD) NTFS permissions for the Everyone group). When the file is copied, it inherits the NTFS permissions from the `D:\Public` folder (the destination folder), so the copied file's permissions are now Change (RWXD) for the Everyone group.

Example 3: Moving a file to a different folder on the same volume You *move* the `D:\Data\Busplan.doc` file (that has the Read (RX) NTFS permissions for the Managers group) to the `D:\Public` folder (that has the Change (RWXD) (RWXD) NTFS permissions for the Everyone group). When the file is moved to a folder on the *same* NTFS volume, it retains its original NTFS permissions. In this case, the moved file's NTFS permissions are still Read (RX) for the Managers group.

Because FAT partitions can't support NTFS permissions, any files that you copy or move to a FAT partition lose all their NTFS permissions, along with the security that those permissions provided.

How NTFS and Share Permissions Interact

When users access a share 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 examples illustrate how NTFS and share permissions interact:

Example 1: A folder named `Documents` is shared on an NTFS volume. The `Documents` share has the Change share permission for the Everyone group, and the files and folders in the share all have the Full Control NTFS permission for the Everyone group. Users who access the `Documents` share over the network only have the Change permission to the files and folders, because Change is the most restrictive permission.

Example 2: A folder named `Apps` is shared on an NTFS volume. The `Apps` share has the Full Control share permission assigned to the Everyone group, and the files and folders in the share all have the Read NTFS permission for the Everyone group. Users who access the `Apps` share over the network only have the Read permission to the files and folders, because Read is the most restrictive permission.

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

Planning Strategies for Sharing and Securing Resources

There is no one right way to share and secure your network resources. However, there are several common practices that you can use when planning your network sharing-and-securing strategy. Consider using some or all of the following tips to provide security for network resources and to simplify administration.

- 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 that users of all client computers can access the share.
- When assigning permissions, use groups, rather than individual users, when possible, to simplify administration.
- Consider using the Domain Users group instead of the Everyone group when assigning permissions to all users in the domain to close up the security loophole that the Everyone group allows.
- Consider storing important data on NTFS volumes instead of on FAT volumes, because of the greater security possible on NTFS volumes.
- Consider storing operating systems on a separate volume from data files, home folders, and applications. This makes backup, restore, and administration easier.
- Always store data files and application files in different folders. This helps prevent accidental deletion of application files and simplifies backup and restore procedures.

- Consider making it a practice to always assign the most restrictive permission that still allows a user to accomplish the tasks they need to perform.
- Consider assigning administrators the Full Control permission to all shares, with the exception of user's home folders (directories).
- When assigning both share and NTFS permissions, consider assigning the Full Control share permission to the Domain Users group, and using the appropriate NTFS permissions to secure the resource. (After you assign the Domain Users group the Full Control share permission, you can remove the Everyone group's Full Control permission from the share.) 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.

Planning Form: Sharing and Securing Resources

You can use this form to help you plan how to apply share and/or NTFS permissions to shared resources on your network. (Find an enlarged version of this form in Appendix G.)

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 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 can always assign permissions to that file or folder. Only files and folders on NTFS partitions have owners.

Occasionally, you may need to change or assign permissions to a file or folder, but not have the Change Permissions NTFS permission (or the Full Control NTFS permission, which includes the Change Permissions NTFS permission) to the file or folder. Without being the owner of the file or folder or having the Change Permissions NTFS permission, the only way you can accomplish changing or assigning 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 Change Permissions NTFS permission (or the Full Control 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.
- The user has the Take Ownership NTFS permission to the file or folder (or has the Full Control NTFS permission, which includes the Take Ownership permission).
- The user has the “Take ownership of files or other objects” user right.

The next section describes the steps involved in taking ownership of a file or folder.

TO TAKE OWNERSHIP OF A FILE OR FOLDER, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Windows NT Explorer.

2. Highlight the file or folder that you want to take ownership of. Select File ➢ Properties.
3. The *File_name* or *Folder_name* Properties dialog box appears. Click the Security tab.
4. On the Security tab, click the Ownership command button.
5. If you currently have no permissions to the file or folder, a warning dialog box appears, as shown in Figure 12-12. Notice that the message asks if you want to try overwriting the current owner.

   Click the Yes command button.

FIGURE 12-12 **Taking ownership warning message**

6. The Owner dialog box appears, as shown in Figure 12-13. Note that the owner of the folder is listed as “Unable to retrieve.”

   Click the Take Ownership command button.

FIGURE 12-13 **Taking ownership of a folder**

7. If you are taking ownership of a folder, Windows NT displays an informational dialog box, asking if you want to take ownership of all the files and subfolders contained in the selected folder. Click the Yes or No command button, as appropriate. (Yes is usually the appropriate response.)
8. If prior to taking ownership you had no permissions to the file or folder, Windows NT displays an informational dialog box, as shown in Figure 12-14. Note that you can choose to grant yourself the Full Control permission to the folder.

   Click the Yes command button.

FIGURE 12-14 **Replacing folder permissions while taking ownership**

9. The *File_name* or *Folder_name* Properties dialog box reappears. Click OK.
10. You are now the owner of the file or folder. Exit Windows NT Explorer.

Auditing Files and Folders on NTFS Partitions

You can't be sure that your network is secure until you know that the permissions and other security measures you've put in place haven't been breached. Windows NT auditing makes it possible for you to determine whether unauthorized users have accessed or attempted to access sensitive data.

Windows NT auditing is *only* available on NTFS partitions. You can't audit files or folders that are located on FAT partitions.

Because auditing generates a large amount of data, it's important that you determine what is really necessary to audit. Not only does auditing data take up space in the security log, it also takes administrative time to review the events in the log. In general, if you won't use the information obtained by auditing a given event, you probably shouldn't choose to audit it.

You can choose to audit both successful and unsuccessful (failure) events. For example, you can audit all successful attempts to access a particular program, or you can audit all unsuccessful attempts to access a file that contains confidential data. Success auditing is often performed to gather information about how resources, such as programs and printers, are used. Failure auditing is normally performed to determine whether unauthorized users are attempting to access restricted files or folders. Sometimes success and failure auditing are used simultaneously to determine if any unauthorized users have been successful in breaching the system's security.

When you choose to audit a sensitive resource to determine if your network security has been compromised, consider auditing the Everyone group's success and failure access to the resource. This way, you can track *all* attempts to access the resource, not just attempts made by Domain Users (in other words, the users that you know about).

Configuring Auditing for Files and Folders on NTFS Partitions

Configuring Windows NT auditing for files and folders on NTFS partitions is a two-part process. First, the audit policy is configured in User Manager or User Manager for Domains. Then, auditing is configured for each file and folder individually using Windows NT Explorer.

Only members of the Administrators group can configure the audit policy. Users with the "Manage auditing and security log" user right can establish file and folder auditing, and view and manage the security log in Event Viewer, but can't set audit policy.

Auditing is configured on an individual computer basis. If you want to audit an event that takes place on a domain controller, such as access to a particular folder, you need to set the audit policy for the domain and configure the folder for auditing on the domain controller. If you want to audit an event that takes place on a non-domain controller, such as access to a particular file, you need to set the audit policy on the non-domain controller and configure the particular file for auditing on the non-domain controller, as well.

The next sections describe how to configure audit policy in User Manager or User Manager for Domains, and then how to configure file or folder auditing in Windows NT Explorer.

TO CONFIGURE AUDIT POLICY, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Administrative Tools (Common) ➢ User Manager (or User Manager for Domains).
2. In the User Manager dialog box, select Policies ➢ Audit.

3. The Audit Policy dialog box appears, as shown in Figure 12-15. Notice that Success and Failure auditing are selected for File and Object Access.

   You must select File and Object Access auditing to audit files and folders. If you configure file and folder auditing, but don't configure the audit policy for File and Object Access, no auditing will occur on the files and folders.

   Select the radio button next to Audit These Events, and check the check boxes to configure success and/or failure auditing of the events you want to audit. Click OK.
4. Exit User Manager (or User Manager for Domains).

FIGURE 12-15 **Configuring audit policy**

TO CONFIGURE FILE OR FOLDER AUDITING, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Windows NT Explorer.
2. In the Exploring dialog box, highlight the file or folder you want to audit. Select File ➢ Properties.
3. In the *File_name* or *Folder_name* Properties dialog box, click the Security tab.
4. On the Security tab, click the Auditing command button.
5. In the Directory Auditing dialog box, click the Add command button.
6. The Add Users and Groups dialog box appears. If you want to audit global groups and users from other trusted domains, click the down arrow in the List Names From drop-down list box and select the domain you want. If you want to audit individual users, click the Show Users command button. Double-click each of the groups or users whose access or attempted access to this resource you want to audit. Click OK.

7. The Directory Auditing dialog box reappears. Select the Success and/or Failure check boxes next to each NTFS permission you want to track for this resource. For example, if you want to know who has viewed or attempted to view a confidential file, you could select Success and Failure auditing for the Read permission.

   If you are configuring auditing for a folder, you have the option of choosing to replace the existing auditing configuration on all files and/or subfolders with the settings you are configuring now. Select or deselect the check boxes next to Replace Auditing on Subdirectories and Replace Auditing on Existing Files as desired. Figure 12-16 shows the configured Directory Auditing dialog box for the `D:\New Products Research Data` folder. Notice that success and failure auditing for the Read permission is configured for the Everyone group.

   Click OK.

FIGURE 12-16 **Configuring folder auditing**

8. If you are configuring folder auditing, *and* if you selected the Replace Auditing on Subdirectories check box, a warning dialog box appears, as shown in Figure 12-17.

   Click the Yes command button.

FIGURE 12-17 **Replacing auditing configuration on subfolders**

9. The *File_name* or *Folder_name* Properties dialog box reappears. Click OK.
10. Exit Windows NT Explorer.

Using Event Viewer to View Auditing Results

You can use Event Viewer to view the results of the auditing you have configured. Event Viewer has three logs: the system log, the application log, and the security log. The security log contains the data generated by auditing.

You can view the security log in its entirety, or you can filter events by date and type of audit event. You can clear the security log when it is full; and you can save (archive) the log to be viewed at a later date by using Event Viewer, a text editor, or a spreadsheet or database program. You can also configure the size of the log and event log wrapping (how the log handles additional auditing data when it becomes full).

An important consideration, from an administrative standpoint, is scheduling time to regularly view auditing events in the security log. The data gathered by auditing is of no value if it is not used.

The sections that follow explain how to access the security log in Event Viewer and how to filter audit events, how to save (archive) and clear the security log, and how to configure the maximum size of the security log and event log wrapping.

TO ACCESS THE SECURITY LOG, AND TO FILTER AND VIEW AUDIT EVENTS, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Administrative Tools (Common) ➢ Event Viewer.
2. In the Event Viewer dialog box, select Log ➢ Security. This accesses the security log.

   Figure 12-18 shows the Security Log dialog box in Event Viewer. Notice that both success and failure events are listed. (Remember, success events are denoted by a key, and failure events are denoted by a lock in the left margin.)

   FIGURE 12-18 **Viewing the security log**

3. To filter security log events by date or type of event, select View ➢ Filter Events.
4. The Filter dialog box appears, as shown in Figure 12-19. Notice the filter configuration options available.

   If you need more information on filtering events, click the Help command button. Configure filtering as desired. Click OK.
5. To view details for a specific audit event, double-click the event.

FIGURE 12-19 **Filtering events in the security log**

TO SAVE (ARCHIVE) AND CLEAR THE SECURITY LOG FOLLOW THESE STEPS:

1. In Event Viewer, select Log ➢ Clear All Events.
2. A dialog box appears, asking if you want to save the log before clearing it. Click the Yes command button to save the log.
3. The Save As dialog box appears, as shown in Figure 12-20. Notice the three types of files that you can save the log as.

   If you want to view the log later by using Event Viewer, save (archive) the log as an Event Log File (`*.EVT`). If you want to view the log later by using a text editor, save the log as a Text File (`*.TXT`). If you want to export the file for analysis in a spreadsheet or database program, save the log as a Comma Delimited Text file (`*.TXT`)

   Type in a file name for the log you are saving, then select a type of file in the “Save as type” drop-down list box. Click the Save command button.
4. A dialog box appears, asking you to confirm that you want to clear the security log. Click the Yes command button. The log is cleared.

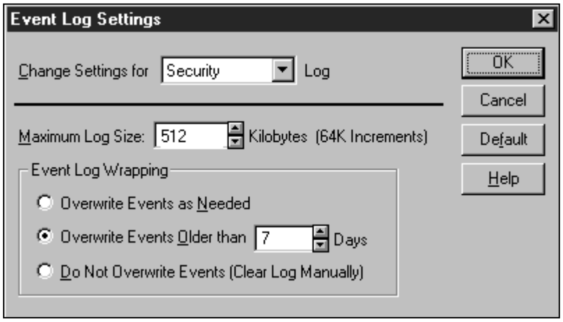
FIGURE 12-20 **Saving the security log**

TO CONFIGURE THE MAXIMUM SIZE OF THE SECURITY LOG AND EVENT LOG WRAPPING, FOLLOW THESE STEPS:

1. Select Log ➢ Log Settings in the Event Viewer dialog box.
2. The Event Log Settings dialog box appears, as shown in Figure 12-21. Notice the available event log wrapping settings. This feature determines how Event Viewer handles new audit events when the security log has reached its maximum size.

   Configure the maximum log size as desired. The available range for this setting is from 64KB to 4,194,176KB. The default maximum log size is 512KB.

   Select one of the three event log wrapping configuration options. Click OK.



Event Log Settings

Change Settings for Security Log

Maximum Log Size: 512 Kilobytes (64K Increments)

Event Log Wrapping

○ Overwrite Events as Needed

● Overwrite Events Older than 7 Days

○ Do Not Overwrite Events (Clear Log Manually)

FIGURE 12-21 **Configuring event log settings**

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. Most resource access problems are caused by incorrectly configured and/or conflicting permissions.

Here are some recommended troubleshooting tips to help you to determine why a user can't access a shared network resource:

- **Look for conflicting share and NTFS permissions**. 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 resource.
- **Look for the No Access permission.** If the user, or any group of which the user is a member, has been assigned the No Access permission to the share or has been assigned the No Access NTFS permission to the resource, the user will not be able to access the resource.
- If you have just assigned the user permission to the resource, and the user can't access the resource, **try having the user log off and log on again,** so the user's access token will be updated.

Key Point Summary

This chapter discussed how to share and secure file systems in a Windows NT environment. The following points illuminate the major issues.

- The Windows NT file and folder attributes are: Archive, Compress, Hidden, Read-only, and System. The file attributes can be used on both FAT and NTFS partitions, with the exception of the Compress attribute, which is only available on NTFS partitions.

- In Windows NT, folders are *shared* to make it possible for users to access network resources. Only members of the Administrators, Server Operators, and Power Users groups can share folders. When a folder is shared, the folder's entire contents, including all files and subfolders (in other words, the entire directory tree under the shared folder), are available to users that have the appropriate permissions to the share. You can use either Windows NT Explorer or Server Manager to share folders.
- *Shared folder permissions* control access to shared folders. Share permissions only apply when users connect to the folder over the network—they do *not* apply when users access the folder from the local computer.
  - The Windows NT share permissions, from most restrictive to least restrictive, are: No Access, Read, Change, and Full Control. Share permissions are assigned by adding a user or group to the permissions list for the share. You can assign share permissions by using Windows NT Explorer or Server Manager.
  - It's not uncommon for a user to be a member of multiple groups that have different permissions to a share. When this occurs, the user and group permissions are additive, and the *least* restrictive permission is the user's effective permission. The exception to this rule is the No Access permission. No Access always overrides other share permissions.
- After a share is created, you may want to modify its properties. You can assign multiple share names to it, change the name of it, or stop sharing it.
- Every time you start Windows NT on a computer, NT automatically creates several hidden shares that only members of the Administrators group have permission to access. These shares are referred to as *administrative shares*. The Windows NT administrative shares are: `C$`, `D$`, `E$`, and so on (one share for the root of each hard disk partition on the computer), and `Admin$` (which corresponds to the folder in which NT is installed). The $ at the end of each administrative share causes the share to be hidden from users when they browse the network. Any share can be configured as a hidden share by appending a $ to the share name, but only access to the hidden administrative shares is automatically restricted to Administrators only. If you don't want administrative shares available on a Windows NT computer, you can configure the Registry so that NT does not create these shares each time Windows NT is started.

- When files and folders are stored on an NTFS volume, *NTFS permissions* can be assigned to provide a greater level of security than share permissions. This is because NTFS permissions can be assigned to individual files and folders, and they apply to local users as well as to users who connect to a shared folder over the network.
  - The NTFS permissions are: Read (R), Write (W), Execute (E), Delete (D), Change Permissions (P), and Take Ownership (O). The individual NTFS permissions are sometimes referred to as *Special Access Directory permissions* and *Special Access File permissions*. To make the assignment of NTFS permissions easier, Microsoft has created a set of standard directory (folder) permissions and a set of standard file permissions. Standard permissions, which are combinations of the most commonly used NTFS permissions, are used in most situations.
  - The standard NTFS directory (folder) permissions are: No Access (None) (None), List (RX) (Not Specified), Read (RX) (RX), Add (WX) (Not Specified), Add and Read (RWX) (RX), Change (RWXD) (RWXD), and Full Control (All) (All). The permissions specified within the first set of parentheses following the permission name apply to the *folder*, and the permissions specified within the second set of parentheses following the permission name apply to *files* within the folder.
  - The standard NTFS file permissions are No Access (None), Read (RX), Change (RWXD), and Full Control (All). NTFS file permissions apply only to the individual file to which they are assigned. Other files in the same folder are not affected.
  - When a user wants to access a file, and the NTFS file and folder permissions conflict, the file permissions are applied. *File permissions take precedence over folder permissions.*
  - As with share permissions, user and group NTFS permissions are additive, and the *least* restrictive combination of permissions applies. The exception to this rule is the No Access permission. No Access always overrides all other NTFS permissions.
  - Only a user who is the owner of the file or folder, or who has the Change Permissions or Full Control NTFS permissions, can assign NTFS permissions to the file or folder. NTFS permissions are assigned to files and folders by using Windows NT Explorer.

- When files are created in a folder on an NTFS volume, the new files inherit the NTFS permissions of the folder they are created in. When new subfolders are created on an NTFS volume, the new subfolders inherit the NTFS permissions of the folder that contains the new subfolder.
- 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 NTFS permissions of the destination folder. The only exception to this rule is when 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.
- *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 creator of a file or folder is its *owner* (except that when a member of the Administrators group creates a file or folder, the Administrators *group*, not the user, is the owner of the file or folder). Without being the owner of a file or folder or having the Change Permissions NTFS permission, the only way you can change or assign permissions to the file or folder is to *take ownership* of the file or folder.
  - A user must either be a member of the Administrators group, have the Take Ownership NTFS permission to the file or folder (or have the Full Control permission, which includes the Take Ownership permission), or have the "Take ownership of files or other objects" user right in order to take ownership of a file or folder.
- *Windows NT auditing is available only on NTFS partitions.* Success auditing is often performed to gather information about how resources are used. Failure auditing is normally performed to determine whether unauthorized users are attempting to access restricted files or folders.
  - There are two parts involved in configuring auditing: first, the audit policy is configured in User Manager or User Manager for Domains; second, auditing is configured for each file and folder individually by using Windows NT Explorer. Only members of the Administrators group can configure audit policy. When configuring audit policy, you *must* select File and Object Access auditing to audit files and folders. If you configure file

  and folder auditing, but don't configure the audit policy for File and Object Access, no auditing of files and folders will occur.

  - You can view the results of auditing that are contained in the security log in Event Viewer. In Event Viewer, you can filter events by date and type, you can clear the security log when it is full, and you can save (archive) the log to be viewed at a later date. The size of the log and event log wrapping (how the log handles additional auditing data when it becomes full) can also be configured.

- Most resource access problems are caused by incorrectly configured and/or conflicting permissions. Some troubleshooting tips for dealing with resource access problems are:
  - Look for conflicting share and NTFS permissions. 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 resource.
  - Look for the No Access permission.
  - If you have just assigned the user permission to the resource, and the user can't access the resource, try having the user log off and log on again.

Applying What You've Learned

Now it's time to regroup, review, and apply what you've learned in this chapter.

The Instant Assessment questions bring to mind key facts and concepts.

The hands-on lab exercises reinforce what you've learned, and allow you to practice some of the tasks tested by the Microsoft Certified Professional exams.

Instant Assessment

1. What Windows NT file attribute can you use to prevent the accidental deletion of application files?
2. What Windows NT file attribute is only available on NTFS partitions?

3. On a Windows NT network, what is the purpose of sharing folders?
4. List the Windows NT share permissions—from most restrictive to least restrictive.
5. When user and group share permissions are combined, which permission always overrides all others?
6. A user, JohnZ, belongs to three groups, whose respective share permissions are Change, Read, and Full Control. What is JohnZ's effective share permission?
7. A user, PaulS, belongs to two groups, whose respective share permissions are Full Control and No Access. What is PaulS's effective share permission?
8. What are the Windows NT administrative shares?
9. How can you configure a share to be a hidden share?
10. How do NTFS permissions provide a higher level of security than share permissions?
11. List the NTFS (individual) permissions.
12. What are the standard NTFS folder permissions?
13. What are the standard NTFS file permissions?
14. When a user wants to access a file, and the NTFS file and folder permissions conflict, which permissions are applied?
15. When a file is created in a folder on an NTFS volume, what NTFS permissions does the file have?
16. Fill in the blank: Normally, when files or folders are moved or copied, they inherit the NTFS permissions of the ______________ folder.
17. What NTFS permissions are applied to a file that is *moved* to a different folder on the *same* NTFS volume?
18. When NTFS and share permissions differ, which permission becomes the user's effective permission to the file or folder in the share?
19. Who is the owner of a file or folder?
20. Why would a user want to take ownership of a file or folder?
21. What are the two parts involved in configuring auditing?
22. What *must* be configured in audit policy in order to audit files and folders?

23. Which Windows NT utility is used to examine the results of auditing?

24. What is the cause of most resource access problems?

T/F

25. Only members of the Administrators group can share folders. _____

26. When a folder is shared, the folder's entire contents, including all files and subfolders (i.e., the entire directory tree under the shared folder) are available to users that have the appropriate permissions to the share. _____

27. User and group NTFS permissions, when combined, are *not* additive. _____

28. Share permissions *don't* apply when a user accesses files in a shared folder on the local computer, but NTFS permissions *do* apply when a user accesses files in a shared folder on the local computer. _____

29. Windows NT auditing is only available on FAT partitions. _____

concept link **For answers to the Instant Assessment see Appendix D.**

Hands-on Lab Exercises

The following hands-on lab exercises provide you with three practical opportunities to apply the knowledge you've gained in this chapter about sharing and securing file systems.

Lab 12.18 *Sharing and securing resources*

MCSE

Workstation
Server
Enterprise

The purpose of this lab is to provide you with hands-on experience in planning a strategy for sharing and securing resources, and in performing the tasks of sharing and securing resources in Windows NT.

This lab consists of three parts:

Part 1: Planning a strategy for sharing and securing resources
Part 2: Sharing and securing folders
Part 3: Establishing NTFS permissions

Begin this lab by booting your computer to Windows NT Server. Log on as Administrator.

Follow the steps below carefully.

Part 1: Planning a strategy for sharing and securing resources

In this section, you plan a strategy for sharing and securing folders on a Windows NT Server computer given a particular scenario.

Scenario: SalesPros, Inc. is a sales organization. (It's the same company you created users and groups for in Lab 7.10). Table 12-8 shows some of SalesPros, Inc.'s employees, their user names, job titles, and respective group membership(s):

TABLE 12-8 SALESPROS, INC.'S USER AND GROUP ACCOUNTS

EMPLOYEE	*USER NAME*	*JOB TITLE*	*GROUP MEMBERSHIP(S)*
Pam Rhodes	PamR	District Manager	Managers, Sales, Accounting, Domain Users
John Spencer	JohnS	Sales Manager	Managers, Sales, Domain Users
Robert Jones	RobertJ	Accounting Manager	Managers, Accounting, Domain Users
Colleen Green	ColleenG	Sales Rep	Sales, Domain Users
Bill Tracy	BillT	Sales Rep	Sales, Domain Users
Mike Calhoun	MikeC	Sales Rep	Sales, Domain Users
Nancy Yates	NancyY	Accounting Staff	Accounting, Domain Users
Mike Cook	MikeCo	Accounting Staff	Accounting, Domain Users

The resources to be shared are located on two partitions on a Windows NT Server computer. The C: drive is a FAT partition that contains applications, and the D: drive is an NTFS partition that contains data folders. The following resources exist:

Use the following criteria for determining your strategy to share and secure resources:

1. All employees need to be able to access all three applications: Word, Excel, and Access. However, employees should *not* be able to save data files to the application folders or to change or delete files in the application folders.
2. Employees should be able to access (create, read, write, and delete files) only the data folders that correspond to the groups to which they belong. For example, only members of the Accounting group should be able to access the `D:\Data\Accounting` folder. Furthermore, members of the Accounting group should *not* be able to access data folders that correspond to groups of which they are *not* members.
3. All employees need to be able to access (create, read, write and delete files) the `D:\Data\AllUsers` folder.
4. Members of the Administrators group require Full Control to all shared resources on the NTFS partition.

Plan a strategy for sharing and securing folders by assigning a share name to each resource (folder), and then choosing the appropriate share and/or NTFS permissions for each resource listed.

Use the following worksheet for your answers:

concept link **For answers to the hands-on lab exercise see Appendix D.**

Continue to Part 2.

Part 2: Sharing and securing folders

In this section, you create several folders to share, then apply appropriate share permissions to each of the folders.

1. Select Start ➢ Programs ➢ Windows NT Explorer.

2. In the Exploring dialog box, highlight the C: drive (or the drive that contains your FAT partition — this is the drive that you installed Windows NT Server and Windows NT Workstation on). Select File ⋗ New ⋗ Folder.
3. The new folder appears in the Name list box. Type in a new folder name of **Apps**. Press Enter. Double-click the `Apps` folder.
4. Select File ⋗ New ⋗ Folder.
5. The new folder appears in the Name list box. Type in a new folder name of **Word**. Press Enter.
6. Select File ⋗ New ⋗ Folder.
7. The new folder appears in the Name list box. Type in a new folder name of **Excel**. Press Enter.
8. Select File ⋗ New ⋗ Folder.
9. The new folder appears in the Name list box. Type in a new folder name of **Access**. Press Enter.
10. Highlight the `Word` folder in the Name list box. Select File ⋗ Properties.
11. In the Word Properties dialog box, click the Sharing tab. Select the radio button next to Shared As. In the Share Name text box, accept the default name of Word. Click the Permissions command button.
12. The Access Through Share Permissions dialog box appears. Click the Add command button.
13. The Add Users and Groups dialog box appears. Double-click the Domain Users group. In the Type of Access drop-down list box, select Change. Click OK.
14. In the Access Through Share Permissions dialog box, highlight the Everyone group. Click the Remove command button. Click OK.
15. In the Word Properties dialog box, click OK.
16. In the Exploring dialog box, highlight the `Excel` folder in the Name list box. Select File ⋗ Properties.
17. In the Excel Properties dialog box, click the Sharing tab. Select the radio button next to Shared As. In the Share Name text box, accept the default name of Excel. Click the Permissions command button.
18. The Access Through Share Permissions dialog box appears. Click the Add command button.
19. The Add Users and Groups dialog box appears. Double-click the Domain Users group. In the Type of Access drop-down list box, select Change. Click OK.

20. In the Access Through Share Permissions dialog box, highlight the Everyone group. Click the Remove command button. Click OK.
21. In the Excel Properties dialog box, click OK.
22. In the Exploring dialog box, highlight the `Access` folder in the Name list box. Select File ➢ Properties.
23. In the Access Properties dialog box, click the Sharing tab. Select the radio button next to Shared As. In the Share Name text box, accept the default name of Access. Click the Permissions command button.
24. The Access Through Share Permissions dialog box appears. Click the Add command button.
25. The Add Users and Groups dialog box appears. Double-click the Domain Users group. In the Type of Access drop-down list box, select Change. Click OK.
26. In the Access Through Share Permissions dialog box, highlight the Everyone group. Click the Remove command button. Click OK.
27. In the Access Properties dialog box, click OK.
28. The Exploring dialog box reappears. Notice that all three folders (`Word`, `Excel`, and `Access`) appear in the Name list box, and that all three appear with a hand under the folder, indicating that they are shared folders.
29. Highlight the D: drive (or the drive that contains your NTFS partition). Select File ➢ New ➢ Folder.
30. The new folder appears in the Name list box. Type in a new folder name of **Data**. Press Enter. Double-click the `Data` folder.
31. Select File ➢ New ➢ Folder.
32. The new folder appears in the Name list box. Type in a new folder name of **Managers**. Press Enter.
33. Select File ➢ New ➢ Folder.
34. The new folder appears in the Name list box. Type in a new folder name of **Accounting**. Press Enter.
35. Select File ➢ New ➢ Folder.
36. The new folder appears in the Name list box. Type in a new folder name of **Sales**. Press Enter.
37. Select File ➢ New ➢ Folder.
38. The new folder appears in the Name list box. Type in a new folder name of **AllUsers**. Press Enter.
39. In the Exploring dialog box, highlight the `Managers` folder in the Name list box. Select File ➢ Properties.

40. In the Managers Properties dialog box, click the Sharing tab. Select the radio button next to Shared As. In the Share Name text box, type **ManagersData**. Click the Permissions command button.
41. The Access Through Share Permissions dialog box appears. Notice that the Everyone group is listed and has the Full Control share permission. (Because this folder is located on an NTFS partition, you will use NTFS permissions to secure this folder, and accept the default share permission.) Click OK.
42. In the Managers Properties dialog box, Click OK.
43. A warning message appears, indicating that the new share name may not be accessible from some MS-DOS workstations. (This is because the name you assigned is longer than eight characters). Click the Yes command button.
44. In the Exploring dialog box, highlight the `Accounting` folder in the Name list box. Select File ➢ Properties.
45. In the Accounting Properties dialog box, click the Sharing tab. Select the radio button next to Shared As. In the Share Name text box, type in **AccountingData**. Click OK.
46. In the Sharing warning dialog box, click the Yes command button.
47. In the Exploring dialog box, highlight the `Sales` folder in the Name list box. Select File ➢ Properties.
48. In the Sales Properties dialog box, click the Sharing tab. Select the radio button next to Shared As. In the Share Name text box, type in **SalesData**. Click OK.
49. In the Sharing warning dialog box, click the Yes command button.
50. In the Exploring dialog box, highlight the `AllUsers` folder in the Name list box. Select File ➢ Properties.
51. In the AllUsers Properties dialog box, click the Sharing tab. Select the radio button next to Shared As. In the Share Name text box, type in **AllUsersData**. Click OK.
52. In the Sharing warning dialog box, click the Yes command button.
53. The Exploring dialog box reappears. Notice that all four folders (`Managers`, `Accounting`, `Sales`, and `All Users`) appear in the Name list box, and that all four appear with a hand under the folder, indicating that they are shared folders.

    In the next section, you assign NTFS permissions to these folders. Continue to Part 3.

Part 3: Establishing NTFS permissions

In this section, you assign the appropriate NTFS permissions to the `Managers`, `Accounting`, `Sales`, and `AllUsers` folders that you created and shared in Part 2.

1. In the Exploring dialog box, highlight the `Managers` folder in the Name list box. Select File ➢ Properties.
2. In the Managers Properties dialog box, click the Security tab. Click the Permissions command button.
3. In the Directory Permissions dialog box, click the Add command button.
4. In the Add Users and Groups dialog box, double-click the Managers group. In the Type of Access drop-down list box, select Change. Click OK.
5. Click the Add command button.
6. In the Add Users and Groups dialog box, double-click Administrators. In the Type of Access drop-down list box, select Full Control. Click OK.
7. In the Directory Permissions dialog box, highlight the Everyone group. Click the Remove command button. Click OK.
8. In the Managers Properties dialog box, click OK.
9. In the Exploring dialog box, highlight the `Accounting` folder in the Name list box. Select File ➢ Properties.
10. In the Accounting Properties dialog box, click the Security tab. Click the Permissions command button.
11. In the Directory Permissions dialog box, click the Add command button.
12. In the Add Users and Groups dialog box, double-click the Accounting group. In the Type of Access drop-down list box, select Change. Click OK.
13. Click the Add command button.
14. In the Add Users and Groups dialog box, double-click Administrators. In the Type of Access drop-down list box, select Full Control. Click OK.
15. In the Directory Permissions dialog box, highlight the Everyone group. Click the Remove command button. Click OK.
16. In the Accounting Properties dialog box, click OK.
17. In the Exploring dialog box, highlight the `Sales` folder in the Name list box. Select File ➢ Properties.
18. In the Sales Properties dialog box, click the Security tab. Click the Permissions command button.
19. In the Directory Permissions dialog box, click the Add command button.
20. In the Add Users and Groups dialog box, double-click the Sales group. In the Type of Access drop-down list box, select Change. Click OK.

21. Click the Add command button.
22. In the Add Users and Groups dialog box, double-click Administrators. In the Type of Access drop-down list box, select Full Control. Click OK.
23. In the Directory Permissions dialog box, highlight the Everyone group. Click the Remove command button. Click OK.
24. In the Sales Properties dialog box, click OK.
25. In the Exploring dialog box, highlight the `AllUsers` folder in the Name list box. Select File ➢ Properties.
26. In the AllUsers Properties dialog box, click the Security tab. Click the Permissions command button.
27. In the Directory Permissions dialog box, click the Add command button.
28. In the Add Users and Groups dialog box, double-click the Domain Users group. In the Type of Access drop-down list box, select Change. Click OK.
29. Click the Add command button.
30. In the Add Users and Groups dialog box, double-click Administrators. In the Type of Access drop-down list box, select Full Control. Click OK.
31. In the Directory Permissions dialog box, highlight the Everyone group. Click the Remove command button. Click OK.
32. In the AllUsers Properties dialog box, click OK. This completes the assigning of NTFS permissions. Exit Windows NT Explorer.

Lab 12.19 *Establishing file and folder auditing*

MCSE

Server
Enterprise

The purpose of this lab is to provide you with hands-on experience in establishing file and folder auditing.

This lab consists of two parts:

Part 1: Establishing file and folder auditing

Part 2: Testing file and folder auditing

Begin this lab by booting your computer to Windows NT Server. Log on as Administrator.

Follow the steps below carefully.

Part 1: Establishing file and folder auditing

In this section, you establish file and folder auditing on the `Managers`, `Accounting`, `Sales`, and `AllUsers` subfolders in the `D:\Data` folder that you created and shared in Lab 12.18.

In Lab 8.11, you implemented success and failure auditing for File and Object Access by using User Manager for Domains. That was the first step in auditing files and folders. This lab completes the process of establishing auditing on files and folders.

1. Select Start ➢ Programs ➢ Windows NT Explorer.
2. In the All Folders section of the Exploring dialog box, click the + sign next to the drive that contains your NTFS partition (usually this is the D: drive). Highlight the `Data` folder. In the Name list box in the Contents of 'Data' section, highlight the `Accounting` folder. Select File ➢ Properties.
3. In the Accounting Properties dialog box, click the Security tab. Click the Auditing command button.
4. In the Directory Auditing dialog box, click the Add command button. Double-click the Domain Users group. Click OK.
5. In the Directory Auditing dialog box, select the Success and Failure check boxes next to Read, Write, and Execute. Click OK.
6. In the Accounting Properties dialog box, click OK.
7. In the Name list box in the Contents of 'Data' section, highlight the `AllUsers` folder. Select File ➢ Properties.
8. In the AllUsers Properties dialog box, click the Security tab. Click the Auditing command button.
9. In the Directory Auditing dialog box, click the Add command button. Double-click the Domain Users group. Click OK.
10. In the Directory Auditing dialog box, select the Success and Failure check boxes next to Delete. Click OK.
11. In the AllUsers Properties dialog box, click OK.
12. In the Name list box in the Contents of 'Data' section, highlight the `Managers` folder. Select File ➢ Properties.
13. In the Managers Properties dialog box, click the Security tab. Click the Auditing command button.
14. In the Directory Auditing dialog box, click the Add command button. Double-click the Domain Users group. Click OK.
15. In the Directory Auditing dialog box, select the Success and Failure check boxes next to Read, Write, Execute, Delete, Change Permissions, and Take Ownership. Click OK.
16. In the Managers Properties dialog box, click OK.
17. In the Name list box in the Contents of 'Data' section, highlight the `Sales` folder. Select File ➢ Properties.

18. In the Sales Properties dialog box, click the Security tab. Click the Auditing command button.
19. In the Directory Auditing dialog box, click the Add command button. Double-click the Domain Users group. Click OK.
20. In the Directory Auditing dialog box, select the Success and Failure check boxes next to Read, Write, and Execute. Click OK.
21. In the Sales Properties dialog box, click OK. Exit Windows NT Explorer. Continue on to Part 2.

Part 2: Testing file and folder auditing

In this section, you clear the security log in Event Viewer, then log on as NancyY and attempt to access each of the data folders you created and shared in Lab 12.18. Then you use Event Viewer to view the results of the auditing that you established in Part 1.

1. Select Start ➢ Programs ➢ Administrative Tools (Common) ➢ Event Viewer.
2. In the Event Viewer dialog box, select Log ➢ Security. Select Log ➢ Clear All Events. (You are clearing the security log to make room for new auditing events.)
3. In the Clear Event Log dialog box, click the No command button, so as to not save the log to a file.
4. In the Clear Event Log dialog box, click the Yes command button to clear the security log.
5. Exit Event Viewer.
6. Select Start ➢ Shut Down.
7. In the Shut Down Windows dialog box, select the radio button next to ”Close all programs and log on as a different user.“ Click the Yes command button.
8. Press Ctrl + Alt + Delete to log on.
9. Click OK in the Important Notice dialog box.
10. Type in a user name of **NancyY**, and a password of **password**. Click OK.
11. A warning message may appear, indicating that your password will expire in *xx* days. Click the No command button.
12. If a Welcome to Windows NT dialog box appears, clear the check box next to “Show this Welcome Screen next time you start Windows NT.” Click the Close command button.
13. Select Start ➢ Programs ➢ Windows NT Explorer.

14. In the Exploring dialog box, click the plus sign next to the drive that contains your NTFS partition (usually this is the D: drive). Click the plus sign next to the `Data` folder on this drive. Highlight the `Accounting` folder. Notice that there are no files in this folder.
15. Highlight the `AllUsers` folder. Notice that there are no files in this folder.
16. Highlight the `Managers` folder. A dialog box appears, indicating that access has been denied. (This is because NancyY is not a member of the Managers group and does not have the appropriate permission to access this folder.) Click the Cancel command button.
17. Highlight the `Sales` folder. A dialog box appears, indicating that access has been denied. (This is because NancyY is not a member of the Sales group and does not have the appropriate permission to access this folder.) Click the Cancel command button. Exit Windows NT Explorer.
18. Select Start ➢ Shut Down.
19. In the Shut Down Windows dialog box, select the radio button next to "Close all programs and log on as a different user." Click the Yes command button.
20. Press Ctrl + Alt + Delete to log on.
21. Click OK in the Important Notice dialog box.
22. Type in a user name of **Administrator**, and a password of **password**. Click OK.
23. Select Start ➢ Programs ➢ Administrative Tools (Common) ➢ Event Viewer.
24. In the Event Viewer dialog box, select Log ➢ Security. Scroll down the log and double-click the first event that lists NancyY in the User column *and* Logon/Logoff in the Category column.
25. The Event Detail dialog box appears. Notice that this is a Success audit of the Logon/Logoff event. Click the Close command button.
26. Scroll down and double-click the event that has a lock (rather than a key) in the left-hand margin, lists NancyY in the User column, *and* Object Access in the Category column. (This should be approximately eleven events down from the one you just viewed.)
27. The Event Detail dialog box appears. Notice that this is a Failure audit event of the Object Access type. (This audit event occurred when NancyY attempted to access the `D:\Data\Sales` folder and was denied access.) Click the Next command button to view the next audit event.
28. Continue clicking on the Next command button to view several more audit events. When you are finished viewing audit events, click the Close command button.

29. Exit Event Viewer.

Lab 12.20 *Troubleshooting resource access and permission problems*

Workstation
Server
Enterprise

The purpose of this lab is to provide you with hands-on experience in troubleshooting some common resource access and permission problems.

For each problem presented, consider the troubleshooting information provided and determine:

1. The cause of the problem, and
2. What steps you would take to resolve the problem.

Problem 1 A user, NancyY, reports that she can't save files to the `AccountingData` share located on an NTFS volume on a Windows NT computer. You begin the troubleshooting process by using User Manager for Domains and Windows NT Explorer to obtain NancyY's group memberships, and the share and NTFS permissions assigned to the `AccountingData` share.

Figure 12-22 shows the Group Memberships dialog box, which lists NancyY's group memberships.

FIGURE 12-22 **Group memberships for NancyY**

Figure 12-23 shows the Access Through Share Permissions dialog box, which lists the share permissions assigned to the `AccountingData` share.

FIGURE 12-23 **Share permissions for `AccountingData` share**

Figure 12-24 shows the Directory Permissions dialog box. This dialog box lists the NTFS permissions assigned to the `D:\Data\Accounting` folder, which is shared as `AccountingData`.

FIGURE 12-24 **NTFS permissions for `AccountingData` share**

What is the cause of the problem?

What would you do to resolve the problem?

Problem 2 A user, JohnS, reports he can't access the `ManagersData` share located on an NTFS volume on a Windows NT computer. You begin the troubleshooting process by using User Manager for Domains and Windows NT Explorer to obtain JohnS's group memberships, and the share and NTFS permissions assigned to the `ManagersData` share.

Figure 12-25 shows the Group Memberships dialog box, which lists JohnS's group memberships.

FIGURE 12-25 **Group memberships for JohnS**

Figure 12-26 shows the Access Through Share Permissions dialog box, which lists the share permissions assigned to the `ManagersData` share.

FIGURE 12-26 **Share permissions for `ManagersData` share**

Figure 12-27 shows the Directory Permissions dialog box. This dialog box lists the NTFS permissions assigned to the `D:\Data\Managers` folder, which is shared as `ManagersData`.

FIGURE 12-27 **NTFS permissions for `ManagersData` share**

What is the cause of the problem?

What would you do to resolve the problem?

concept link **For answers to the hands-on lab exercise see Appendix D.**