

Windows File Sharing

8/2008

This document explains some of the bare essentials for configuring a Windows Server for file sharing.

Create File Shares

- Folders must be “Shared” before they can be accessed remotely by users.
- To access a remote share, the user must connect to the share using the format:
[\\server\share](#)
Note: Using the FQDN for the server is a best practice. Shorter NetBIOS names will work under many circumstances.
- Access to files remotely is a combination of Share and NTFS file system permissions. When permissions have been assigned both to the shared resource and at the file system level, the more restrictive permission always applies.
- Share Permissions that will only give your users the ability to access the file share remotely, but not the folders and files.
- NTFS file system permissions control the actual access to the folders and files.

Example:

This example shows how to create a simple share named **Shared**, and assigns basic permissions so everyone can read and write to it. A full hierarchy of subfolders with different permissions for different groups can be created, but is out of scope for this discussion.

- Create a folder named **Shared** on the D: drive of a server named itcs-server1.adsroot.itcs.umich.edu.
- Right click on folder and choose “Security and Sharing”
- Select “Share this folder”. Notice that the Share name is entered.
- Click on the Permissions button.
Select Everyone and click Remove
- Select Add and add your OU Admins group
Select the Allow Full Control checkbox.
- Select Add and add a group you want to have access to this folder, for example **unit-all-users**.
Select the Allow Change and Read permissions.
Note: These are the Share Permissions that will only give your users the ability to access the file share remotely, but not the folders and files.
- Click OK to return to the Properties of the folder.
- Select the Security tab. These are the NTFS permissions and control the actual access to the folders and files.
- Select Add and add your OU Admins group
Select the Allow Full Control checkbox.

- Select Add and add a group you want to have at least read access to the root of this folder with more possibly access to lower folders., for example **unit-all-users**. Leave the default security, Read and Execute, List and Read. Select Allow Write and Modify
- Click OK. Your users can now access this folder remotely by mapping a drive to: [\\itcs-server1.adsroot.itcs.umich.edu\Shared](http://itcs-server1.adsroot.itcs.umich.edu/Shared) and have read and write access to all files, folders, subfolders and files.

More info on NTFS Permissions:

<http://www.windowsecurity.com/articles/Understanding-Windows-NTFS-Permissions.html>

Configure computers to access file shares

Computers can be configured to access file shares in many ways. Use the server and share name you created in the above step using the format [\\server\share](#). It is generally better to use the FQDN name of the server to insure reliable name resolution.

If your computer is a member of the domain and you have logged onto the computer with your domain credentials (not a local logon), then you will not be prompted to enter a username and password.

- Map a drive using Windows Explorer. You can choose whether or not to reconnect at logon.
- Map a drive using a logon script. (See Logon Script Basics document)
- Start > Run [\\server\share](#)
- Create a shortcut icon with the target of [\\server\share](#).
- Create from the command line: `net use X: \\server\share`

Disk Quotas

Disk Quotas are set per volume per user or group on the Quota tab of the Properties of the volume. They are not particularly granular or useful. Use the new File Resource Manager for more granular control.

File Resource Manager

File Server Resource Manager is a suite of tools that allows administrators to understand, control, and manage the quantity and type of data stored on their servers. By using File Server Resource Manager, administrators can place quotas on folders and volumes, actively screen files, and generate comprehensive storage reports. This set of advanced instruments not only helps the administrator to efficiently monitor existing storage resources but it also aids in the planning and implementation of future policy changes.

See <http://technet.microsoft.com/en-us/library/cc755603.aspx> for more information.

Shadow Copy

Shadow Copies for Shared Folders is a new file-storage technology in the Microsoft Windows Server 2003 operating systems. Shadow Copies for Shared Folders uses the Volume Shadow Copy service to provide point-in-time copies of files that are located on a shared network resource, such as a file server. With the Previous Versions client for Shadow Copies for Shared Folders, users can view shared files and folders as they existed at points of time in the past, without administrator assistance.

- Enable Shadow Copies by selecting the properties of a logical disk in Windows Explorer
- Select Enable
- Select Create Now

Introduction to Shadow Copies of Shared Folders

<http://www.microsoft.com/windowsserver2003/techinfo/overview/scr.msp>

Access Based Enumeration

Windows Server 2003 Access-based Enumeration 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. This download provides a GUI and a CLI that enables this feature.

Windows Server 2003 Access-based Enumeration

<http://www.microsoft.com/downloads/details.aspx?FamilyId=04A563D9-78D9-4342-A485-B030AC442084&displaylang=en>

Distributed File System – DFS

With Distributed File System (DFS), system administrators can make it easy for users to access and manage files that are physically distributed across a network. With DFS, you can make files distributed across multiple servers appear to users as if they reside in one place on the network. Users no longer need to know and specify the actual physical location of files in order to access them.

ITCS needs to set up the initial DFS folder for your unit. Then you can manage it yourself. Contact windows.support@umich.edu

<http://technet.microsoft.com/en-us/library/cc738688.aspx>