Return to article

Let's Get Organized: File Server Basics

From the May 2007 Edition of Windows IT Pro
April 25, 2007
Eric B. Rux
Feature
InstantDoc #95354
Windows IT Pro

Although a file server is one of the most basic services in the server room, I've been surprised at how disorganized many organizations' file servers are. After helping several companies reorganize their file servers, I decided to share some of the common problems that I've seen and introduce you to some ways to fix them by using Windows 2003 built-in features, free add-ons, or new business processes. Come on—let's get organized!

Scattered Data

One company I worked with had fewer than 100 employees but had eight file servers and hundreds of shares. The administrator had a hard time finding the files he needed, and users' desktops were a sea of shortcuts. For this company, consolidating servers and shares onto one large file server made sense. Depending on the service level agreement (SLA) that your IT department has, you might want to consider a cluster or other technology to reduce the risk of putting all of your eggs in one basket. Regardless of your choice, the important thing is to keep your file server structure as easy as possible for users.

For companies that have data scattered all over creation, I recommend a complete reorganization. This option isn't as difficult as it sounds if you carefully plan and communicate well with the rest of the organization. You can gauge the level of file server organization by learning how content or frustrated users are. If the problem isn't that bad (i.e., users can generally get to the information they need), then a simple housecleaning might be in order. Regardless of the scope of your reorganization, I can't over-emphasize the importance of ensuring that the cleanup is a company objective and not just an IT project. You need the support of your company's decision makers.

My ideal file server has just one share that contains multiple parent subfolders. This structure is clean, simple, and provides one-stop shopping for users. Every company is different, but the structure typically looks something like the example that Figure 1 shows. As you can see, the file server has an appropriate name, the share describes the file server's contents, and the subfolders are logically laid out. What about the subfolders that are in the parent folders? Each department should organize its own folders, but you can provide some guidance. I typically ask users leading questions such as the following:

- Do you have any sub-departments or teams? If so, you might create subfolders to further segregate the data. A large IT department might create subfolders such as Infrastructure, Development, Project Management, and Quality Assurance.
- Is your work separated geographically, or do you all work together? If multiple locations daily share data, it wouldn't make sense to create Seattle, Portland, and New York subfolders for each location. If the business divisions work independently, a single folder wouldn't be efficient. This example shows why this project can't be just an IT project; the business needs to own the plan.
- Does your department include different levels of security access? Securing individual files is time-consuming and leads to mistakes. These "one-offs" are easy to forget about, and the security is easy to overwrite if security settings are pushed down from the parent folder to the files. If the department has security boundaries, help department members create their subfolders to mirror those boundaries.
- If you had to print out all of this data, how would you organize it in a filing cabinet? This question helps users stop thinking about data as bits on a screen and start thinking in terms of documents. Help users organize the file structure as they would organize manila folders in metal drawers.

Once you've set up and secured a basic file-server structure, each department can start to move its data to the new structure. (We'll cover more information about security permissions in a moment.) Be sure to teach users the difference between moving and copying. Moving the data provides a clean break from the old way of storing documents and lets users handle their own data. A good practice is to give users a "due date" when all of the files must be moved.

"Simplify Your Life: Role-Based Security

Now that you have a fresh folder structure, you need a simple way to secure it. In every company that I've consulted with, I've found at least one user account in the Security tab of a file or folder. These rogue accounts typically appear because an administrator or Help desk technician was in a hurry and wanted to close a trouble ticket quickly. Unfortunately, this practice can cause headaches down the road if the user you've given special privileges to changes departments.

For example, one company I worked with regularly moves its temporary accounting help to a full-time position on the operations floor. If a user has permissions to access accounting files and moves to a new position, it can be a real challenge to find all of the places that user had permissions. Finding the permissions is so difficult that often the user would transfer to a new position with the old accounting permissions still intact.

In such a case, the answer is to use security groups. Groups have been around since the early days of LAN Manager. Although most organizations have security groups, many aren't using groups to their full potential. In my consulting work, I typically call security groups "roles." When combined with official roles in the company, security groups are a powerful

security solution. So instead of using obscure security group names that only IT understands, roles let managers control the data their employees can access. Imagine a list of security group roles for the accounting department that looks like this:

- Role Accounting VP
- Role Accounting Manager
- Role Accounting AP
- Role Accounting AR
- Role Accounting Temp
- Role Accounting All

Only these roles have access to your new folder structure. Now when a new accounting employee is hired, it's easy for the manager to explain to the Help desk exactly what security groups the user should belong to.

When you add roles to the security of the folder, you can use the naming convention I show above and the additions will be a snap. Find the folder for which you want to configure security. Right-click the folder, and choose Properties. Click the Security tab and click Add. Type the word Role in the *Enter the object names to select* field, as Figure 2 shows, and you'll get a list of the roles that are in your Active Directory (AD).

Folder Free-For-All

What does your file server's root-share folder structure look like? Do you have a lot of folders, individual files, and the occasional shortcut? If so, you're giving folder permissions too liberally. You need to take back control.

When setting up your new structure or reorganizing an existing one, be sure to set the root folder's NTFS permissions for the Everyone group to Read & Execute, List Folder Contents, and Read, as Figure 3 shows. These basic permissions keep the root clear of erroneous files and new folders that don't comply with your new structure.

Figure 4 shows an example of permissions to set for the example file server structure in Figure 1. Setting the permissions this way gives members of the Everyone group read access to folders so that they can navigate to subfolders. Users can then write to appropriate folders based on the roles they belong to.

Folder Overload

In Figure 1's example, you can see all of the folders under the Data share. Most likely, your users also see all of the subfolders in your file structure, regardless of whether they have permissions for them. Until recently, this exposed view was necessary because all Windows servers worked that way; your permissions on the folder had no bearing on whether you could see the folder. If you come from a Novell environment, as I do, then you probably think this folder exposure is a huge oversight on Microsoft's part. Fortunately, Microsoft has finally remedied the problem (for Windows Server 2003 only) by supplying a small add-on called Windows Server 2003 Access-based Enumeration (ABE).

According to Microsoft, ABE "makes visible only those files or folders that the user has the rights to access. When Access-based Enumeration is enabled, Windows will not display files or folders that the user does not have the rights to access." Chances are, most of your users don't have access to all of the parent folders, so why show them the entire list? For example, a user who has permissions to work only with the Production folder doesn't need to see all the folders in the list in Figure 1. With ABE enabled, the folder list in Figure 1 is reduced to one folder: Production.

I've heard some people argue that ABE is simply "security through obscurity." But ABE doesn't simply hide the folder so that users don't accidentally stumble on and access it. ABE hides the folders you don't have access to. It's not a security feature, it's a management feature that can make your file server easier to navigate.

Installing and configuring ABE is simple. You can downloaded the add-on from the Microsoft downloads site (http://www.microsoft.com/downloads) by typing "download ABE" in the search box. The installation is quick and asks you only for basic input such as acceptance of the license agreement and where you want to install the add-on. Once the installation is complete, find a folder that's shared (or share a folder), right-click the folder, and choose Properties. You'll notice a new tab called Access-based Enumeration, which Figure 5. From this tab, you can choose to enable ABE on just this folder or on all shared folders on the computer. That's it!

Folder Security: Who's in Charge?

In the Microsoft networking classes that I've taught, we cover folder and file security extensively. We do so for a good reason: A junior administrator must have an intimate understanding of how these security technologies work. Unfortunately, these same junior administrators are also expected to know what security permissions each folder and file should have. When they receive a Helpdesk ticket asking them to change a folder's security, these administrators are somehow expected to know whether "Bob" should have access to the Accounting folder. Clearly, this expectation is unrealistic.

One company I know has successfully turned that paradigm around. Not only is IT out of the file- and folder-security business, company policy now forbids IT staff from changing folder permissions for other departments. Let me explain how this model works.

Who knows the most about the files that a department creates? That department, of course. In my example company's model, users are responsible for placing their own files in the appropriate place on the file server. Only the users are the data owners of their files. Like the junior administrator, users receive training in file security, the importance of roles, and how to ask for help if they get stuck.

This model is fine for the files that users create. But who's responsible for the department's data overall? Who ensures that someone from the manufacturing floor can't accidentally access accounting's files? The responsible person probably should be the vice president or manager in charge of the department, but often the responsibility is often delegated to a "file-security manager" in the department. This person is the file-security expert in the department and is responsible for ensuring that the department's data is secure. The company in question even has a role called Role Accounting File Security Manager that has access to all of the data for the Accounting department. If users need help or have a question, the Help desk is always available to assist. But gone are the days of an administrator who has to guess whether to give a user access to a folder.

So, how do you convince your company to use role-based security? The sidebar "Selling Role-Based Security," page 45, outlines some of the questions that your company's executives might want to know when you present the idea to them.

Share and NTFS Permission Confusion

So how do I teach junior administrators how to troubleshoot folder-security problems? In class, it goes a little something like this.

First, a little history. The notion of a share (from Microsoft, anyway) first debuted in 1987 with LAN Manager, which lets users connect to a hard drive on a server. Administrators then assign to the share permissions such as Full Control, Change, or Read. The concept seems simple now, and shares work the same today as they did back then.

With Windows NT 3.0, Microsoft introduced NTFS. Unlike FAT, which doesn't have any security features, NTFS lets you secure folders and files by using granular security. Thus, multiple users can log on to the same machine but have separate, secure work areas that other users can't access.

So now that we know that shares and NTFS both have security permissions that can be assigned to a folder (even though their original uses were different), what's the best way to proceed? One thought is to simply open up the share to Everyone with Full Control, then lock down security by using NTFS permissions. Another option is to use share and NTFS permissions together. Either way, you must be able to determine what a particular user's access to the data is.

Figure 6 shows an example of how you can choose the best security for a given user. In Figure 6's D:\data folder, Bob has the following NTFS permissions: Full Control, Modify, Read & Execute, and Read. Of these permissions, Full Control is the least restrictive. Bob also has Read permission on the data share. Because this is the only permission Bob has, it's the least restrictive permission he has on the share. (If Bob had Read and Change permissions on the share, then Change would be the least restrictive.)

Now that we know Bob's least restrictive NTFS and share permissions, we must find his resultant permission by finding the most restrictive permission between the least restrictive NTFS and share permissions. If Bob attempts to access this share from the network, he'd have Read permission. He wouldn't be able to change, delete, or add new files.

Troubleshooting mixed NTFS and share security permissions can be a challenge. That's why many companies just configure the share by giving Everyone Full Control, then lock down the files and folders by using NTFS permissions.

Go Forth and Organize

Perhaps you know of a file server or two that looks a lot like the ones I describe in this article. If so, then it's time to set up a practice lab and configure a file server the right way. Once you have a clear understanding of how the technologies work, go forth and organize!

Figure 1

Figure 1: A clean file-server structure

Figure 2

Figure 2: Add a security role

Figure 3

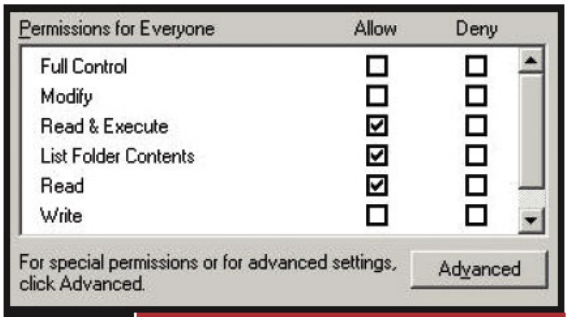


Figure 3: Basic permissions for the Everyone group

Figure 4

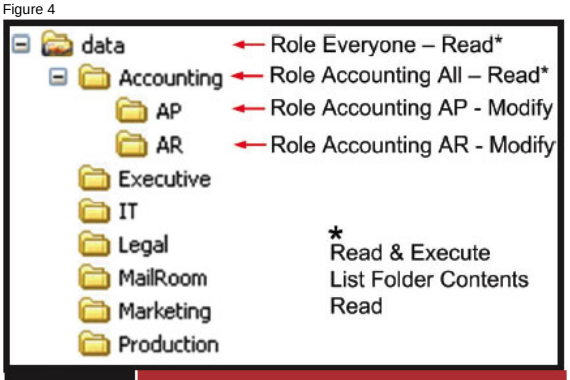


Figure 4: Permissions for the example file-server structure

Figure 5

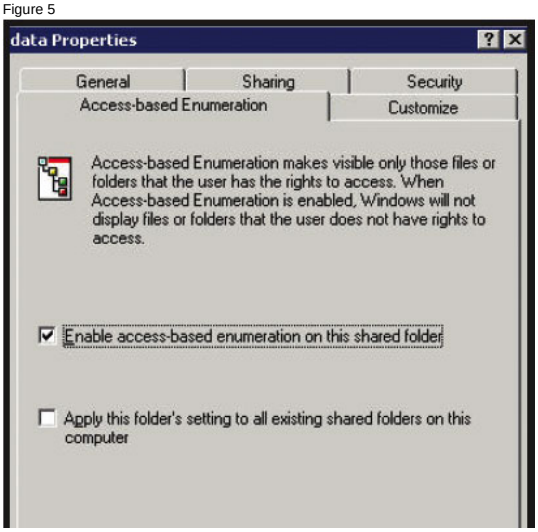
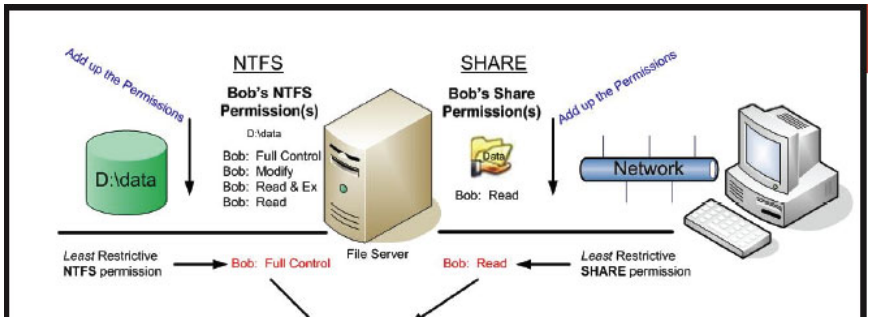


Figure 6



Reader Comments

Good artical, but in the printer frendly version Figure 6 is cut off!!

norris.norman.c2@edumail.vic.gov.au -May 24, 2007