

Realtime  
publishers

"Leading the Conversation"

*The Definitive Guide<sup>™</sup> To*

# Building a Windows Server 2008 Infrastructure



*Greg Shields*

---

Chapter 4: File Servers & Storage Management .....	82
The Role of the File Server .....	83
Basic and Advanced Folder Sharing .....	84
Installing the File Services Role .....	87
Share & Storage Management .....	88
Access-Based Enumeration .....	90
File Services Role Services .....	91
Distributed File System – Namespaces .....	91
Distributed File System – Replication .....	93
File Server Resource Manager .....	95
Quota Management .....	96
File Screening Management .....	97
Storage Reports Management .....	98
Services for Network File System .....	99
Windows Search Service .....	101
Windows Server 2003 File Services .....	102
Properly Managing Storage Eliminates Critical Downtime .....	103

## Copyright Statement

© 2008 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at [info@realtimepublishers.com](mailto:info@realtimepublishers.com).

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

## Chapter 4: File Servers & Storage Management

This guide is designed to give you an overview of the topics and technologies you need to know to properly deploy a Windows Server 2008 infrastructure. Along those lines, the order of topics I've chosen to present here should align with how you'll likely be bringing these services into your existing Windows environment. We have spent time talking about the prerequisites and installation processes associated with getting servers onto hardware. We then focused on the centralized management tool Server Manager where you're likely to initially be spending a lot of time. In Chapter 3, we discussed Active Directory (AD) in-depth and its installation to candidate Domain Controllers.

Now that we have a domain in place running atop Server 2008, the next likely place where Server 2008 will make its way into your environment is within your file servers. Why here? As with Domain Controllers, owing to their composition and requirements, file servers make excellent candidates for early Server 2008 adoption:

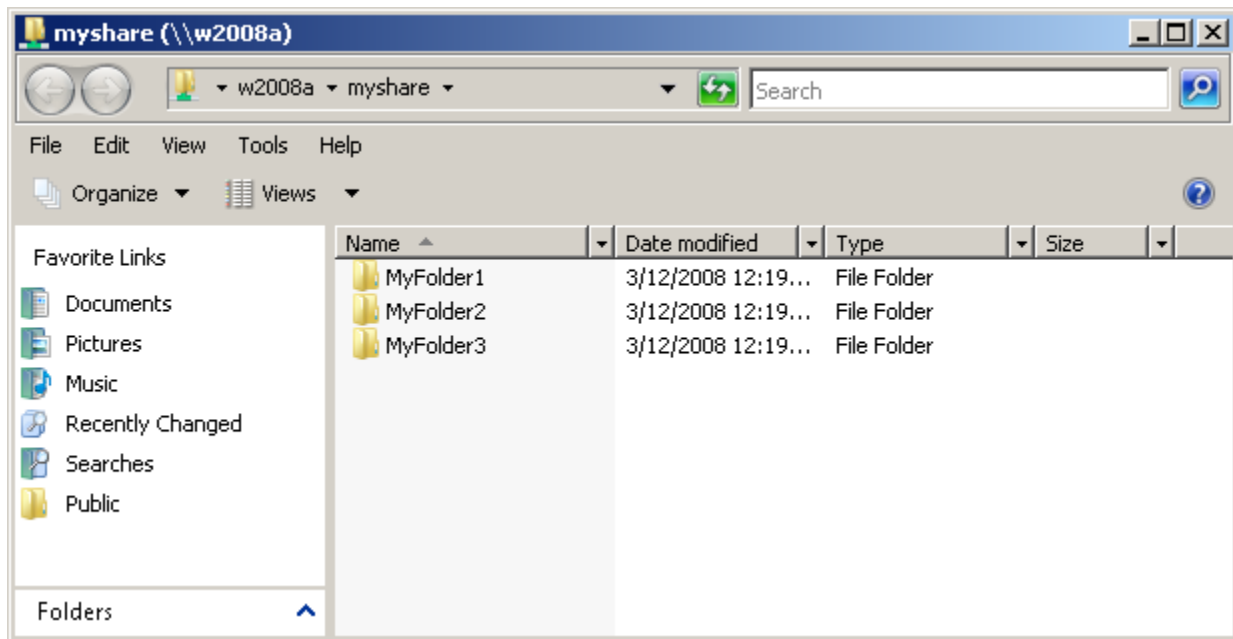
- They are typically not installed with large numbers of third-party applications other than the somewhat-common antivirus and backup software.
- The process of serving file shares is an inherent part of the Windows OS and does not require a large number of add-on components.
- File servers—though highly critical to business operations—are not highly complex.
- The files stored on file servers are often fully segregated from the OS. Thus, the wholesale OS replacement is easy because it has virtually no impact on data files.

Because of each of these, the risk associated with migrating file servers to Server 2008 is low. Cutting your teeth with these servers as a first penetration of Server 2008 into your environment will give you the skills and experience you need for future upgrades.

In this chapter, we'll be talking about the role of the file server in IT organizations and how Server 2008 enhances file sharing through a greater formalization of its role. We'll look at each of the Role Services that comes with the new File Services Role and how each augments traditional file serving. We'll talk about the new wizards that enhance the process of provisioning new shares and volumes, and conclude with a look at the new tools available to administer this "hard drive over the network."

## The Role of the File Server

Even in today's world of SharePoint portals and content management systems, the venerable file share remains a popular tool in many IT organizations for supplying access to file-based data. The reasons for this are as much historical as they are interface-driven. Back even before Windows NT, file shares have in one manner or another been a long-held mechanism for users to access their data. File shares are easy to locate, easy for inexperienced users to navigate, and are good tools when secured properly to present file-based data to users. Because of their historical advantage and easy setup as a native part of the Windows OS, file shares today still enjoy a widespread representation.




**Figure 4.1:** File shares have been around for longer than virtually every other form of file sharing tool. Thus, they are well recognized within the user community.

What is unique about file sharing in Server 2008 is in the codification of this historically subjective service. With Server 2003 and earlier versions, the process to create a file server involved little more than creating a file share on that server and declaring to users that the server now operated as one. With virtually all Windows servers using some form of file shares, in many cases for IT uses alone, this subjective identification of servers as “file servers” was the cause for some confusion within business organizations.

In Server 2008, the role of file serving has been changed to make the process a bit more formal. The File Services Role is now a formalized Server 2008 Role that exists whenever a share is used for the purposes of housing files. This formalization of the File Services Role provides administrators with a better “line in the sand” to identify which servers are responsible for this functionality.

Also changed with Server 2008 is the aggregation of many of the other technologies commonly associated with file serving in previous editions but not directly tied to their management. With Server 2008, these other components such as the Distributed File System, the File Server Resource Manager, and Services for Network File System have been combined into a single interface within Server Manager for easier administration.

 As an example, if you've ever had to search to find and install *Services for UNIX* in previous OSs, you'll be excited to know that this as well as other components are now easily installed and managed through the Server Manager interface.

But before we get into our discussion of these new features, let's talk a bit about how Server 2008 makes a few changes to the process of sharing folders.

## Basic and Advanced Folder Sharing

Even before you get to installing the File Services Role, you'll notice some changes have been made to the process of sharing folders in Server 2008. By right-clicking a folder and selecting Share, the File Sharing wizard appears. This wizard looks similar to the image in Figure 4.2. What you'll immediately notice is that this wizard is somewhat less complex and includes much less functionality than its equivalent in Server 2003 and earlier.

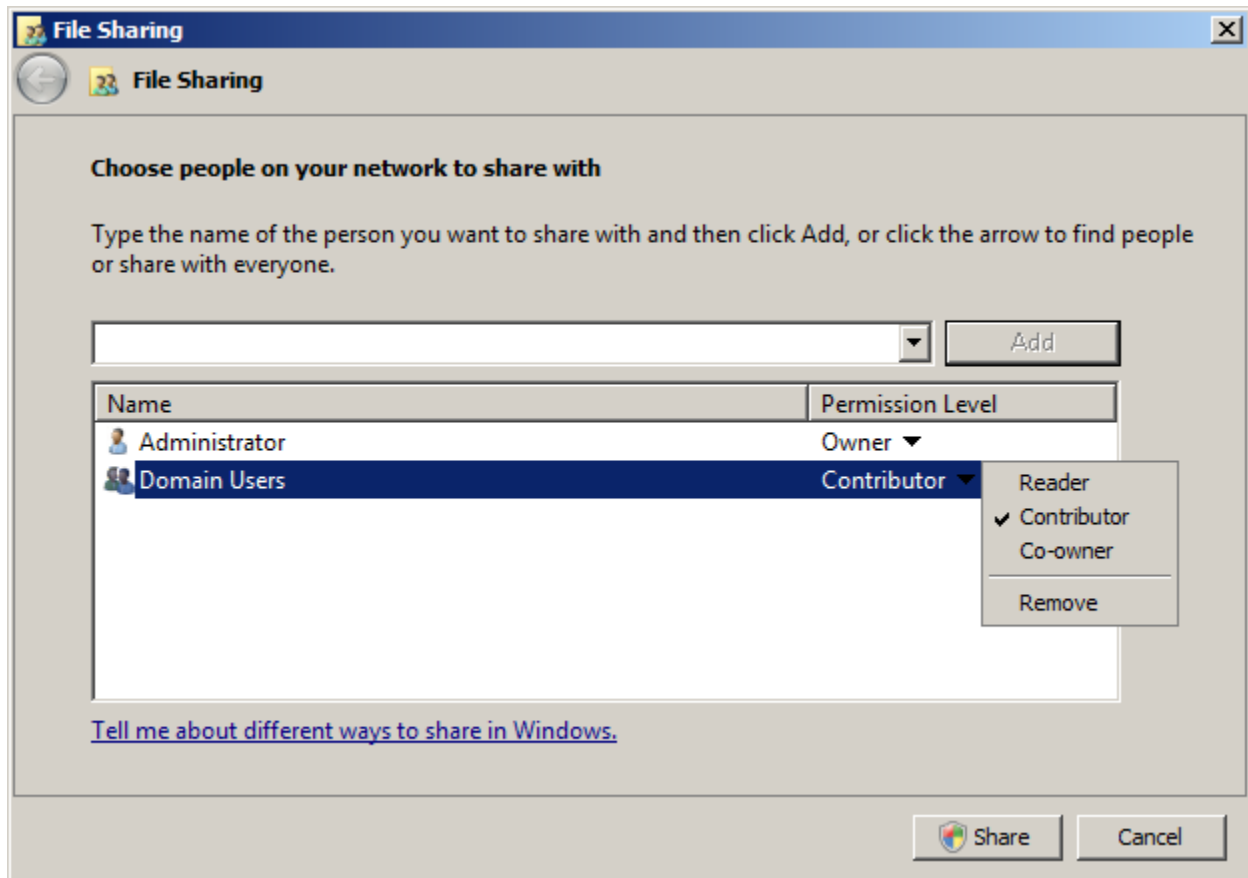


Figure 4.2: Server 2008's "simple" File Sharing wizard.

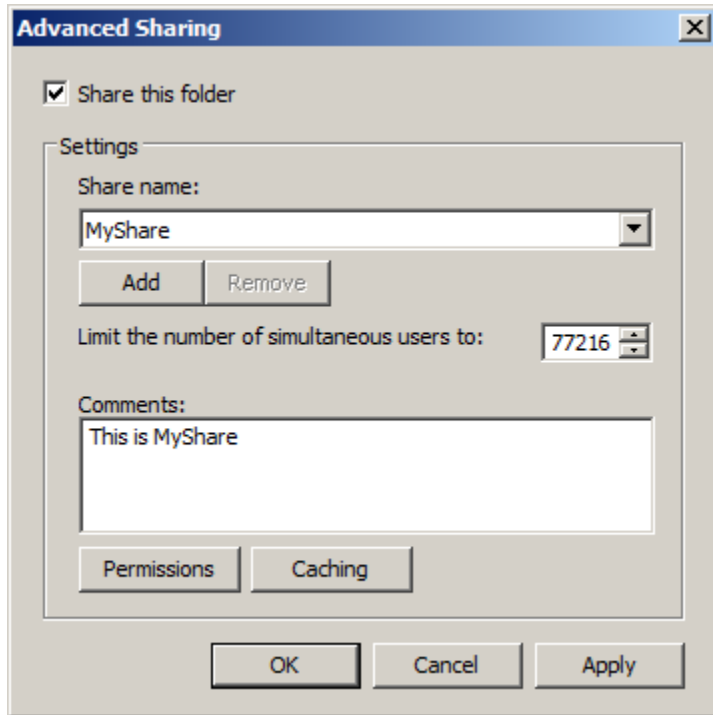
With Server 2008, Microsoft has made an effort to separate what we used to think of as “traditional” share configuration into two different management interfaces. This is similar to how file sharing was first separated at the client level with Windows XP. The first tool, what we see in Figure 4.2, is the “simple” sharing wizard. Here, Microsoft has simplified the process of sharing files. Whereas our standard options for setting permissions on shares was formerly relatively complex, here only three options are available for sharing: Reader, Contributor, and Co-owner:

- Reader—This permission restricts the user or group to viewing files in the folder.
- Contributor—This permission enables the user or group to view and add files to the folder. It also allows them to modify or delete the files that they previously created.
- Co-owner—This permission allows the user or group to view, modify, and delete any files in the shared folder.

Click Share after selecting the users and groups and their appropriate level of sharing. The resulting screen will provide a link to the newly created share that can be either copied to the clipboard or emailed to users as a way of notifying them that the share has been created.


In many cases, this simplistic level of permissioning will be sufficient. However, file shares and their use have advanced to the point in many organizations where greater granularity is needed. Administrators in these environments require greater options for locking down and otherwise restricting the use of shares. When more advanced needs are required, it is possible to bring back the Advanced Sharing wizard.

To do so, right-click the folder and choose Permissions. There, select the Sharing tab and then click Advanced Sharing. This brings forward the screen shown in Figure 4.3. You’ll see that this wizard provides quite a bit more configuration granularity than the simple sharing wizard. It is possible through this wizard to set the maximum number of simultaneous users, provide comments associated with the share, adjust how this folder is handled by users when they synchronize offline folders, and set share permissions using the traditional permissions wizard.



**Figure 4.3:** The Advanced Sharing wizard provides more granular setting of share permissions and settings.

If you prefer the Advanced Sharing wizard over what you get with simple sharing, you can change the default behavior. To do so, you'll have to dig quite a bit within the interface. So much so, in fact, that one presumes Microsoft anticipates administrators will prefer using the basic wizard. To change the default, click Tools | Folder Options and navigate to the View tab. There, scroll the list of Advanced Settings and clear the setting check box named Use Sharing Wizard (Recommended). Click OK to complete the setting.

 Why would Microsoft simplify share permissions? Likely because of the propensity for inexperienced administrators to apply too much permissioning. Remember that share permissions work in combination with NTFS permissions on files and folders. Thus, simplicity is best. When share and NTFS permissions are overused, this adds excessive complexity to later troubleshooting. By simplifying the share wizard, one presumes Microsoft is attempting to help reduce this complexity.



## Installing the File Services Role

With all the disparate shares across a Windows server, in previous editions, it was sometimes difficult to locate and manage each individual share and its settings. To assist with this problem, Microsoft incorporated into the File Services Role a number of new features. Among other things, those features consolidate shares and share configurations into a single manageable location. To enable this, you must first install the File Services Role.

As with all Roles in Server 2008, installing the File Services Role is done via Server Manager. To begin the process, right-click the Roles node and click Add Roles. When prompted, select the File Services Role in the interface and click Next. The File Services Role is equipped with 10 additional Role Services that augment its functionality. Those services as seen in Server Manager are displayed in Figure 4.4 and will be discussed in detail in the next section.

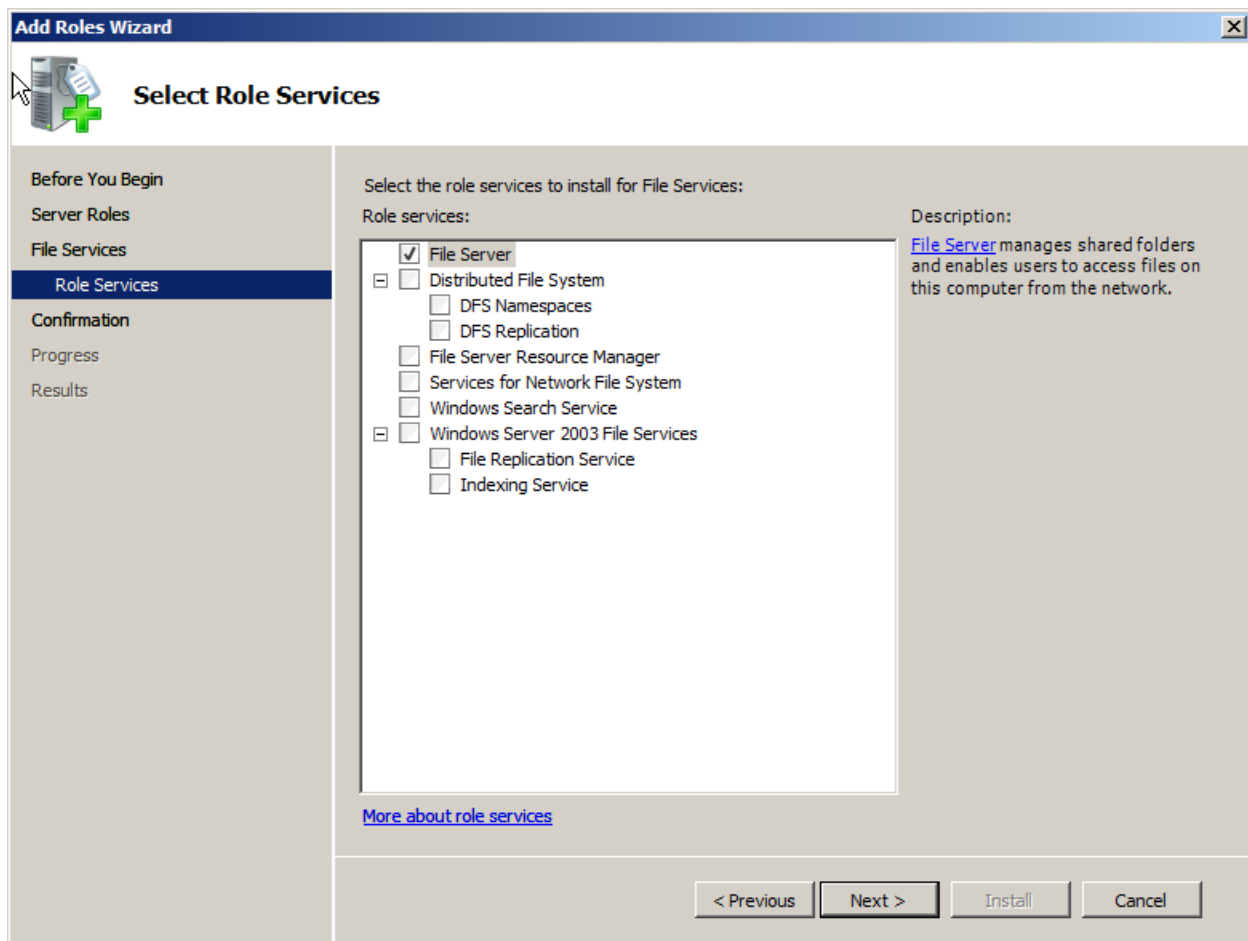


Figure 4.4: A listing of the Role Services that augment the File Services Role.

At this point, choosing only the default File Server Role Service will enable the basic functionality you're used to seeing with shares in previous OSs. What's interesting about the installation of this role is that it is one of the few roles that does not require this formalized process to be completed in order to recognize its functionality. Sharing the first folder on a Server 2008 installation will also automatically install the role. Thus, this installation is much different than others done through Server Manager.

## Share & Storage Management

Once the role has been installed completely, a new node in Server Manager called File Services with a sub-node titled Share and Storage Management will be enabled. This new console is shown in Figure 4.5. The Share and Storage Management console provides a single location where all shares and volumes on the server can be managed. Right-clicking any of the shares available in the interface allows you to quickly Stop Sharing as well as modify advanced Properties.

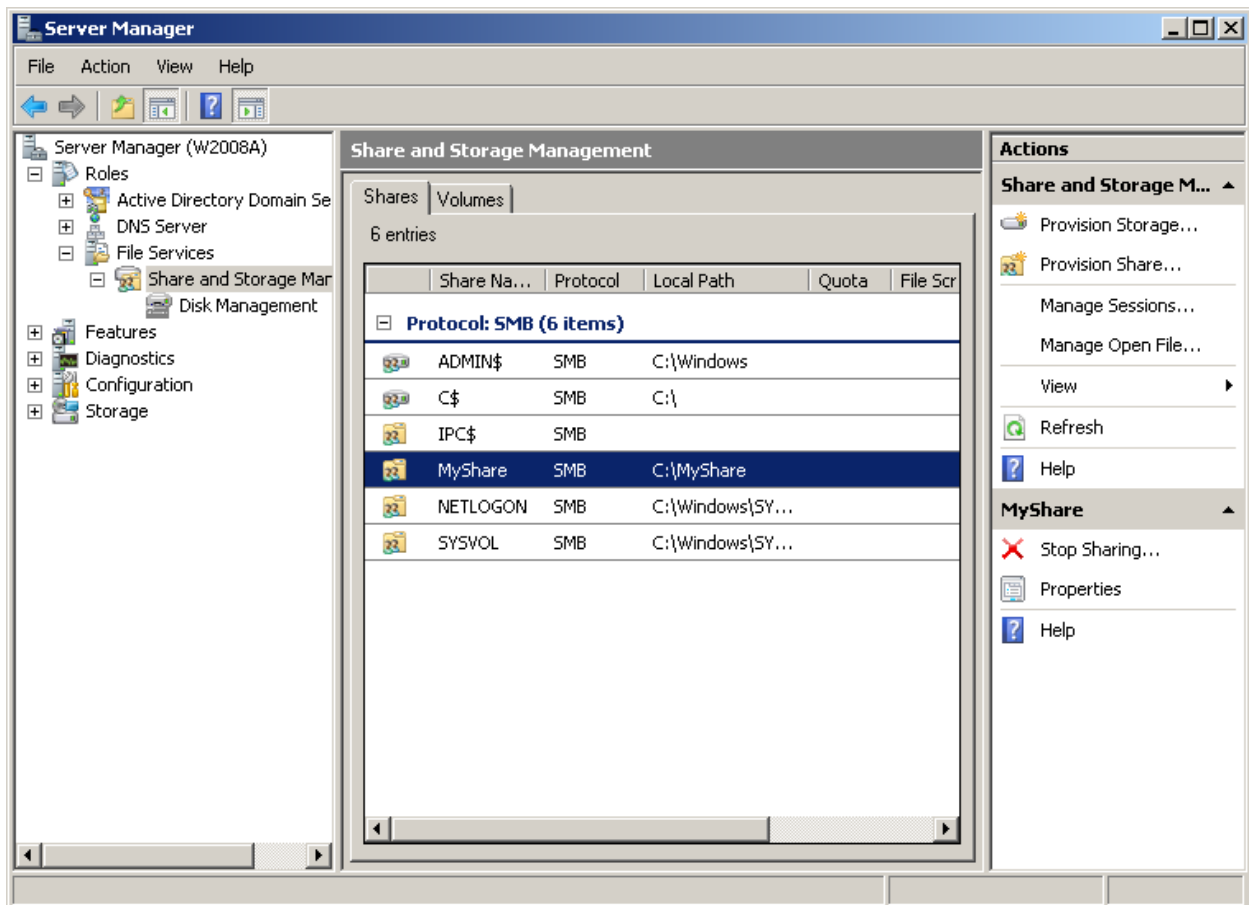
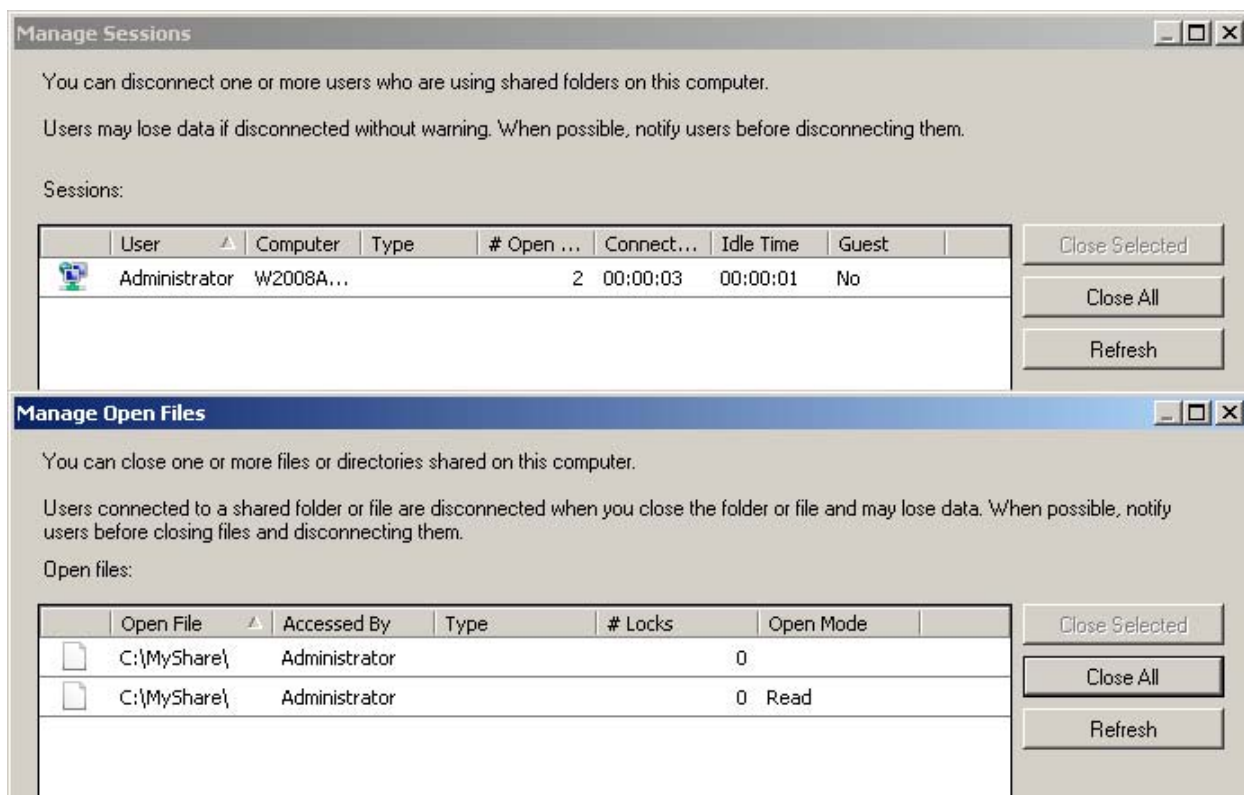


Figure 4.5: The Share and Storage Management wizard.

Of particular interest in this console are four new screens that handle the management of shares, volumes, sessions, and open files:

- **Provision a Shared Folder Wizard**—Unlike the basic and advanced tools discussed in the previous section for sharing folders, the Provision a Shared Folder Wizard aggregates all of the potential configurations for sharing folders into a single interface. With this wizard, it is possible to create a new share; provision storage for that share; set share and NTFS permissions for the share; enable the SMB and NFS protocols; set user limits, offline caching, and access-based enumeration; and publish the share to a Distributed File System namespace. All of these configurations are done as part of the wizard, which helps eliminate the “missed steps” that were often overlooked in previous OS versions.
- **Provision Storage Wizard**—The Provision Storage Wizard can only be used when disks are available on the system that are online and have unallocated space. When no disks exist that meet these criteria, an error message appears in place of the wizard. Clicking the Provision Storage Wizard enables the creation of new disk space and the configuration of its size, drive letter or mount, format options, and allocation size. As with the Provision a Shared Folder Wizard, this tool unifies the previously separated tools found in Disk Management in Server 2003.
- **Manage Sessions**—From time to time there is a need to stop idle users’ open sessions with their connected file server. This may be to free a file or perform some work on the server that requires users to be disconnected. In Server 2003, the tool to locate and close active sessions on a file share was buried in the Computer Management interface under System Tools | Shared Folders | Sessions. In Server 2008, it is prominently displayed in the actions page. Figure 4.6 shows an example of this wizard alongside the Manage Open Files tool.
- **Manage Open Files**—Similar to the Manage Sessions Wizard but focused on files rather than users, the Manage Open Files tool provides a single location where all files across all file shares can be closed. This is often done when a user accidentally leaves a file in an open state and another user wants to make use of the file. When that occurs, closing the open file enables the second user to begin working with the file. This was also found in Computer Management within Server 2003 under Tools | Shared Folders | Open Files but is now available natively within Server 2008 in the actions pane.




**Figure 4.6:** The *Manage Sessions* and *Manage Open Files* wizards showing the result of the Administrator user opening a connection to a shared folder.

### Access-Based Enumeration

Much of the use of the wizards within Share and Storage Management is relatively self-explanatory, with the single exception of Access-based Enumeration (ABE). A feature that was first incorporated into Windows with the release of Windows Server 2003 R2, ABE is a feature that enables administrators to hide files and folders for users who do not have permissions to view them. ABE is not new to file shares, having been first used in Novell-based systems many years ago. However, it is relatively new to the users of Window-based file shares.

When ABE is enabled for a particular share, the files and folders on that share are reconfigured such that they are not visible to users who do not have Read permissions. Although ABE is configured on a per-share basis, the results of ABE are seen by users on a per-file and per-folder basis. Files and folders that users have Read rights to are visible within the share, while those that don't are not visible.

The incorporation of ABE can be either a help or a hindrance for users if they are not properly prepared for the ABE incorporation into file shares. Although enabling ABE outwardly helps to improve security on file shares by eliminating the visibility into files and folders that users don't have access to, it can also be a challenge when users are attempting to find files and folders for which they need access but don't have it.

 Be careful with the use of ABE. Although it can seem like a good idea to prevent nosy users from "snooping" around in locations to which they don't have access, ABE makes it difficult for legitimate users to find files and folders that they may need to request legitimate access.

## File Services Role Services

In addition to the regular functioning and management of file shares and volumes, the File Services Role includes a set of nine optional Role Services that augment its functionality. These additional Role Services are used to ease the process of provisioning shares to users, monitoring their use and misuse, and enabling support for other shares to and from other OSs. In this section, we'll take a look at each of these Role Services in turn.

### ***Distributed File System – Namespaces***


The Distributed File System – Namespaces (DFS-N) is a tool that is used with Server 2008 to aggregate shared folders across multiple servers into a single location. This location is called a namespace and presents the appearance to the user of a single location from which all shares can be accessed. Using DFS-N, users in multiple locations can connect to servers in multiple locations, all through what appears to be a single file share.

Why is this useful? Think for a minute about the shares in a typical Windows network. There may be many, if not dozens or hundreds, of file servers within the network. Those file servers each may contain multiple file shares. They may be located in different places on the network, and each location may have different network connectivity to the client. DFS-N provides a mechanism whereby the file shares across all these servers can be aggregated into a single “share” that includes pointers to the individual locations.

Traditionally, when users needed to access file shares, IT made those shares available through the use of drive letter mappings. But the use of drive mappings can grow unwieldy when the number of file shares grows large. Adding to the complexity can be the dynamic nature of the file shares themselves. With a direct drive mapping at the client, when changes to shares are necessary, a similar change to drive mappings are required to all clients. Depending on the process in which drive mappings are made to clients, this can be a complicated process. With DFS-N, the process to change a share's representation happens in one place for all users. DFS-N effectively adds a “layer of abstraction” between the client's drive mapping and the file shares they intend to use.

DFS-N installation is done through Server Manager by adding the Distributed File System and DFS Namespaces Role Services to the File Services Role. Upon installing the Role Service, you will be asked if you want to create a namespace immediately or later using the DFS-N management snap-in. Once the Role Service is installed, a new node called DFS Management will appear in Server Manager under File Services. Two sub-nodes are also available, one for Namespaces and another for Replication. In this section, we'll be using the Namespaces sub-node.

Two types of namespace exist. Standalone namespaces are designed for smaller uses of less than 5000 DFS folders or for environments that do not have AD in-place. Standalone namespaces also support clustering using Windows Server Failover Clustering. The second type, domain-based namespaces, are used when an AD is in place and administrators want the ability to publish the namespace to AD. The process of publishing the namespace to AD further abstracts this layer from users and their files and folders.

 Publishing the namespace to AD allows users to access the namespace by knowing only their AD domain name and the namespace name. So, for example, with a domain name of realtime-windowsserver.com and a namespace name of MyNamespace, users would access the namespace by using \\realtime-windowsserver.com\mynamespace.

As an example, let's create a new domain-based namespace in the realtime-windowsserver.com domain. To do so, right-click the Namespaces node and select New Namespace. In the resulting screen, supply the name of the server that will host the namespace. In this case, that server will be the server w2008a. In the following screen, provide a name for the namespace. In this example, we will use the name MyNamespace. A button appears at the bottom of this screen that allows for the configuration of the local namespace path as well as shared folder permissions. The default permission here is to provide all users with read-only access.

The next screen resembles Figure 4.7 and provides the option to select the type of namespace. The domain being used is at the Windows Server 2008 domain functional level, so Windows Server 2008 mode is available as an option. The Windows Server 2008 domain functional level enables support for ABE within the namespace as well as increases the total number of folders the namespace can support. You'll also see that creating a domain-based namespace enables users to connect using the domain name rather than a specific server name. Clicking Create at the final screen creates the namespace.

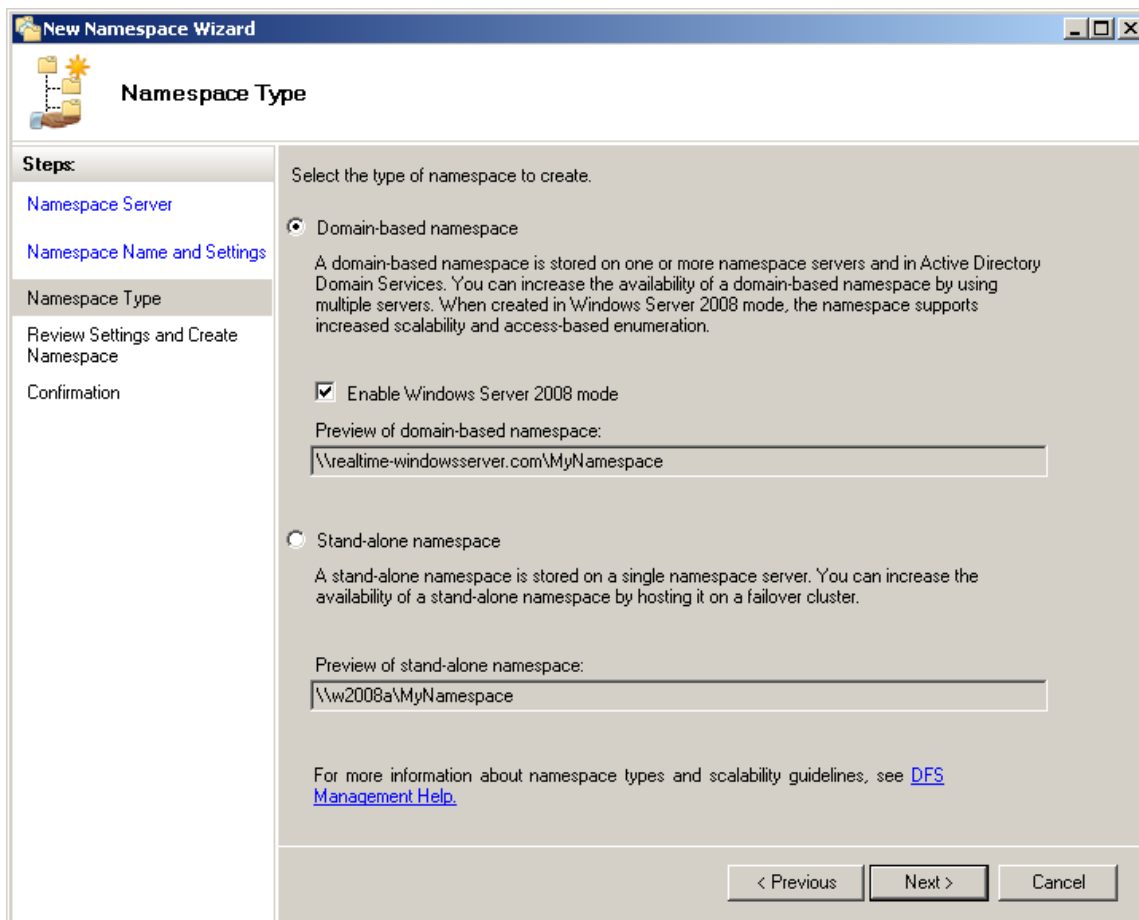




Figure 4.7: Creating a domain-based namespace with the New Namespace Wizard.

Once the namespace is created, you can add folder targets by right-clicking the namespace and selecting New Folder. In the resulting screen, provide a friendly name and path to the folder target to add the target into the namespace. Additional advanced configurations can be made by right-clicking the namespace and selecting Properties.

 There are some server edition requirements to support DFS-N. Server 2003 and Server 2008 Standard Edition as well as Server 2003 Web Edition can support the hosting of only a single namespace. Server 2003 and Server 2008 Enterprise and Datacenter Editions can support the hosting of multiple namespaces.

### **Distributed File System – Replication**

Whereas DFS-N is used for aggregating file shares into a single interface, the Distributed File System – Replication (DFS-R) encompasses another entirely different capability. DFS-R enables Server 2008 to multi-directionally replicate files and folders among multiple servers. DFS-R can be considered the “upgrade” from Server 2003’s File Replication Service (FRS). DFS-R is substantially improved from FRS, making possible its use for more than AD’s relatively light SYSVOL replication requirements. DFS-R can be used to support replication of file-based data between multiple servers and across multiple network sites. It can be set up as a solution for replicating this data between two or more servers in a multi-master configuration. Alternatively, it can be used as a tool for aggregating data from remote site servers to a local file share for centralized backup. In this secondary configuration, bi-directional replication is established between two servers, though most of the replication will occur from the remote site to the local site. Once replication is established, backup software at the local site can then be used to back up the remote site’s replicated data at the local site.

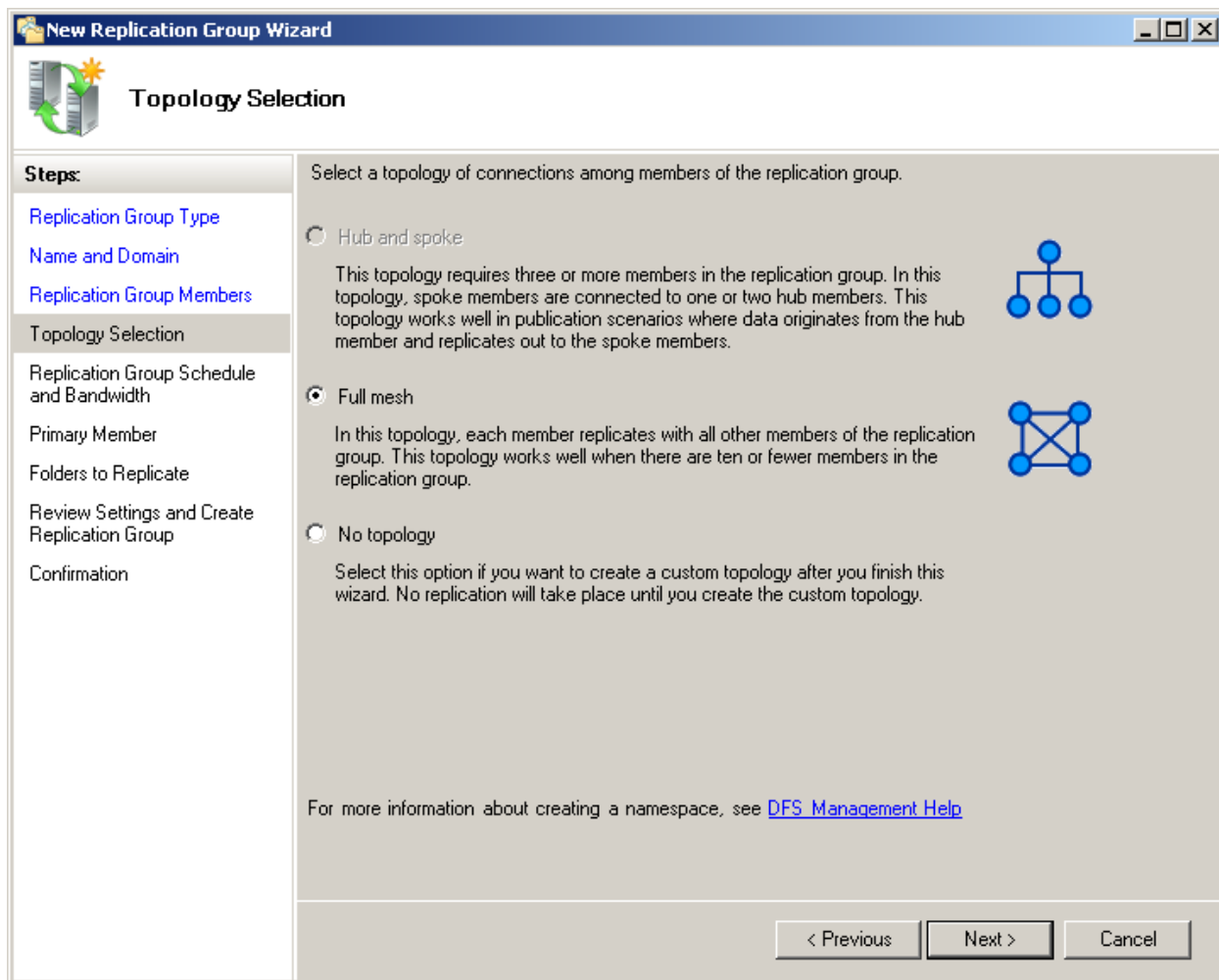
 As a side note, one feature gained when an AD is upgraded to the Windows Server 2008 domain functional level is the use of DFS-R as the service to replicate SYSVOL.

Installing DFS-R involves no initial configuration as part of the installation. To install the Role Service, right-click the File Services node and select Add Role Services. Click through the resulting status screens to complete the installation. Once installed, the process to set up replication between two hosts involves a number of steps.

 The DFS-R Role Service must be installed individually to each replication member.

First, right-click the Replication sub-node under DFS Management, and select New Replication Group. In the resulting screen, you’ll be given the option to select a *Multipurpose replication group* or a *Replication group for data collection*. Here, choose the first option to set up multi-master replication. Provide the replication group a name, an optional description, and a domain in the next screen, and in the screen following, enter the group members.

The next screen, shown in Figure 4.8, allows for the establishment of the group’s topology. As you can see in the figure, three topologies are available: hub and spoke, full mesh, and no topology. The hub and spoke topology is primarily used when replication data is mostly unidirectional with the hub being the source of most changes. The full mesh is used when equal levels of change are expected among members. The no topology option allows you to later determine the topology after the group is created.



**Figure 4.8: Selecting a DFS-R topology.**


The next screen configures the bandwidth or schedule for replication. For continuous replication, you can select a bandwidth throttle in Kbps or Mbps. For scheduled replication, a schedule editor is provided. Bandwidth can similarly be throttled in the schedule editor if desired.

Next is the selection of the Primary Member. This selection determines which member's data is considered authoritative at the time of first replication and is a critical consideration when data exists to be replicated on multiple machines. Lastly is the selection of folders to be replicated. Click Add to select folders to be replicated. Here also is the ability to select how the folders are displayed and any repermissioning to be done.

Before establishing the replication, the wizard presents a screen called Local Path of {Folder Name} on Other Members. Here you can select whether you want to enable the replicated folder to be available on remote servers. This is required if you want users to make use of the replicated folder on those remote systems.

Once created, the servers will begin replicating once they have been informed of the update through standard AD replication. Additional members or replicated folders among members can be added by right-clicking the replication group and selecting New Member or New Replicated Folders. A new topology can additionally be designed as necessary by selecting New Topology.




 DFS-R is good for use as a replication tool when the same data is not being changed at the same time in multiple places. This would be the case when one user attempts to modify a file in one location while at the same time another user attempts to modify the same document in another location. When this behavior occurs within the environment, DFS-R can be problematic due to replication conflicts between the changed documents. In this case, another tool such as Microsoft Office SharePoint Server with its ability to check-in and check-out documents may be a better solution.

One element to pay close attention to is called Create Diagnostic Report. When replication begins to experience problems, this report creation utility can assist with quickly finding the result of the problem. Three types of reports are available:

- Health reports detail the health and efficiency of the replication connection
- Propagation tests verify replication by creating a test file in a replicated folder
- Propagation reports detail the replication of a test file through a replication test

### ***File Server Resource Manager***

A management tool that first appeared with Server 2003 R2 and is natively available in Server 2008 is the File Server Resource Manager (FSRM). This tool enables administrators to monitor the use of files and folders within their environment. That monitoring can provide periodic storage reports to identify usage trends as well as create and manage template-based user quotas across multiple file shares. It can also enforce the use of file type screening that prevents users from storing inappropriate (and wasteful) files on file servers.

 If you're tired of user MP3 files hogging your storage space, you can use FSRM to screen out these files from being saved to high-dollar enterprise storage.

Installing the FSRM Role Service to a server involves the same process as has been used for each of the other Role Services we've discussed to this point. When installing FSRM, you will be asked to optionally identify the disks to be monitored for Storage Use Monitoring. These disks can be selected during the installation or later after the installation is complete. Once installed, FSRM is administered under the Share and Storage Management node of the File Services Role.

FSRM's capabilities are broken down into three areas: quota management, file screening management, and storage reports management. We'll discuss each of these in the following sections.

## Quota Management

Quotas are designed to be template-based policies that govern users' capacity to store files and folders within a particular file share or server. These templates allow users to store a certain level of megabyte or gigabyte of space on a file share or server while at the same time providing reports and/or alerts to users when they go beyond their allowable limit. Figure 4.9 shows an example of a template that gives users a 200MB hard limit with user notifications at 85%, 95%, and 100% of that limit. Setting a hard limit means that users will be prevented from exceeding that limit. Soft limits are used for monitoring user's use of space and will not prevent users from going beyond their stated limit.

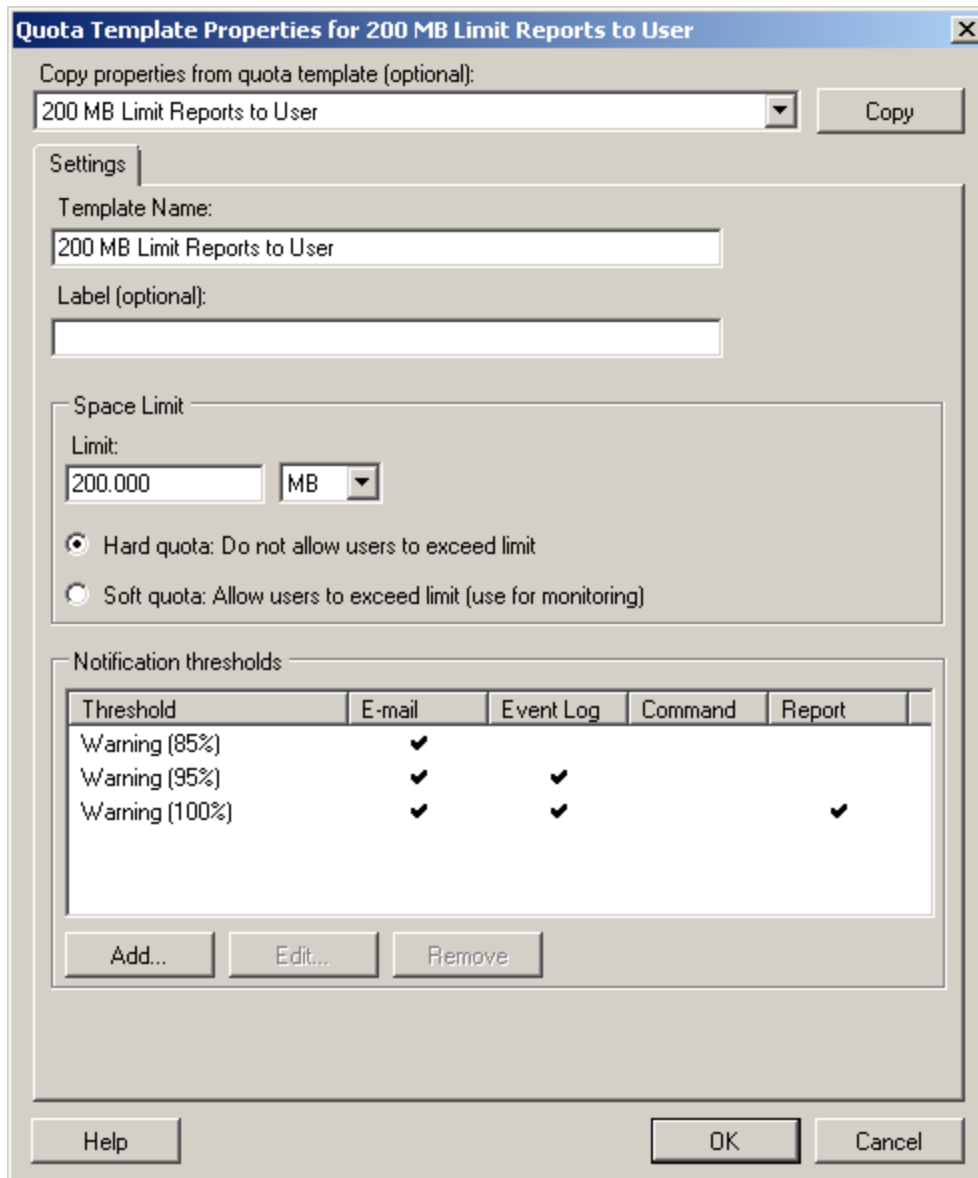



Figure 4.9: An FSRM quota template limiting users to 200MB of space.

By clicking any of the notification thresholds and selecting Edit, you will be shown the type of warning (email, event log, command, or report) and specifics for configuration of each. Email and report notifications require an SMTP server to be configured to accept the email traffic.

 The concept with these notifications is to provide a visual indication to users when they are approaching and reach their maximum level of space on file servers. The idea is to encourage users to limit the amount of data they store on file servers and “clean up” their work when necessary so that you don’t have to.

Once a template is created that includes the size limits, actions, and notifications of value, the next step is to create a quota based on that template. This can be done by right-clicking the template and choosing Create Quota from Template. In the resulting screen, you’ll be asked to identify the root path for the quota template to be assigned. The template can be extended to support all subfolders of that path to ensure full compliance with the template.

## File Screening Management

File screens can also help in preventing or deterring users from storing inappropriate file types onto file servers. The difference between file screens and quotas has to do with the types of files prevented from storage as opposed to the quantity. File screening management is broken into three separate elements that work together in creating a policy:

- **File groups**—File groups are categories of files and associated extensions that relate to that category. For example, the file group Audio and Video Files includes 37 file extensions such as .MP3 and .AVI for restricting audio/video files. New groups can be created and extensions added and removed from existing groups tailored to the needs of the environment.
- **File screen templates**—Once a file group is assigned, it can be incorporated into a file screen template to enable the actions shown to the user when they attempt to store a configured file type. Similar to quotas, file screen templates can make use of email, event log, command, and report notifications to alert users when they have attempted to store a configured file type. File screen templates can be set to actively block the file type from storage or merely record its storage for monitoring purposes.
- **File screens**—This element brings together the settings from the other two and applies them to a location on a server. Figure 4.10 shows an example of how a Block Audio and Video Files template, which leverages the Audio and Video Files group, is being set for the C:\MyShare folder.

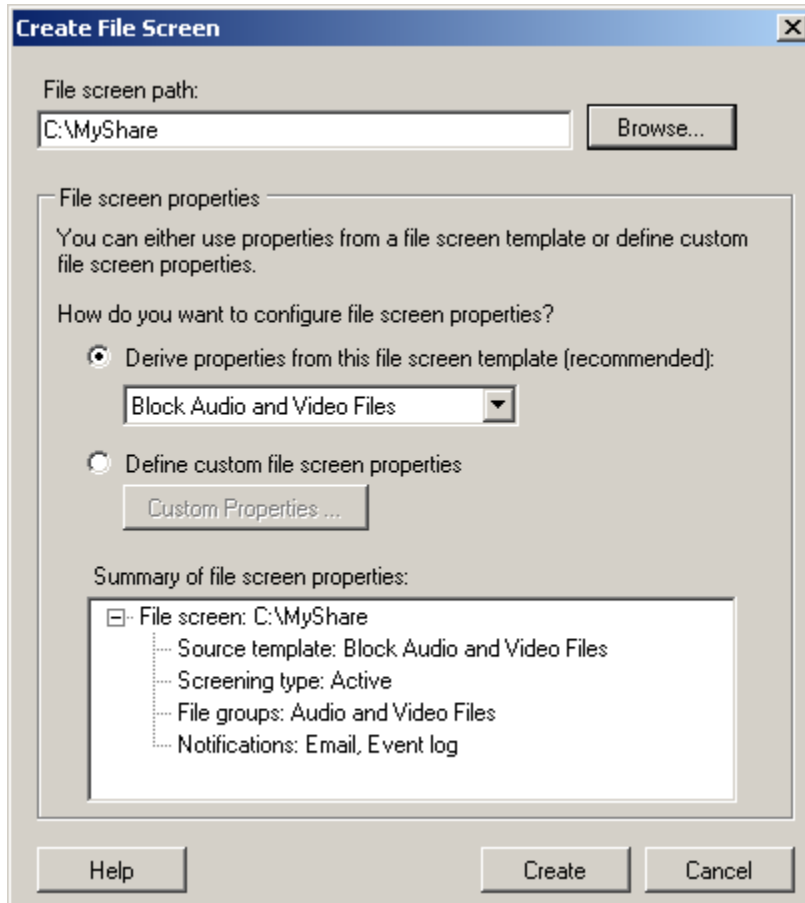


Figure 4.10: A file screen that prevents the storage of Audio and Video files.

## Storage Reports Management

Storage reports management schedules and views reports based on the use of storage in a particular volume or folder. Eight reports are available, and each can be customized to a minimal extent. Depending on the needs of the administrator, reports can be run on-demand or scheduled to occur at other times. Also, depending on the size of the folder or volume being reported against, creating a report can take an extended period of time. Thus, scheduling reports to occur at regular intervals will prevent waiting for the report to complete. Preparing scheduled reports also helps with identifying trends in storage use. Reports can be optionally delivered to an email account when run or viewed within the interface. Figure 4.11 shows an example Storage Reports Task and the storage reports to be generated as part of the task.

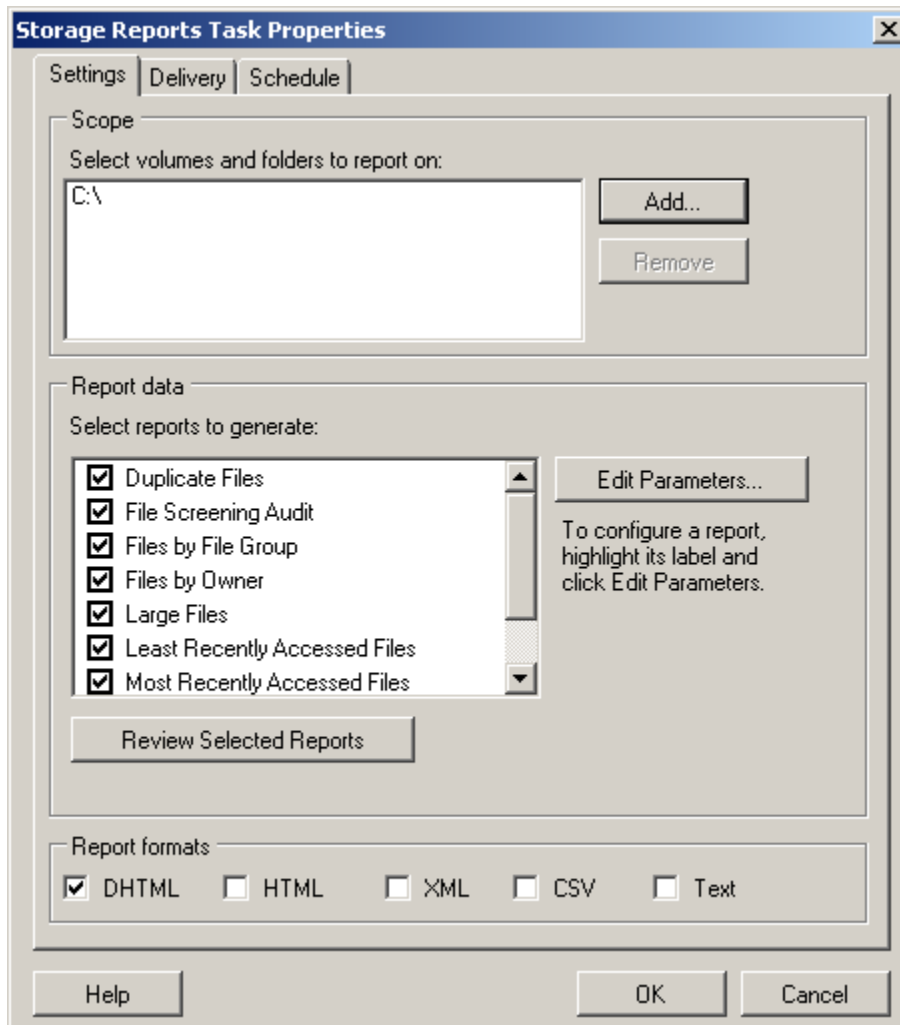


Figure 4.11: A Storage Report Task that analyzes usage on C.

### Services for Network File System

In heterogeneous environments, it is often necessary for UNIX- and Linux-based machines to connect with and exchange files with Windows-based machines. Because UNIX/Linux uses a different file system than does Windows, the conversion required in making this connection necessitates that software exist on one end or the other that supports the transfer.

Server 2008 includes as part of the File Services Role a Role Service called Services for Network File System (NFS). This Role Service enables Server 2008 to either connect to an NFS mount on a UNIX/Linux host or host a Windows share as an NFS mount for serving to those same hosts. The process of installing the Services for NFS Role Service is similar to doing so for the other services we've discussed to this point.

Once installed, Services for NFS creates new options that are seen within the Share and Storage Management node and adds the Services for NFS option in Administrative Tools. Once installed, click the link in the Actions pane titled Edit NFS Configuration. Because UNIX/Linux and Windows often have segregated identity management tools, it is necessary to configure identity mapping between UNIX/Linux identities and Windows identities if you want to use permissions other than anonymous. Clicking Identity Mapping Wizard in the resulting screen brings forward the wizard. This wizard can configure AD as the mechanism for identity mapping.

Once mapping is set up properly, new NFS-enabled shares can be created through the Provision a Shared Folder Wizard. In the screen titled Share Protocols, enable the NFS protocol as shown in Figure 4.12 and provide a Share name. The Share path will be populated by the wizard and is the path that will be used by NFS clients for connection. Enabling the NFS protocol will create a new screen in the wizard titled NFS Permissions where client groups and host permissions can be set for the share.

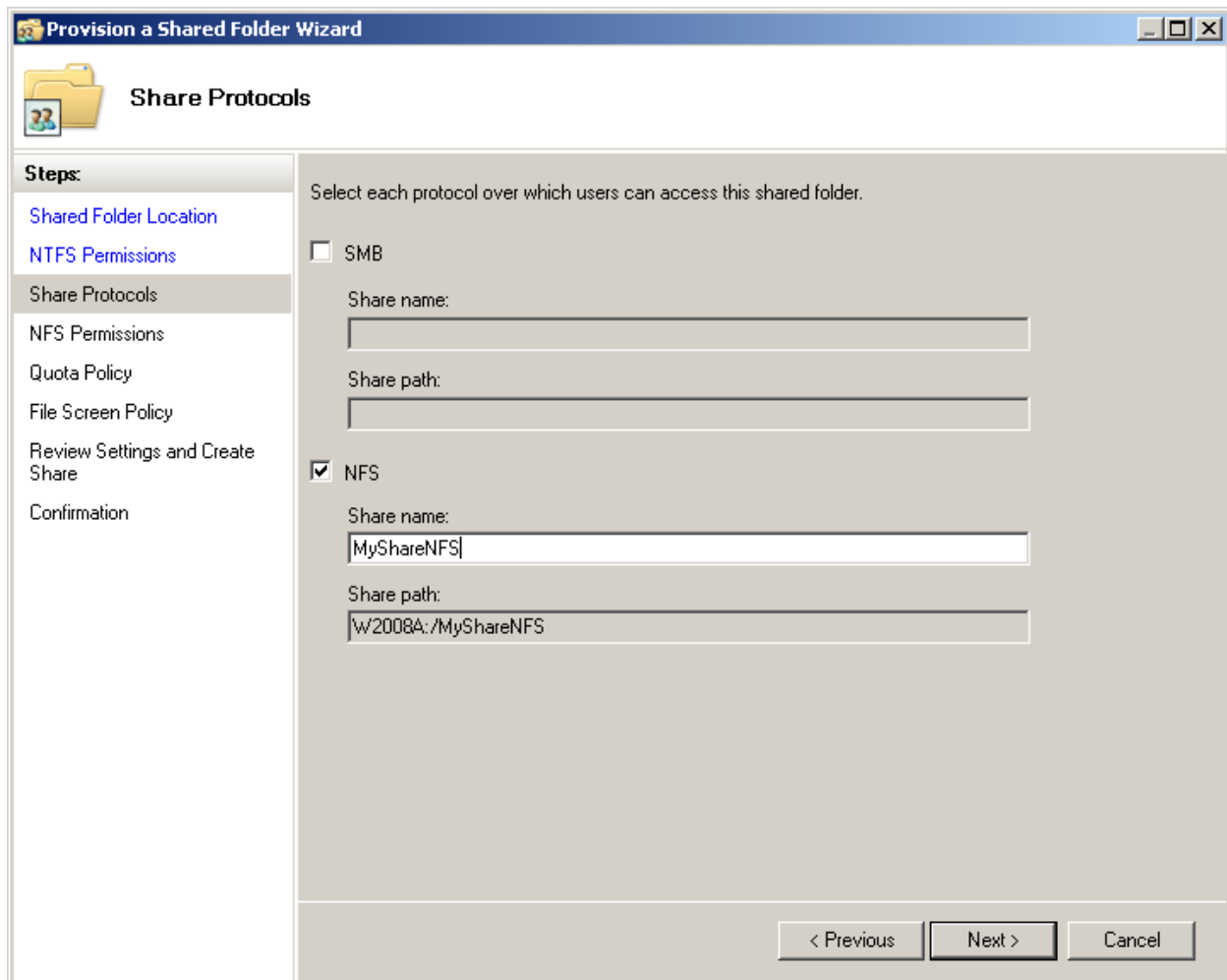


Figure 4.12: Enabling NFS on a share in the Provision a Shared Folder Wizard.

NFS handles permissions through a much different model than NTFS, allowing per-host restrictions but limiting permissions to Read-Only and Read-Write. Anonymous permissions can similarly be set on the folder by checking the box for *Allow anonymous access* and setting the NTFS permissions on the folder to grant the correct level of access to the Everyone group—though this is not recommended due to security concerns.

Also possible with Services for NFS is the ability to connect a Windows server to a UNIX/Linux NFS mount using Client for NFS and the command-line mount command. This command connects an NFS mount to a local drive letter and requires special configuration on the UNIX/Linux host for functionality.



Details about cross-OS file sharing and identity mapping are complex topics that are outside the scope of this chapter. More information about Services for NFS that includes client and server components can be found on the Microsoft Web site at <http://technet2.microsoft.com/windowsserver2008/en/library/187ea492-4d0e-41d9-a11c-05f5fea922061033.msp?mfr=true>.

### **Windows Search Service**

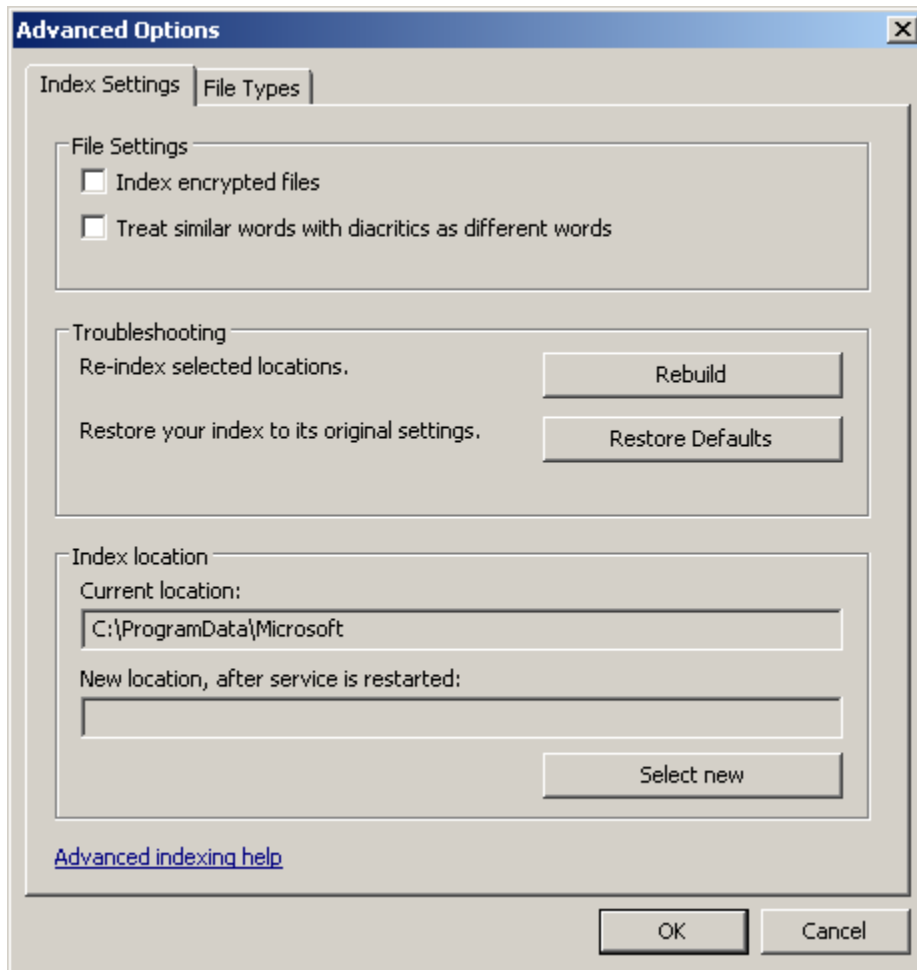
In environments with small file servers and few users, Microsoft provides the native Windows Search Service. This tool, which replaces the Indexing Service in Server 2003, speeds the process of searching for files and folders on file shares. Clients must be specifically configured to support the Windows Search Service; Windows Vista includes native support while Windows XP and Server 2003 require a separate installation of the Windows Desktop Search client. This client is a free download from the Microsoft Web site.

The process of installing the Windows Search Service Role Service is similar to that of the other services we've discussed to this point. As part of the installation, you will be asked to select the local volumes you want to index.



The indexing process can consume a noticeable amount of server processor resources.

Once installed, the configuration for the Windows Search Service is found under Control Panel | Indexing Options. There you can configure which folders should be indexed and which should be excluded from indexing. Figure 4.13 shows the result of selecting Advanced. There, it is possible to configure the indexing of encrypted files as well as change the location of the index, restore defaults, or completely rebuild the index. As you'll see, much of the indexing service—other than configuring which folders should be part of the index—occurs behind the scenes.



**Figure 4.13:** The advanced options within the Indexing Options control panel settings.

### **Windows Server 2003 File Services**

Three additional Role Services are available for legacy support of Server 2003 file services. These Role Services specifically install the predecessor to DFS-R, FRS, as well as the predecessor to the Windows Search Service, called the Indexing Service.

These two features are used in environments in which support for previous versions is needed to maintain functionality with legacy systems. In both cases, DFS-R and Windows Search Service provide performance, stability, and management benefits to their previous versions. Thus, these legacy versions should be installed only in situations in which previous version support is required.



## Properly Managing Storage Eliminates Critical Downtime

Server 2008 comes equipped with a host of new and improved features that improve the experience of hosting and managing storage on server systems. The proper management of that storage ensures the highest levels of uptime. Ensuring that storage is being used for the right business purposes, is easy to locate, can be replicated to locations both local and remote for redundancy and performance reasons, and can be quickly searched for critical data ensures that users gain access to their critical file-based data with the highest levels of efficiency. As you've seen throughout this chapter, Server 2008 provides a host of options for fulfilling each of these critical storage needs.

In our next chapter, we'll move away from what we're used to considering the "full" version of Server 2008 to what some think of as Server 2008 "lite." Server Core is a command-line version of Server 2008 that is specially designed for certain applications. Its fewer hardware requirements mean it can be installed to older equipment, which extends the lifetime of existing hardware. And its reduced attack surface makes it an excellent addition for quasi-secured environments and branch offices. The only hard part is learning how to administer it completely from the command prompt. In Chapter 5, we'll talk about Server Core with a special focus on how to do just that.

## Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.