Network basics: Part 20 - File level permissions

In the previous part of this series, we introduced shared folders that can be protected using share level permissions or NTFS permissions.

Brien M. Posey

In the previous part of this series, we introduced shared folders that can be protected using share level permissions or NTFS permissions. In that article, we also introduced how to use share-level permissions, but it has a lot to do with secure file sharing with NTFS permissions, so in this section we will introduce more. to you about these terms.

Convert command (Convert)

As we explained many times before, you can only use file level security for partitions formatted with the NTFS file system. If the partition is formatted with FAT or FAT32, you will be limited in using share level permissions. However, you can convert between FAT or FAT32 partition into NTFS without having to reformat the partition. Perform such conversions with the Convert command. If the partition you are concerned about is already formatted as NTFS, then this section can be ignored.

This switch command is very simple to use. In its simplest form, you only need to specify the drive letter assigned to the partition you want to convert, the file system you want to use (in this case, NTFS). For example, if you want to convert drive D: to NTFS, the command structure will look like this:

CONVERT D: / FS: NTFS

Although this basic syntax always works, there are two additional switches that we recommend using with this command. The first switch to use is **/ X.** This switch requires that the partition be removed before the conversion process takes place. The reason why you should use this switch is because it will avoid opening file corruption during the conversion process. Obviously a minor effect here is that the management of open files will be disconnected.

Another switch is **/ NoSecurity** . This switch tells Windows that you want to leave everything on the partition so everyone has access to it after the conversion process is complete. Obviously, applying the switch has gone against the whole purpose of converting the original partition. However, we still like this switch because it lets you choose to enforce all security settings from a particular attack instead of dealing with the default security settings of Windows. When both of these conversions are applied, the command will look like the following:

CONVERT D: / FS: NTFS / X / NoSecurity

NTFS permissions

For the most part, NTFS permissions are very easy to set up terms. Just right-click a folder and select the **Properties** command. You can assign NTFS permissions to the folder on the **Security** tab of the properties page as shown in Figure A below.

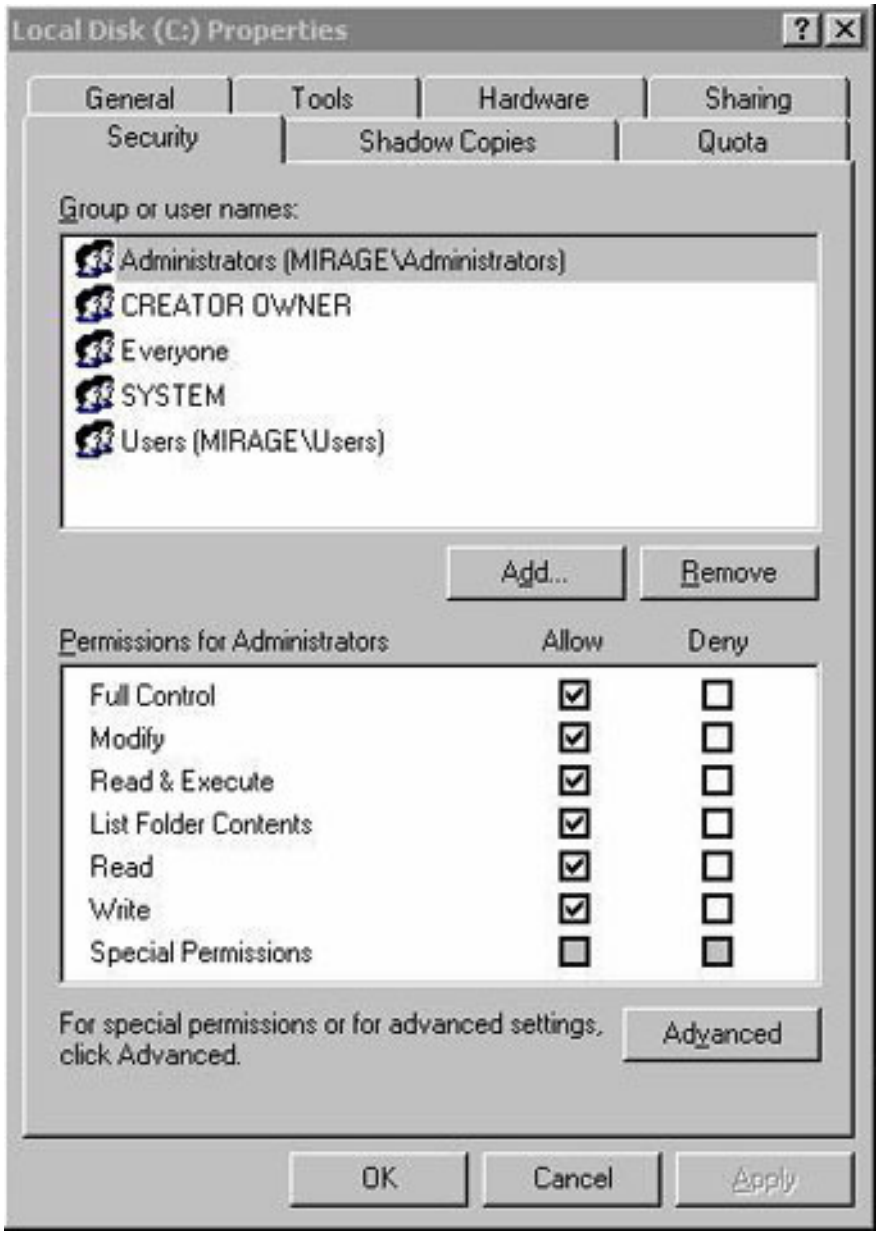

Figure A: NTFS permissions are assigned via the Security tab of the property sheet

As you can see in the picture, the upper part of the tab contains a list of users and groups. You can use the **Add** and **Remove** buttons to add or remove users and groups from this list. You can also set permissions for users or groups by selecting a user or group from the list, and then using the checkboxes in the section below the tab.

These terms themselves are very understandable, so we will not go into specifically what is in each of those

terms. There are only two things you need to know about this tab: before you can choose to 'allow permission', 'denying permission', or 'not doing either'. Note that the 'denying permission' option always overrides a previous clause. You also need to realize that if you do not set a clause, you may not receive the clause through inheritance. We will talk more about this inheritance issue in the next section.

Another thing to know about this tab is, although you can set permissions on individual users or groups, but for individual users it is often assigned poor terms (poor than). If you assign permissions to individual users, there will be some missing things that can make you quite unhappy. Therefore, you should assign terms to groups.

Another point that you can see in the image above is the **Advanced** button. Since this is a beginner's blog, we don't want to spend a lot of time talking about advanced concepts but there are two very important aspects of NTFS permissions that you need to know.

If you click on the **Advanced** button, you will see the **Advanced Security Settings** property sheet, shown in Figure B below. Look at the two check boxes below the **Permissions** tab.

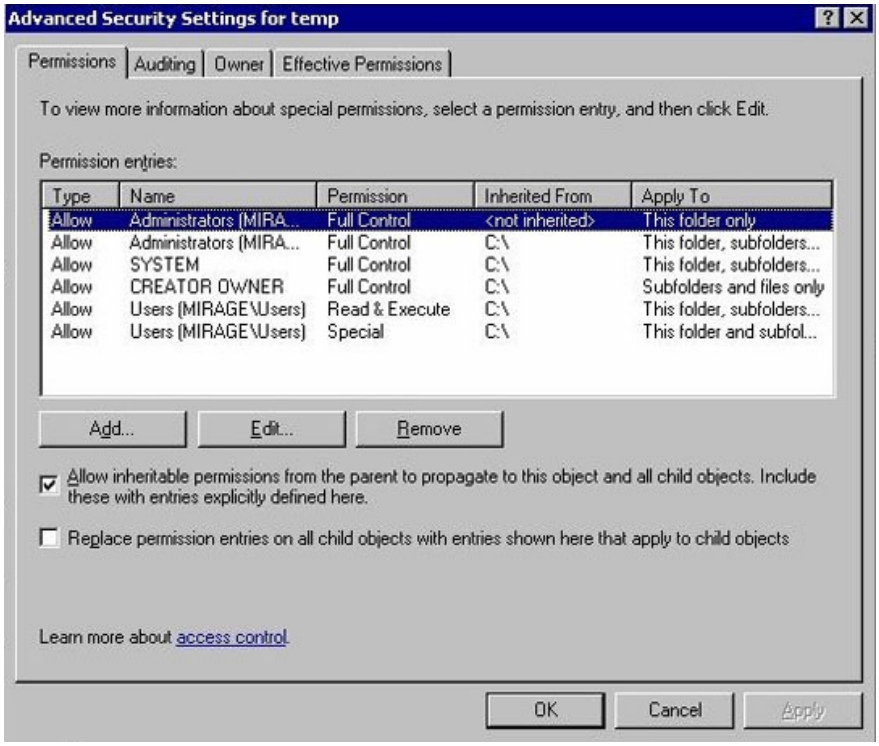

Figure B: Two checkboxes at the bottom of the Permissions tab allow you to control inheritance

The NTFS file system uses a concept that is inheritance. This concept means that when you set a clause, that provision applies to any file or subdirectory below it. The first checkbox in the Permissions tab is defaulted. It allows inheritance to apply to selected folders and subdirectories within it.

The second checkbox allows you to replace any existing permissions on files and subdirectories using the terms shown in the list above.

As you can imagine, these check boxes are very powerful and using them incorrectly can have big consequences.

Therefore we recommend that you never use them and in fact Microsoft also advises that.

Conflicts

There is one thing about how the NTFS file system works and how the Windows security system works in general, sometimes there are conflicting issues in security. For example, a user can be a member of two different groups with conflicting terms. When this happens, there will be a whole set of rules that can be applied to indicate which permissions have a higher priority.

Since this series is written for beginners, we won't go into the complexities of rules. One thing we want to tell you here is that the denial statement will always override other terms. Instead of using another introduction to the rest of the rules, I want to show you a tool that can be used to determine the permissions that are in effect.

We have already shown you the **Advanced Security Settings** property sheet, but consider its **Effective Permissions** tab, shown in Figure C below. This tab allows you to enter the names of users and groups. Through it it will display the terms that are valid for that user or group.

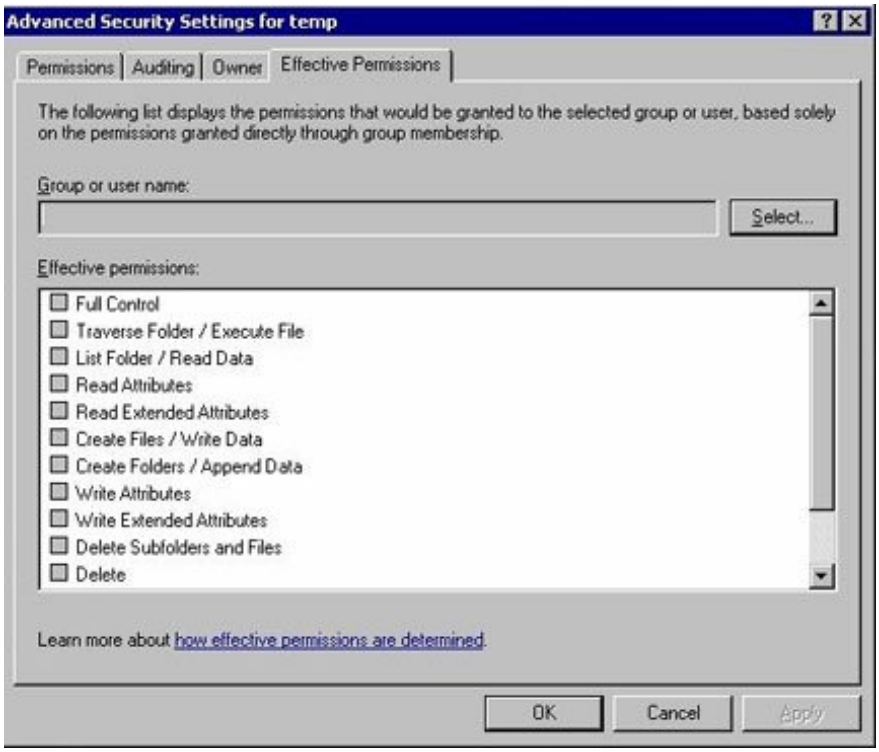

Figure C: Tab Effective Permissions allows you to see NTFS permissions valid for certain users or groups

Conclude

This will be the last part in this series, the reason we want to stop writing because the purpose of this series is for novices to network. Therefore, in-depth referrals will make you difficult to understand. However, in the future we will provide you with further knowledge about this topic, please read and send feedback.

articles on tips and guides. Thank you for reading and for following us regularly.