Using NTFS Security

BY GUY C. YOST

In previous columns, I explored using NT's Server and User Managers, as well as strategies for deploying users and groups. This month, I'll cover the basics of NT security and point out some of the sticky areas that might get you into trouble.

Although you can install NT on a FAT partition, you will not be able to take advantage of NT's file and directory-level security unless you use the NTFS (NT File System). Don't fret if you've already installed NT using a FAT file system; you can reliably convert the FAT partition to NTFS without losing any data by using the CONVERT utility as shown in the following example:

```
CONVERT C: /FS:NTFS
```

Be sure you run this as administrator or equivalent when no one is logged on to the system and while no other processes are active. The actual conversion will take place at startup after you reboot the computer. The only danger you face during a conversion is if the server loses power during the actual conversion process. This happened to me once, and I lost the partition. Therefore, it's a good idea to make a backup of the FAT partition before conversion if it contains valuable data.

Let's first define some MS-specific terminology. What others would call "rights," Microsoft calls "permissions." In NT, rights are specific management functions that can be performed on NT servers (such as shutting down the system) and are defined in the User Manager. Permissions describe the actual file and directory-level actions that can be performed by users and groups and are assigned either in File Manager (NT 3.x and 4) or Explorer (NT 4 only). **Note:** For those NT 4 users who became accustomed to 3.x's File Manager, you can still run WINFILE.EXE which ships with NT 4.

Permissions can be assigned to files, directories and shares. (They can also be assigned to shared printers, but more on that in a subsequent column). Shares allow workstations to access specific directories on servers and other workstations, whereas permissions control what actions can be performed on files and directories made available by a share. This month, I'll examine file and directory permissions, and next month, I'll present how to set up shares.

DIRECTORY AND FILE PERMISSIONS

There are six permissions available for files and directories:

- **Read** - Allows opening of file, displaying file contents and viewing information about file's attributes, owner and permission settings.
- **Execute** - Allows execution of binary file (applications).
- **Write** - Allows changing contents of files, attributes and file name.
- **Delete** - Allows files or directories to be deleted.
- **Permissions** - Allows assignment of permissions to other users.
- **Ownership** - Allows taking ownership of a file or directory. The owner has full (supervisory) permissions. Note that even though the ownership permission can be assigned directly to a user or group, actual ownership of a file or directory can only be taken by someone with the Ownership permission. Even as administrator, you can't directly assign ownership to a group or user.

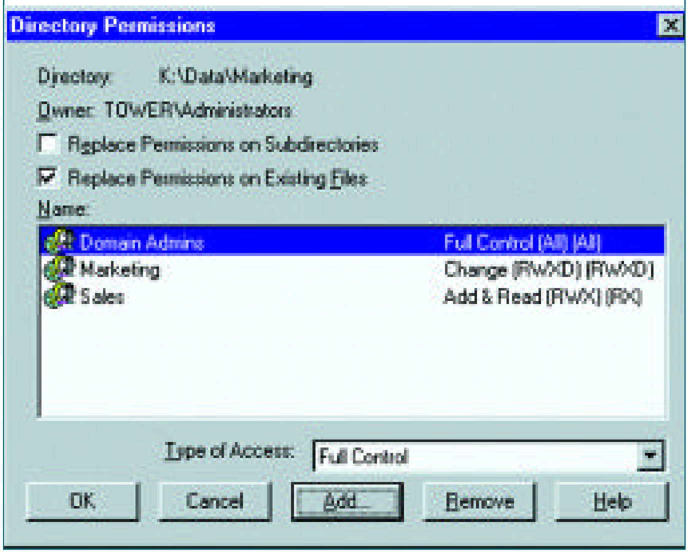
Permissions are typically assigned in predefined combinations called collections. Collections are simply descriptions of what action the combination of permissions will allow. The predefined collections are:

- **No Access** — Applies to directories and files. Overrides all other permissions and blocks access for particular users and groups.
- **List (RX)** — Applies to directories. Allows users to list (dir) files.
- **Read (RX)** — Applies to directories and files. Allows data files to be opened and read, binary programs can Execute.
- **Add (WX)** — Applies to directories. Allows files to be added (created and copied) to a directory.

Gate's Gotcha

The default permission to the root of a new NTFS partition is FULL CONTROL for the group Everyone. When a new directory is created off of the root, it will inherit the root's permissions. When building a new directory structure, be aware of this default as it is likely too open for your applications and shared data. You might want to change the permissions to the Everyone group to RX, or remove Everyone from the root's ACL before building the directory structure.

Figure 1: Assigning NTFS Permissions to Directories and Files



Directory: K:\Data\Marketing

Owner: TOWER\Administrators

□ Replace Permissions on Subdirectories

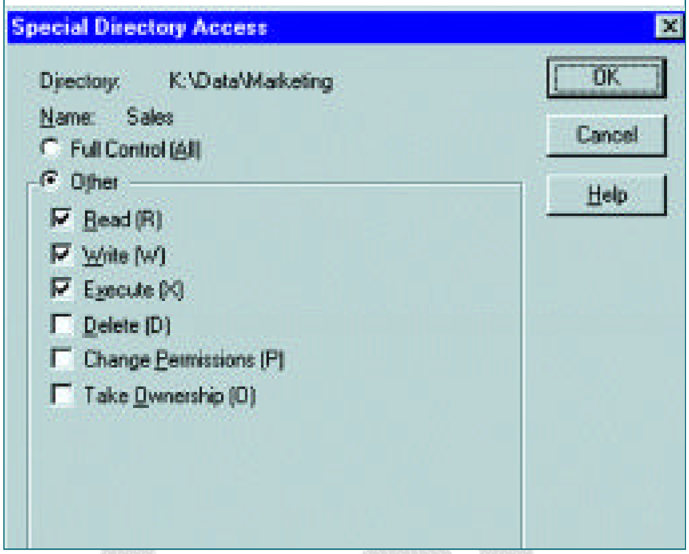
☑ Replace Permissions on Existing Files

Name:

Domain Admins	Full Control (All) (All)
Marketing	Change (RWXD) (RWXD)
Sales	Add & Read (RWX) (RX)

Type of Access: Full Control

Figure 2: Assigning Special Directory Access



Directory: K:\Data\Marketing

Name: Sales

○ Full Control (All)

● Other

☑ Read (R)

☑ Write (W)

☑ Execute (X)

□ Delete (D)

□ Change Permissions (P)

□ Take Ownership (O)

- **Add and Read (RWX to dir; RX to files in directory)** — Allows files to be added to directory and files to be read.
- **Change (RXWD)** — Applies to directories and files. Allows files and directories to be created and changed, as well as attributes modified.
- **Full Control** — Applies to directories and files. Allows all actions including changing permissions and taking ownership.

Assigning NTFS rights to files and directories is straightforward. In NT 4, highlight the file or directory in My Computer or Explorer, and click on the right mouse button to display the options menu. Choose Properties from the bottom of the list and then click on the Security Tab. Next, click on the Permissions button to display the Permissions assignment window similar to Figure 1.

From this screen, add the appropriate groups to the directory's ACL as indicated by your NRM (see my March 1998 column for an example of a Network Resource Matrix) by clicking on the Add button and choosing the group name that you want to have access to the directory. (From the Add Users and Groups window you can add individual users to the ACL if you wish by clicking on the Show Users button. However, as a rule, only groups are displayed by default as to suggest using groups rather that users.) Permissions are assigned by clicking on the Type of Access pull-down menu and choosing one of the previously described collections. Alternatively, you can assign any explicit combination of the permissions by selecting "Special" access from the pull-down menu and selecting each permission individually as shown in Figure 2.

Note from Figure 1 that you can assign different collections of permissions to different groups for the same directory. Also note that you can force the permission assignments to apply to all files and subdirectories within the directory by selecting the two options at the top of the window.

As a time saver, you can highlight multiple (peer) directories using the shift or control key along with the mouse click and assign common permissions in one shot. Likewise, in File Manager, if the directories you'll work with are displayed in the right-most window you can use the control and shift keys to select multiple directories or files to work in one operation.

Note: *When a file is copied, the newly created file inherits the permissions of the destination directory and the copier becomes the owner of the new file. When a directory is copied, the newly created directory and its files inherit the default directory and file permissions of the receiving directory, and the copier becomes the owner of the directory and files. When a file or directory is moved, the permission and owner assignments are not changed.*

SUMMARY

NTFS security can be effective, but as you can see, you need to be aware of the caveats before implementing a secure network. Also, if you have properly planned the security implementation of your network using a NRM, then the process of assigning permissions will be simply mechanical.

Next month I'll examine how to set up shares and how NTFS and share-level permissions interact. As always,thanks for reading. ts

NaSPA member Guy C. Yost is the owner of Redstone Consulting, an IT management consulting firm in New York. He has authored several books on networking for Que Publishing, including Learning NetWare 4.1, and NetWare 4.1 SmartScan, and contributes to Technical Support magazine as an author, columnist and technical editor. Guy also develops and conducts seminars on networking with Windows NT, UNIX, NetWare and Internet/intranet technologies across the United States and Canada. He can be reached at (518) 674-5606 or gyost@logical.net.