Network basics: Part 19 - Sharing level terms

In the previous part of this series, I began showing you how to create a shared network that can be used to share resources on a server. So far, we have created a ch

Brien M. Posey

In the previous part of this series, I began showing you how to create a shared network that can be used to share resources on a server. So far, we have created a share but have yet to give anyone access to that share. In this section, we will continue the discussion of the differences between file level and share level permissions.

Secure shared password

Although the whole purpose of sharing is to allow users on the network to access the resources within the shared item, you must still be careful about the level of access to resources for users. . For example, suppose the company has a spreadsheet that lists salary information for each employee. Now assume that everyone in the accounting department can access that spreadsheet and update the content inside. Since the accounting department is responsible for printing invoices, they need to access this spreadsheet, but you may not want them to make modifications. Because of the sensitivity of the information in the spreadsheet, you may not want anyone in the company to access it. With those notes, let's consider how this type of security can be implemented.

The first thing you need to understand about sharing is that there are two different types of security that can be used. You can choose to use shared-level security, file-level security, or both.

Share level security is used directly for the share point you created. When a user connects to SharePoint to access the file, the sharing level permissions that you set will apply. In contrast, file level permissions are applied directly to files and folders instead of sharing.

The reason there are two different types of permissions in Windows is because the Windows operating system supports two different formats: FAT and NTFS. FAT is a pre-existing file system and was introduced in the 1980s. FAT is a file system that does not support file level security and NTFS is designed to fix these vulnerabilities. You can apply file level security directly to files and folders placed on NTFS formatted drives.

Because the NTFS file system does not support file-level security, Microsoft allows you to use shared-level security as a way to improve file system deficiencies. Today the NTFS file system is mostly used and the FAT file system is still there but is rarely used. You can still use share level permissions if you want, but you better use file level sharing permissions.

So what makes file level permissions better than share level permissions? For starters, share level permissions apply only if the user is accessing the file through a share. This can be a problem because Windows allows you to create multiple share points on one drive. If sharing points have been created in a less careful way, they may overlap with other points. This can cause users to have unexpected permissions levels for files and folders.

Another reason why file level permissions are preferred over share level permissions is because share level permissions do not provide protection unless users access files through SharePoint. If a user has logged into an internal server management interface, they can browse to the internal hard drive without going through SharePoint. If the sharing terms are the type of clause being used then the user can access with full access to the shared files inside.

File level permissions also allow data protection if the server is started to switch the operating system, or if the hard drive is removed from the server and replaced with another server. Shared level permissions do not provide this type of protection.

Because file level permissions are much higher than share level permissions, you might be wondering why you want to create a share for everyone. You need to create a share because it acts as an entry point for accessing the file system in the network. If you need to allow users to access files on a file server, you don't really need to create shares. However, you can protect sharing by using file level permissions instead of depending on share level permissions.

We created a folder named Data in the previous part of this series, then shared that folder. To set permissions in this directory, right-click it, select **Properties** . After doing so, you will see a folder properties page.

Now consider the Sharing tab of this property sheet, see Figure A for more details. As shown in the picture, this tab has a **Permissions** button. You can click this button to set share level permissions for sharing.

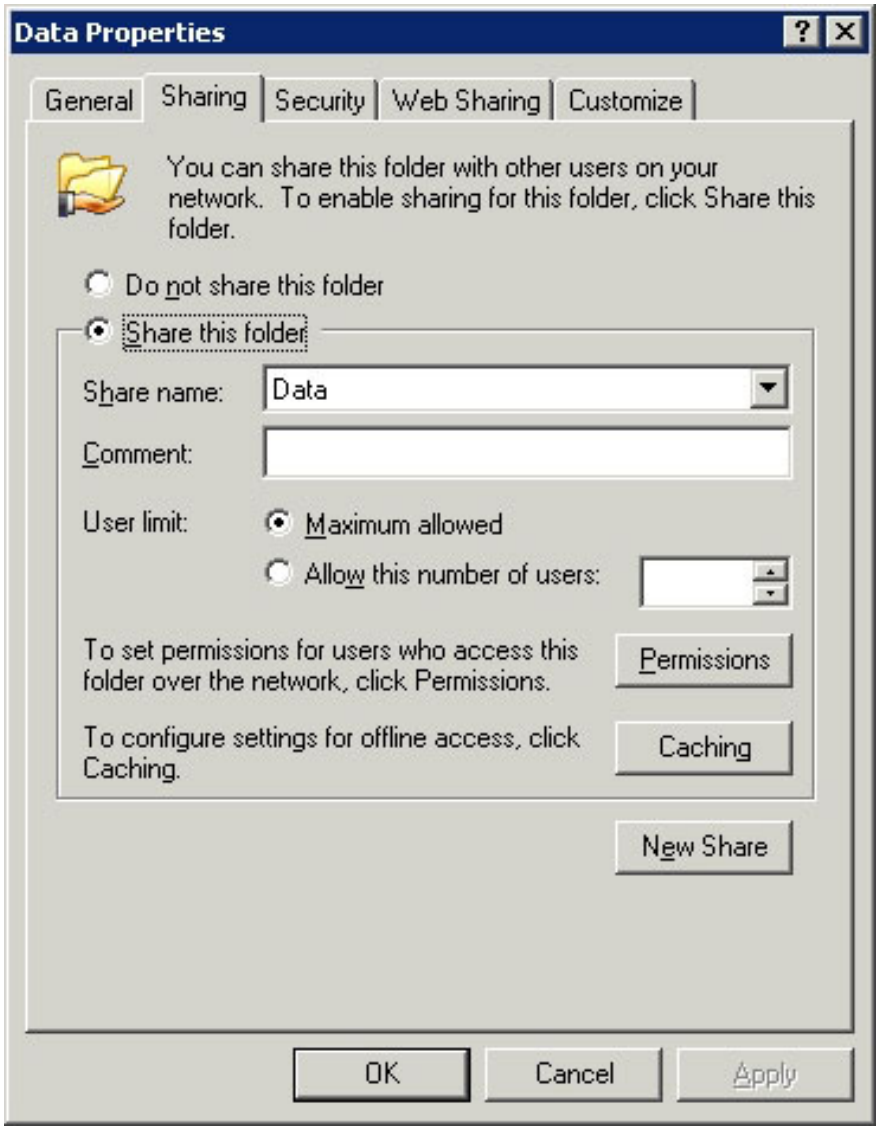

Figure A: The Permissions button is used to set sharing level permissions

Let's take a look at the **Security** tab. This tab is used to set file level permissions, starting at this directory or later, SharePoint will be bound. The first thing you need to know about file level permissions is that in any case they use the inheritance concept. Inheritance here simply means that when you set up a clause, that provision applies not only to the directory and also to everything in it. It can include existing subdirectories and files within subdirectories.

Another thing you need to know about file level permissions is the inheritance of some permissions that apply automatically. If you look at Figure B, you will see the **Security** tab of the properties page. As you can see in the figure, several different sets of terms have been applied. Details of how these settings are described are detailed in the following series. Now you just need to know the fact that there are some terms that apply automatically.

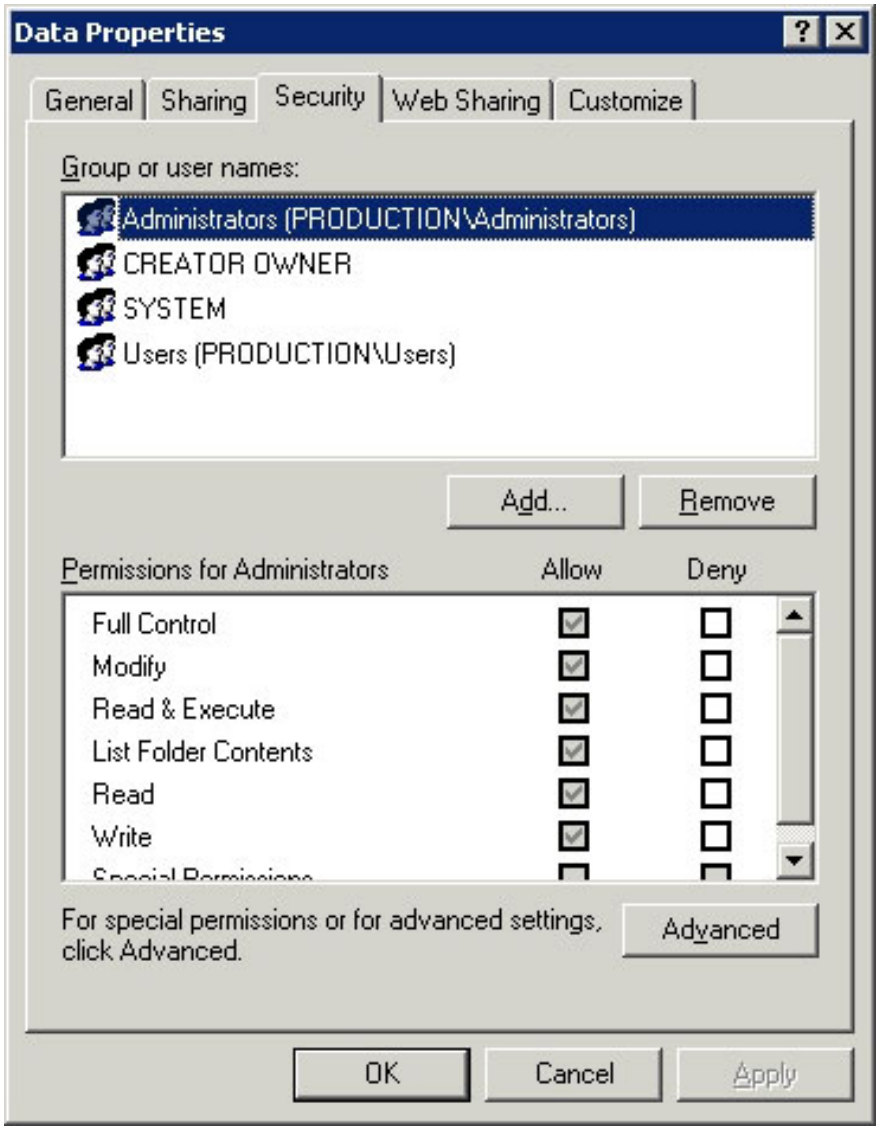

Figure B: The Security tab can be used to set file level security
for the directory that SharePoint is bound to.

If you look at the **Security** tab, you'll notice that the first half of this tab contains a list of users and groups. Below that is a list of terms. If you want to apply a set of permissions to a user or group, simply select the user or group you want to work on the upper half of the tab, then set the permissions in the lower half. Obviously before you can set the permissions you need to understand what those terms mean. We will cover that in detail in the next part of this series.

Conclude

In this article, I have shown you how to protect a SharePoint using file level or share level permissions, or both. In the next part of this article series, I will show you how these permissions work and how to apply them to files and folders.