File and Folder Permissions

from Chapter 13, Microsoft Windows 2000 Administrator's Pocket Consultant by William R. Stanek.

On NTFS volumes, you can set security permissions on files and folders. These permissions grant or deny access to the files and folders. You can view security permissions for files and folders by completing the following steps:

1. In Windows Explorer, right-click the file or folder you want to work with.
2. From the pop-up menu, select Properties, and then in the Properties dialog box click the Security tab.
3. In the Name list box, select the user, contact, computer, or group whose permissions you want to view. If the permissions are dimmed, it means the permissions are inherited from a parent object.

Understanding File and Folder Permissions

The basic permissions you can assign to files and folders are summarized in Table 13-3. File permissions include Full Control, Modify, Read & Execute, Read, and Write. Folder permissions include Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write.

Anytime you work with file and folder permissions, you should keep the following in mind:

- Read is the only permission needed to run scripts. Execute permission doesn't matter.
- Read access is required to access a shortcut and its target.
- Giving a user permission to write to a file but not to delete it doesn't prevent the user from deleting the file's contents. A user can still delete the contents.
- If a user has full control over a folder, the user can delete files in the folder regardless of the permission on the files.

Table 13-3 File and Folder Permissions Used by Windows 2000

Permission	Meaning for Folders	Meaning for Files
Read	Permits viewing and listing of files and subfolders	Permits viewing or accessing of the file's contents
Write	Permits adding of files and subfolders	Permits writing to a file
Read & Execute	Permits viewing and listing of files and subfolders as well as executing of files; inherited by files and folders	Permits viewing and accessing of the file's contents as well as executing of the file
List Folder Contents	Permits viewing and listing of files and subfolders as well as executing of files; inherited by folders only	N/A

Modify	Permits reading and writing of files and subfolders; allows deletion of the folder	Permits reading and writing of the file; allows deletion of the file
Full Control	Permits reading, writing, changing, and deleting of files and subfolders	Permits reading, writing, changing and deleting of the file

The basic permissions are created by combining special permissions in logical groups. Table 13-4 shows special permissions used to create the basic permissions for files. Using advanced permission settings, you can assign these special permissions individually, if necessary. As you study the special permissions, keep the following in mind:

- If no access is specifically granted or denied, the user is denied access.
- Actions that users can perform are based on the sum of all the permissions assigned to the user and to all the groups the user is a member of. For example, if the user GeorgeJ has Read access and is a member of the group Techies that has Change access, GeorgeJ will have Change access. If Techies is in turn a member of Administrators, which has Full Control, GeorgeJ will have complete control over the file.

Table 13-4 Special Permissions for Files

Control	**Full Modify**	**Execute**	**Read & Read**	**Write**	**Special Permissions**
Traverse Folder/Execute File	X	X	X		
List Folder/Read Data	X	X	X	X	
Read Attributes	X	X	X	X	
Read Extended Attributes	X	X	X	X	
Create Files/Write Data	X	X			X
Create Folders/Append Data	X	X			X
Write Attributes	X	X			X
Write Extended Attributes	X	X			X
Delete Subfolders and Files	X				
Delete	X	X			
Read Permissions	X	X	X	X	X
Change Permissions	X				
Take Ownership	X				

Table 13-5 shows special permissions used to create the basic permissions for folders. As you study the special permissions, keep the following in mind:

- When you set permissions for parent folders, you can force all files and subfolders within the folder to inherit the permissions. You do this by selecting Reset Permissions On All Child Objects And Enable Propagation Of Inheritable Permissions.
- When you create files in folders, these files inherit certain permission settings. These permission settings are shown as the default file permissions.

Table 13-5 Special Permissions for Folders

Full Modify	Execute	Read & Contents	Folder Read	List Write	Special Permissions	Control
Traverse Folder /	X	X	X	X		
Execute File						
List Folder /Read Data	X	X	X	X	X	
Read Attributes	X	X	X	X	X	
Read Extended	X	X	X	X	X	
Attributes						
Create Files /	X	X				X
Write Data						
Create Folders /	X	X				X
Append Data						
Write Attributes	X	X				X
Write Extended	X	X				X
Attributes						
	X					

Delete Subfolders						
and Files						
Delete	X	X				
Read Permissions	X	X	X	X	X	X
Change Permissions	X					
Take Ownership	X					

Setting File and Folder Permissions

To set permissions for files and folders, follow these steps:

1. In Windows Explorer, right-click the file or folder you want to work with.
2. From the pop-up menu, select Properties, and then in the Properties dialog box click the Security tab, shown in Figure 13-12.
3. Users or groups that already have access to the file or folder are listed in the Name list box. You can change permissions for these users and groups by doing the following:
    - Select the user or group you want to change.
    - Use the Permissions list box to grant or deny access permissions.

    Tip Inherited permissions are shaded. If you want to override an inherited permission, select the opposite permission.
4. To set access permissions for additional users, contacts, computers, or groups, click Add. This displays the Select Users, Computers, Or Groups dialog box shown in Figure 13-13.

Figure 13-12: Use the Security tab to configure basic permissions for the file or folder.

5. Use the Select Users, Computers, Or Groups dialog box to select the users, computers, or groups for which you want to set access permissions. You can use the fields of this dialog box as follows:

- **Look In** This drop-down list box allows you to access account names from other domains. Click Look In to see a list of the current domain, trusted domains, and other resources that you can access. Select Entire Directory to view all the account names in the folder.
- **Name** This column shows the available accounts of the currently selected domain or resource.
- **Add** This button adds selected names to the selection list.
- **Check Names** This button validates the user, contact, and group names entered into the selection list. This is useful if you type names in manually and want to make sure they're available.

6. In the Name list box, select the user, computer, or group you want to configure, and then use the fields in the Permissions area to allow or deny permissions. Repeat for other users, computers, or groups.
7. Click OK when you're finished.

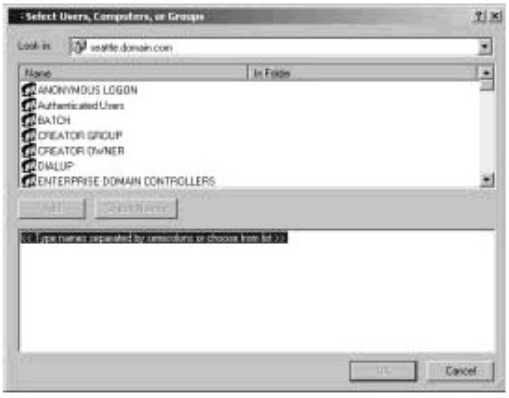

Figure 13-13: Select users, computers, and groups that should be granted or denied access.

Auditing System Resources

Auditing is the best way to track what's happening on your Windows 2000 systems. You can use auditing to collect information related to resource usage, such as file access, system logon, and system configuration changes. Anytime an action occurs that you've configured for auditing, the action is written to the system's security log, where it's stored for your review. The security log is accessible from Event Viewer.

Note: For most auditing changes, you'll need to be logged on using an account that is a member of the Administrators group or be granted the Manage Auditing And Security Log right in Group Policy.

Setting Auditing Policies

Auditing policies are essential to ensure the security and integrity of your systems. Just about every computer system on the network should be configured with some type of security logging. You configure auditing policies with Group Policy. Through Group Policy, you can set auditing policies for an entire site, domain, or organizational unit. You can also set policies for an individual workstation or server.

Once you access the Group Policy container you want to work with, you can set auditing policies by completing the following steps:

1. As shown in Figure 13-14, access the Audit Policy node by working your way down through the console tree. Expand Computer Configuration, Windows Settings, Security Settings, and Local Policies. Then select Audit Policy.
2. The auditing options are
   - **Audit Account Logon Events** Tracks events related to user logon and logoff.

- **Audit Account Management** Tracks account management by means of Active Directory Users And Computers. Events are generated anytime user, computer, or group accounts are created, modified, or deleted.
- **Audit Directory Service Access** Tracks access to the Active Directory. Events are generated any time users or computers access the directory.
- **Audit Logon Events** Tracks events related to user logon, logoff, and remote connections to network systems.
- **Audit Object Access** Tracks system resource usage for files, directories, shares, printers, and Active Directory objects.
- **Audit Policy Change** Tracks changes to user rights, auditing, and trust relationships.
- **Audit Privilege Use** Tracks the use of user rights and privileges, such as the right to back up files and directories.

  Note: The Audit Privilege Use policy doesn't track system access–related events, such as the use of the right to log on interactively or the right to access the computer from the network. These events are tracked with Logon and Logoff auditing.
- **Audit Process Tracking** Tracks system processes and the resources they use.
- **Audit System Events** Tracks system startup, shutdown, and restart, as well as actions that affect system security or the security log.

3. To configure an auditing policy, double-click its entry or right-click and select Security. This opens a Properties dialog box for the policy.
4. Select Define These Policy Settings, and then select either the Success check box or the Failure check box, or both. Success logs successful events, such as successful logon attempts. Failure logs failed events, such as failed logon attempts.
5. Click OK when you're finished.

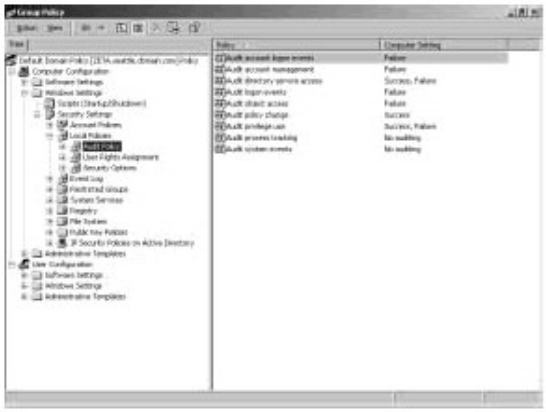

Figure 13-14: Set auditing policies using the Audit Policy node in Group Policy.

Auditing Files and Folders

If you configure a group policy to enable the Audit Object Access option, you can set the level of auditing for individual folders and files. This allows you to control precisely how folder and file usage is tracked. Auditing of this type is only available on NTFS volumes.

You can configure file and folder auditing by completing the following steps:

1. In Windows Explorer, right-click the file or folder to be audited, and then from the pop-up menu select Properties.
2. Choose the Security tab, and then click Advanced.
3. In the Access Control Settings dialog box, select the Auditing tab, shown in Figure 13-15.
4. If you want to inherit auditing settings from a parent object, ensure that Allow Inheritable Auditing Entries From Parent To Propagate To This Object is selected.
5. If you want child objects of the current object to inherit the settings, select Reset Auditing Entries On All Child Objects And Enable Propagation Of Inheritable Auditing Entries.

Figure 13-15: Once you audit object access, you can use the Auditing tab to set auditing policies on individual files and folders.

6. Use the Auditing Entries list box to select the users, groups, or computers whose actions you want to audit. To remove an account, select the account in the Auditing Entries list box, and then click Remove.
7. To add specific accounts, click Add, and then use the Select Users, Contacts, Computers, Or Groups dialog box to select an account name to add. When you click OK, you'll see the Auditing Entry For New Folder dialog box, shown in Figure 13-16.

   Note: If you want to audit actions for all users, use the special group Everyone. Otherwise, select the specific user groups or users, or both, that you want to audit.
8. As necessary, use the Apply Onto drop-down list box to specify where objects are audited.
9. Select the Successful or Failed check boxes, or both, for each of the events you want to audit. Successful logs successful events, such as successful file reads. Failed logs failed events, such as failed file deletions. The events you can audit are the same as the special permissions listed in Table 13-5—except you can't audit synchronizing of offline files and folders.
10. Choose OK when you're finished. Repeat this process to audit other users, groups, or computers.

Figure 13-16: Use the Auditing Entry For New Folder dialog box to set auditing entries for a user, contact, computer, or group.

Auditing Active Directory Objects

If you configure a group policy to enable the Audit Directory Service Access option, you can set the level of auditing for Active Directory objects. This allows you to control precisely how object usage is tracked.

To configure object auditing, follow these steps:

1. In Active Directory Users And Computers, access the container for the object.
2. Right-click the object to be audited, and then from the pop-up menu select Properties.
3. Choose the Security tab, and then click Advanced.
4. In the Access Control Settings dialog box, select the Auditing tab. To inherit auditing settings from a parent object, make sure that Allow Inheritable Auditing Entries From Parent To Propagate To This Object is selected.
5. Use the Auditing Entries list box to select the users, contacts, groups, or computers whose actions you want to audit. To remove an account, select the account in the Auditing Entries list box, and then click Remove.
6. To add specific accounts, click Add, and then use the Select Users, Contacts, Computers, Or Groups dialog box to select an account name to add. When you click OK, the Auditing Entry For dialog box is displayed.
7. Use the Apply Onto drop-down list box to specify where objects are audited.
8. Select the Successful or Failed check boxes, or both, for each of the events you want to audit. Successful logs successful events, such as successful file reads. Failed logs failed events, such as failed file deletions.
9. Choose OK when you're finished. Repeat this process to audit other users, contacts, groups, or computers.