realtimepublishers.com®

The Definitive Guide™ To

Securing Windows in the Enterprise

SCRIPTLOGIC

Don Jones

Copyright Statement

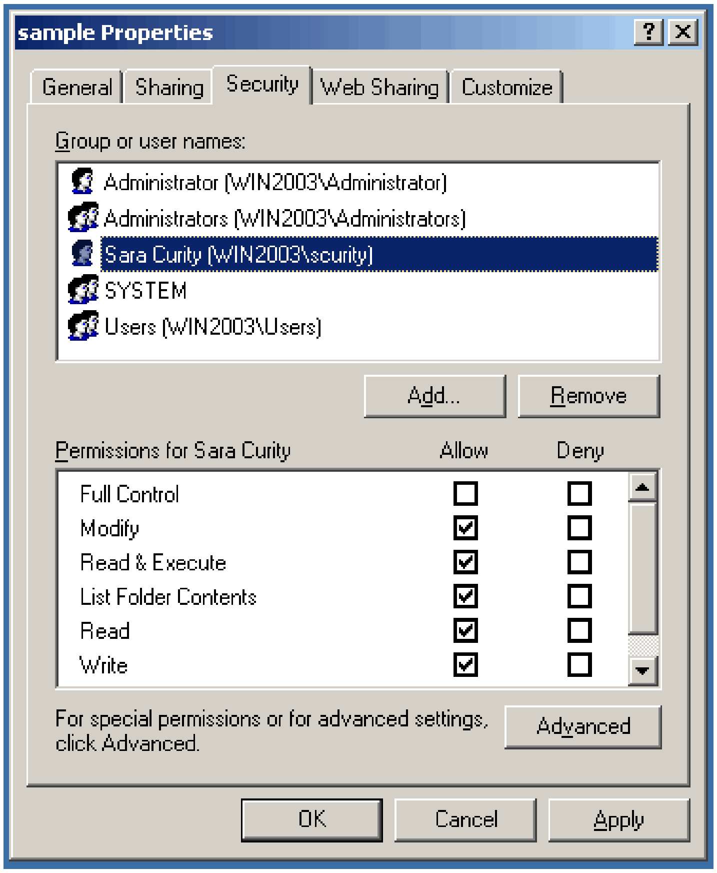
[**Editor's Note:** This eBook chapter was downloaded from Content Central. To download other chapters from this eBook, please visit http://cc.realtimepublishers.com/portal.aspx?pubid=335.]

Chapter 5: Securing File Servers

A file server is one of the most common roles for a Windows server. After all, Windows got its start in business as a departmental file server, and file services is still one of Windows' biggest strong points. Some organizations have had file servers in place for years, so it's no surprise that security on these servers isn't at the highest possible level. This chapter will explore the most common security problems with file servers, and show you ways to easily address those problems, resulting in a more secure Windows enterprise.

When Good File Servers Go Bad

As with most security issues, time is the file server's enemy. Most administrators who are setting up a new file server do so with the best of intentions, following every security best practice they know; over time, however, those best practices may be followed less rigorously, or may even change, resulting in a file server with less-than-stellar security. Figure 5.1 shows every administrator's worst nightmare (or what should be their worst nightmare): file and folder permissions assigned directly to one or more users rather than a group.



Group or user names:

- Administrator (WIN2003\Administrator)
- Administrators (WIN2003\Administrators)
- Sara Curity (WIN2003\scurity)
- SYSTEM
- Users (WIN2003\Users)

Permissions for Sara Curity	Allow	Deny
Full Control	□	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Figure 5.1: File permissions assigned to a user rather than a group.

Per-user permissions are perhaps the most common security problem on file servers. Per-user permissions are more difficult to manage than group-based security settings and become increasingly complex over time as users leave the company, move to new roles within the company, and so forth. Although the best practice is to assign permissions only to groups and to place users in the appropriate groups in order to give them permissions (other than on users' home directories, where per-user permissions are the norm), the scenario that Figure 5.1 shows is far from uncommon in most environments. Per-user permissions creep in over time as harried (and sometimes less-knowledgeable) administrators do whatever is necessary to get their jobs done as quickly as possible.

> Later in this chapter, I'll give you some tips for solving the per-user permission nightmare.

Additional security problems also exist on most file servers. For example, in most Windows environments, users can see every available file share and folder, even if they don't have access to those resources. Windows makes this poor practice difficult to avoid. File servers are often configured with less-than-ideal security settings at the network level, too, opening the environment to spoof attacks (in which users access a rogue server that they think is legitimate), poor authentication protocols, and more. In addition, file servers may not be well-configured for data resilience, which can be a security problem when critical data is lost or intentionally destroyed or altered. Even well-meaning administrators, seeking to remove old files from expensive storage resources, can create security and operational issues by inadvertently removing critical corporate data from a file server. All of these security problems are, however, easily corrected if you have access to the right techniques and technologies.

> File servers are, as their name states, *servers.* There are a lot of security issues that pertain to servers in general, rather than file servers in particular: Service configuration, password policies, and port management are just a few of these issues. Chapter 6 will address these more generic server security problems; this chapter will focus on the issues unique to file servers.

What You Can't See Won't Hurt You

If you've been working with networks for a while, you probably know that Novell NetWare—all the way back in its 2.x versions—had a useful feature that prevented users from seeing network shares to which they didn't have access. This feature was useful from a usability standpoint because users wouldn't be calling the Help desk asking why they couldn't access a particular share, when in fact they didn't have permission to do so. From a security standpoint, it was a useful feature because it helped prevent users from trying to work around security settings on items to which they didn't have access simply because the users wouldn't realize that those things were there to begin with.

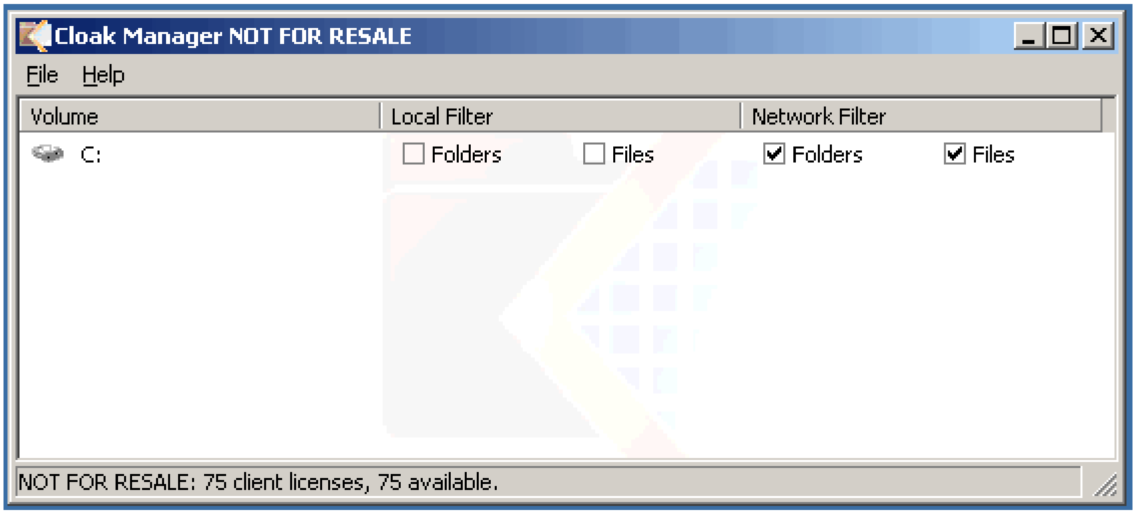
It's odd that Microsoft never implemented a similar capability in Windows, especially because Windows started out competing primarily with NetWare. Finally, WS2K3 Service Pack 1 (SP1) includes a feature called *Access-based Enumeration* (ABE). Essentially, ABE prevents the server from showing any resources to which a user doesn't have access, including shares and the folders living beneath a share. Unfortunately, ABE isn't intuitive to configure. It is turned off by default and must be turned on for each individual share. Further, there is no graphical user interface (GUI) from which to configure ABE. A free third-party utility called Sheflgs.exe (available from JoeWare.net) can be used to simplify the process. Run

```
    Sheflgs \\Server\Share /abe true /forreal
```

to enable ABE on \\Server\Share. Sadly, you still have to do this on a per-share basis, and there is no way to extend the functionality to WS2K3 machines that are not running SP1 (nor can you use ABE on Win2K servers).

My preference is to turn on ABE for every share on a server. There is very little reason not to—if a user doesn't have access to a share, there is no reason for the user to *see* it, right? Unfortunately, the fact that ABE only exists in WS2K3 SP1 and that it has to be configured on a per-share basis is certainly a bit limiting (that there is no graphical means of activating it and it isn't turned on by default is a bit bewildering).

Another option—one that includes a GUI and runs on Win2K servers—is to use a third-party tool. As Figure 5.2 shows, a third-party option is easy to operate, and can be configured on a per-volume basis to hide files and folders from either local or network users.



Volume	Local Filter		Network Filter	
C:	□ Folders	□ Files	☑ Folders	☑ Files

NOT FOR RESALE: 75 client licenses, 75 available.

Figure 5.2: Configuring ScriptLogic Cloak to hide access to files and folders.

☞ Cloak's ability to hide local files and folders means it's suitable for use on shared client computers, allowing you to hide local files and folders to which the currently logged-on user doesn't have access.

Remember, these tools aren't hiding items to which users *have* access; it's only hiding resources that the user won't be able to access anyway.

✎ Note that this approach is *very* different than simply adding a dollar sign ($) to the end of the share name. That technique hides the share from the browse list of *all* users, whether they have access or not; I dislike that technique if it's being used to hide shares from users who have access simply so that those users won't *realize* they have access. If you don't want someone accessing a share, don't give them permission to do so—don't rely on obfuscation (for example, hiding the share) to protect the share's contents. Third-party tools and ABE simply take their cue from the underlying file, folder, and share permissions, permitting users to see only what they already have rights to access.

☞ One area in which either ABE or a third-party tool can be useful is in user home directories. With ABE or another solution in use, you can map all users to a generic share, such as \\Server\Users, under which you've created individual folders for each user. With the appropriate permissions applied to each subfolder, ABE or the third-party tool will ensure that users see only their *own* subfolders and not other users' subfolders. This setup removes the need to create individual shares for each user, making network management much more convenient and efficient.

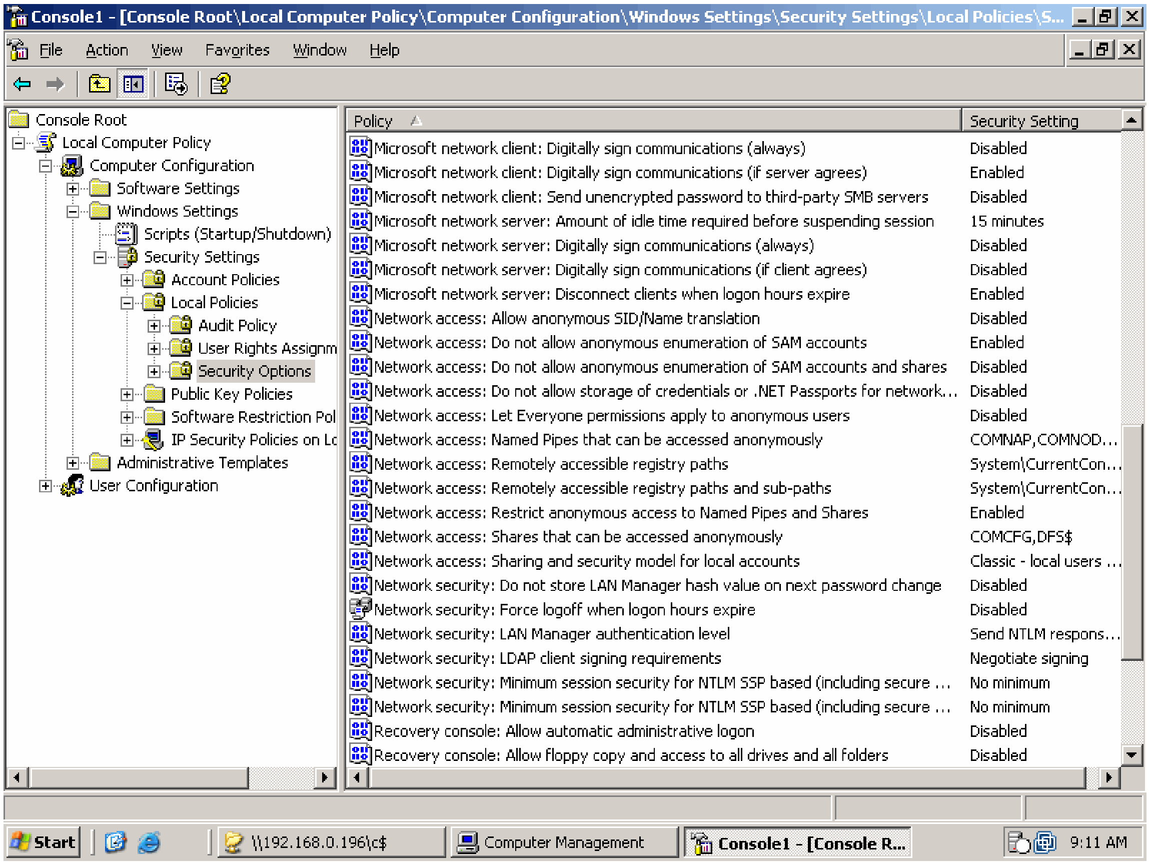
Of course, a key to all of this hide-the-share capability is having the correct file, folder, and share permissions in place to begin with—a setup that we'll explore toward the end of this chapter.

At the Network Level

File servers—especially those that have been in the environment for a while and may have been upgraded from older versions of Windows—often have the most security issues at a network level. Older versions of Windows lack the security features of newer versions, and as older file servers are upgraded, administrators often overlook the need to investigate and configure new security options. Many of these options are, however, targeted at making file services more secure, and they're worth looking into.

✎ Although this chapter focuses on WS2K3 as the server operating system (OS), the majority of these features and settings are available, in some fashion, on Win2K as well.

Figure 5.3 shows some of the security policies that can be configured to make file services more secure in general. Note that some of these policies also apply to the client computers in your environment—because they relate specifically to file services (for example, client interaction with file servers), they're covered here.



Policy	Security Setting
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of credentials or .NET Passports for network...	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	COMNAP,COMNOD...
Network access: Remotely accessible registry paths	System\CurrentCon...
Network access: Remotely accessible registry paths and sub-paths	System\CurrentCon...
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Shares that can be accessed anonymously	COMCFG,DFS$
Network access: Sharing and security model for local accounts	Classic - local users ...
Network security: Do not store LAN Manager hash value on next password change	Disabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Send NTLM respons...
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure ...	No minimum
Network security: Minimum session security for NTLM SSP based (including secure ...	No minimum
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled

Figure 5.3: Examining the security options on a file server.

The settings shown in the figure are the default settings for a newly-installed WS2K3 server; the settings active on any particular server will be different if it was upgraded from an older version of Windows. Also note that the figure is displaying these settings from the computer's Local Policy; these settings can be configured on a per-server basis in Local Policy or can be centrally configured in AD using Group Policy (which is easier, more consistent, and definitely the recommended means of doing so). Key settings include:

- Microsoft network client [and server]: Digitally sign communications. There are two settings here; one that always signs communications and one that only does so if the server agrees to do the same. This policy is useful to apply on clients and servers because it allows computers to detect rogue servers that are attempting to fake (or *spoof*) a network connection in order to intercept information. Enable these settings for the best security.

Enabling signatures can create problems for older client computers (such as Windows 98) that don't support this feature; investigate the possible ramifications of enabling this setting in your environment before doing so.

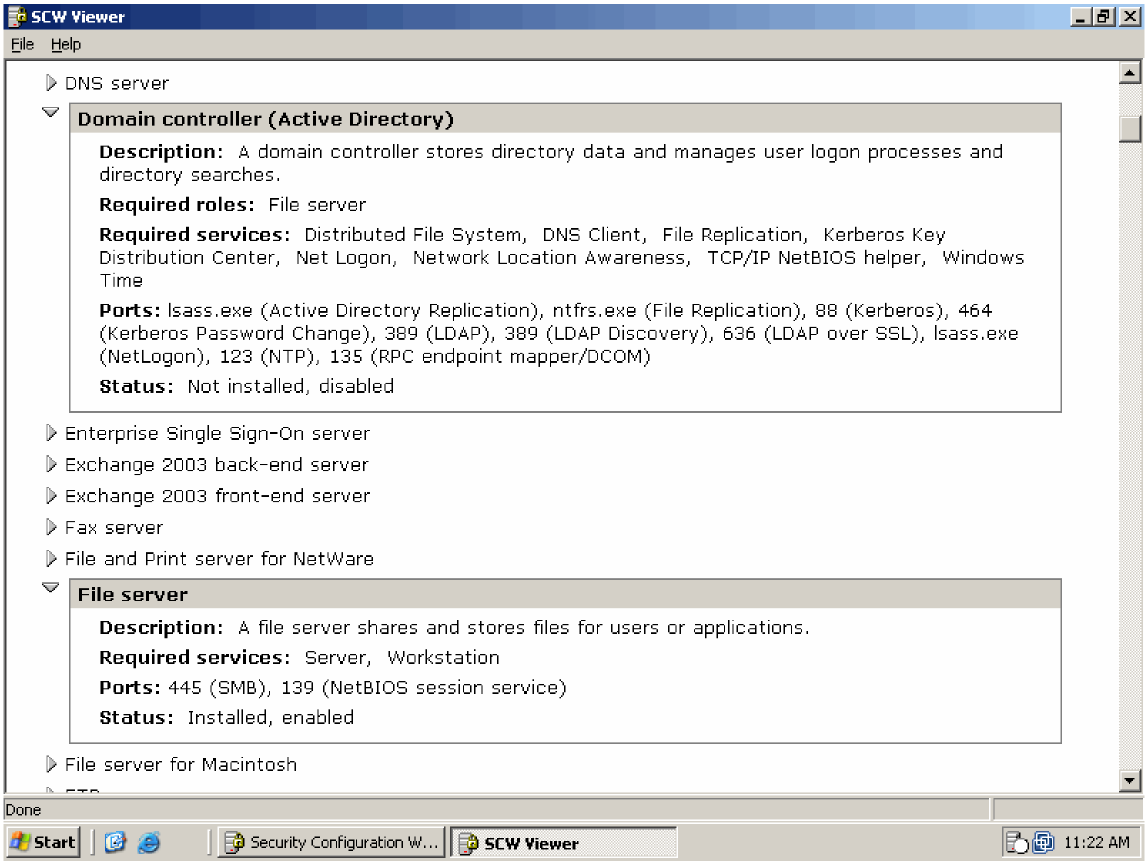
- Do not allow anonymous enumeration of the Security Accounts Manager (SAM) accounts and shares. The *shares* part of this setting is critical—allowing anonymous users to list the shares available on a server is a bad idea because it helps an anonymous attacker get an idea of which resources are available to attack. Enable this setting for better security.
- Let Everyone permissions apply to anonymous users. For best security, ensure that this setting is disabled, preventing the built-in “Everyone” group from including anonymous, unauthenticated users.
- Restrict anonymous access to Named Pipes and Shares. Once again, anonymous equals attacker in a security expert’s point of view, so enabling this setting will help defeat anonymous attackers seeking to gain information and access.
- Shares that can be accessed anonymously. There are a couple of shares in a domain environment that are typically meant to be accessed anonymously; this setting allows you to list them (the default settings are COMCFG and DFS$, required for COM configuration and Distributed File System). Ensure that no unnecessary shares are listed.

Another area of network security that file servers can benefit from is port restrictions. Normally, I’m a big fan of locking down servers’ ports so that only the ports absolutely necessary to the servers’ operations are open. However, I’m absolutely clear on how terrifying it can be to mess with a server’s ports: One wrong move and the whole company is screaming at you. File servers in particular are scary because they use so *many* ports. Despite numerous Microsoft articles listing required ports and so forth, most administrators are quite understandably reluctant to touch their servers’ port configurations.

To ease fears, you can use WS2K3 SP1’s Security Configuration Wizard (SCW). You have to install the SCW, which is an optional Windows component available to you after SP1 is installed. SCW can be used to generate templates, which can in turn be used to configure one or more servers. The beauty of the SCW is that, under the hood, it uses a Microsoft-produced XML file that describes various roles (such as file server or domain controller) that a server can fulfill. For each role, Microsoft has determined which services, ports, and other resources are required. In other words, you tell SCW that your server is a file server and it takes care of the rest, locking down unnecessary ports, services, and so forth.

☞ You don’t need to install the SCW on every server, or even run it on every server. When you run the SCW, it creates a security template; that template contains the configuration information you need. Templates can be applied manually by using the command-line Secedit.exe tool or imported into a Group Policy Object (GPO) and applied through AD.

Figure 5.4 illustrates the SCW’s Viewer, which shows the configuration database after SCW tries to figure out which roles your server is already fulfilling based upon the services and applications already running. In this example, the server is a file server but not a domain controller.



DNS server

Domain controller (Active Directory)

Description: A domain controller stores directory data and manages user logon processes and directory searches.

Required roles: File server

Required services: Distributed File System, DNS Client, File Replication, Kerberos Key Distribution Center, Net Logon, Network Location Awareness, TCP/IP NetBIOS helper, Windows Time

Ports: lsass.exe (Active Directory Replication), ntfrs.exe (File Replication), 88 (Kerberos), 464 (Kerberos Password Change), 389 (LDAP), 389 (LDAP Discovery), 636 (LDAP over SSL), lsass.exe (NetLogon), 123 (NTP), 135 (RPC endpoint mapper/DCOM)

Status: Not installed, disabled

Enterprise Single Sign-On server

Exchange 2003 back-end server

Exchange 2003 front-end server

Fax server

File and Print server for NetWare

File server

Description: A file server shares and stores files for users or applications.

Required services: Server, Workstation

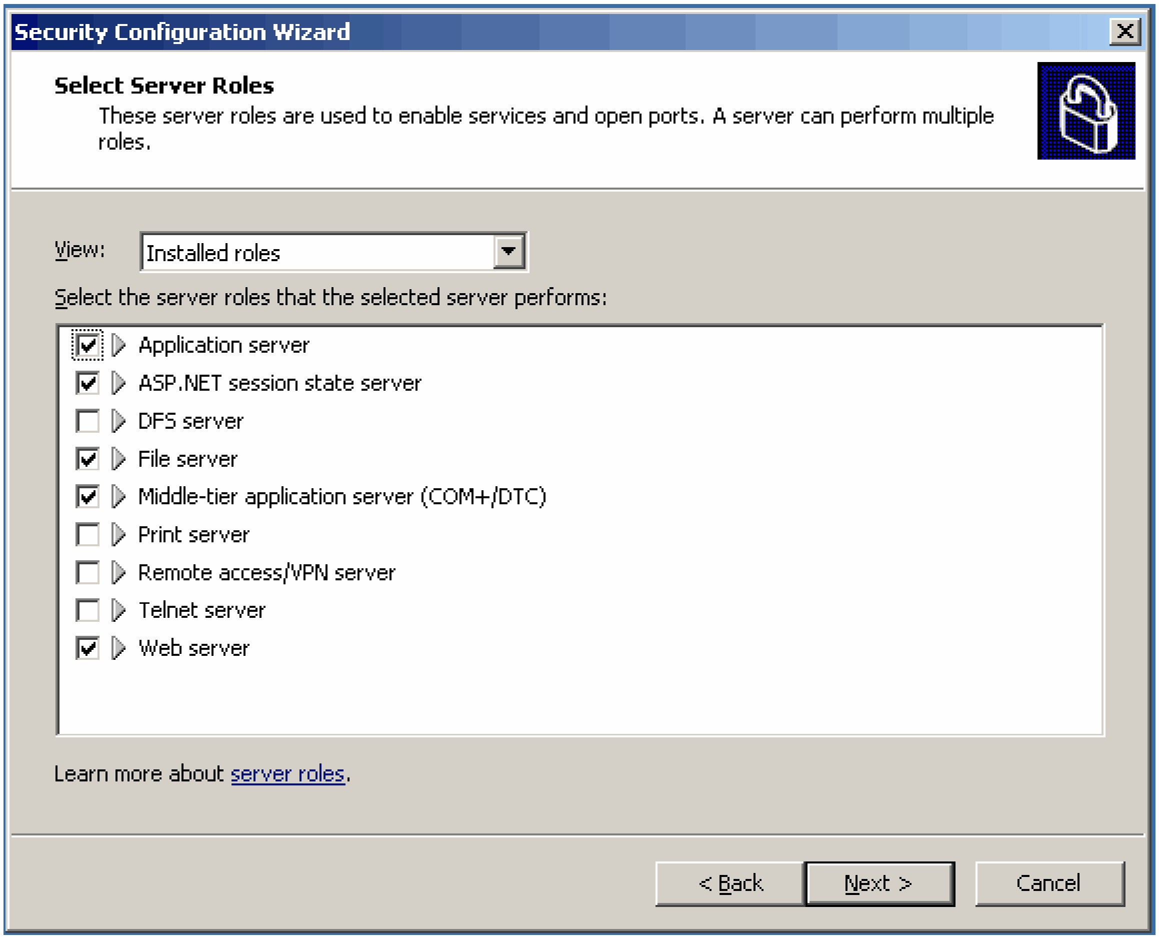
Ports: 445 (SMB), 139 (NetBIOS session service)

Status: Installed, enabled

File server for Macintosh

Figure 5.4: Using the SCW Viewer to examine configured server roles.

After analyzing your server, SCW will ask you—as Figure 5.5 shows—which roles you *want* the server to fill. As shown, it starts by assuming the server is in fact meant to be running all of the software SCW detected. If, for example, you didn’t mean for this server to be running IIS, you would clear the *Application server* check box, the *Web server* check box, and so forth. The check boxes shown can be filtered to include only roles for which software is already installed (as shown), all possible roles, and so forth.



Select Server Roles

These server roles are used to enable services and open ports. A server can perform multiple roles.

View: Installed roles

Select the server roles that the selected server performs:

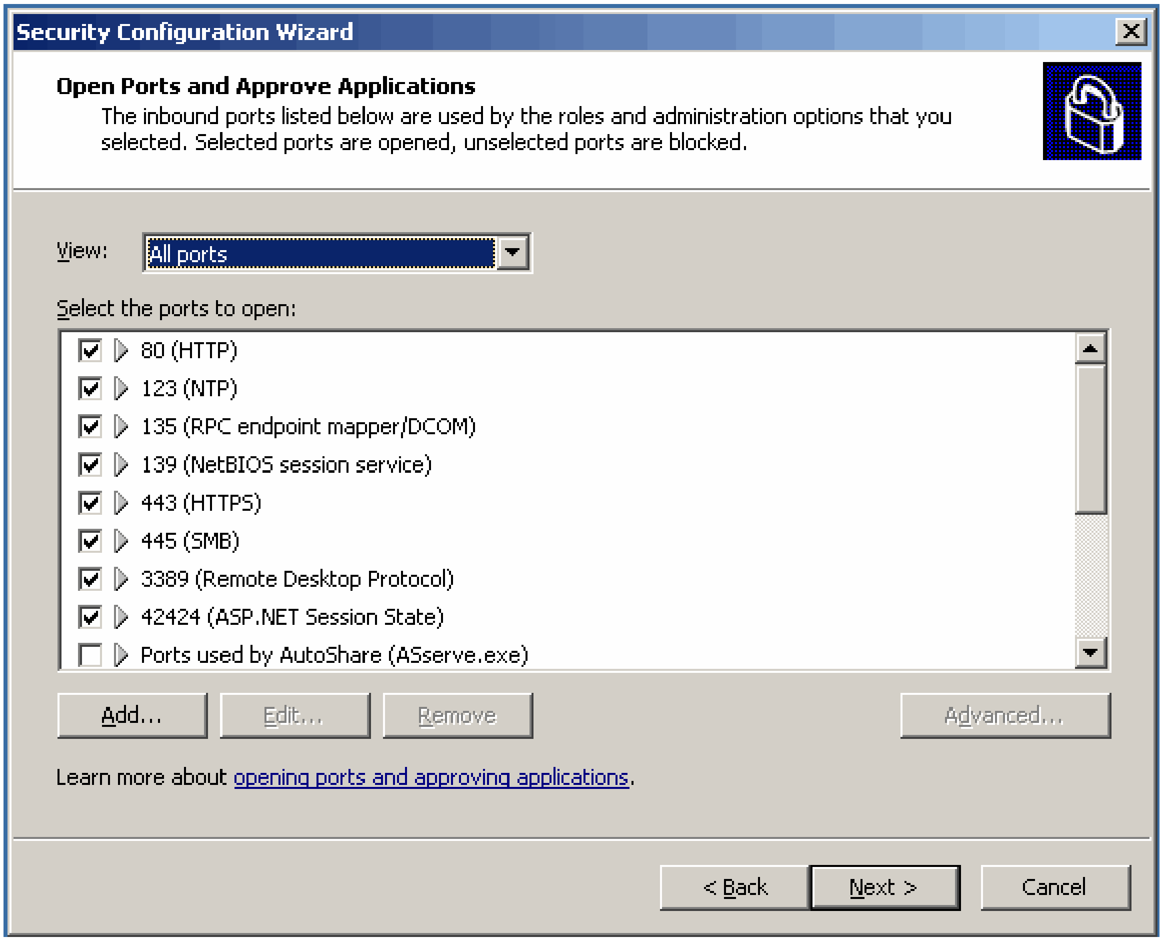
☑ Application server
☑ ASP.NET session state server
□ DFS server
☑ File server
☑ Middle-tier application server (COM+/DTC)
□ Print server
□ Remote access/VPN server
□ Telnet server
☑ Web server

Learn more about server roles.

Figure 5.5: Configuring the intended roles.

> ☞ Remember, changing check box settings won't automatically reconfigure your server and break anything. The SCW's end product is a template, or policy, not an immediate reconfiguration of the machine.

As Figure 5.6 illustrates, the SCW also looks specifically at the TCP/IP ports that are open on the computer, pre-selecting the ports that are required for the roles you selected for the server. This functionality is the SCW's real strength because its underlying XML configuration file knows which ports go with which roles and features of Windows, eliminating guesswork on your part.



Open Ports and Approve Applications

The inbound ports listed below are used by the roles and administration options that you selected. Selected ports are opened, unselected ports are blocked.

View: All ports

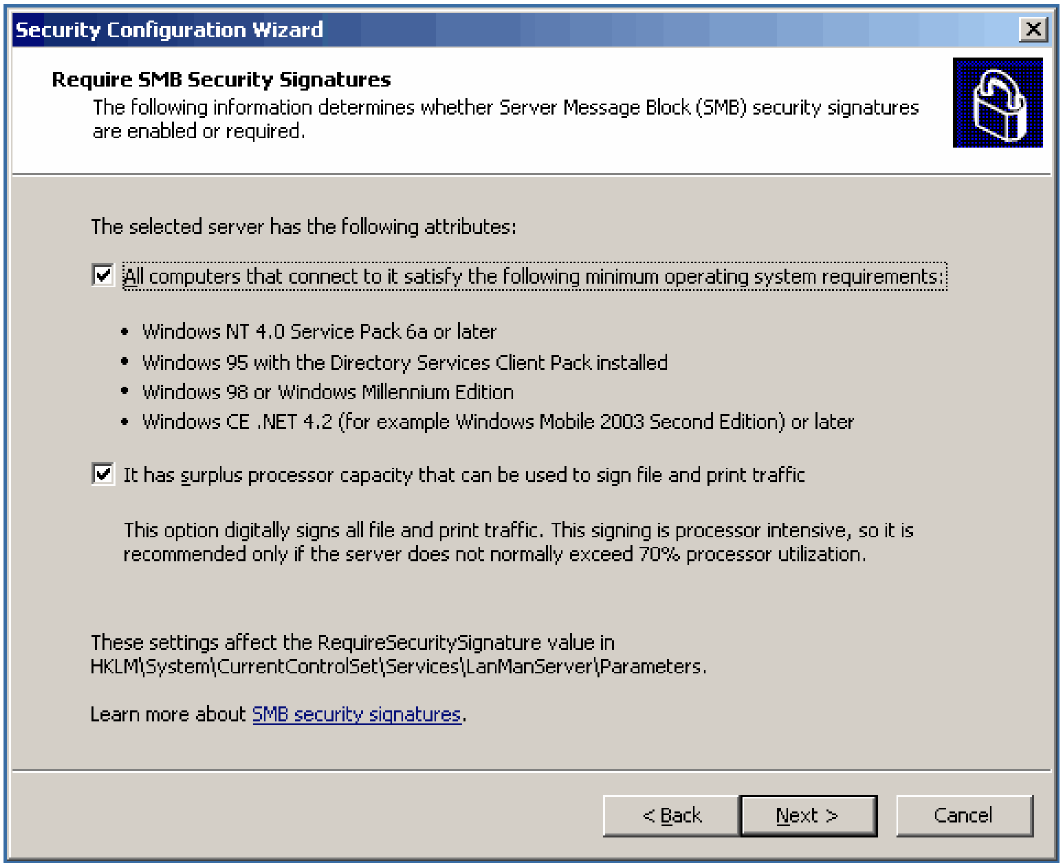
Select the ports to open:

- ☑ 80 (HTTP)
- ☑ 123 (NTP)
- ☑ 135 (RPC endpoint mapper/DCOM)
- ☑ 139 (NetBIOS session service)
- ☑ 443 (HTTPS)
- ☑ 445 (SMB)
- ☑ 3389 (Remote Desktop Protocol)
- ☑ 42424 (ASP.NET Session State)
- □ Ports used by AutoShare (ASserve.exe)

Learn more about opening ports and approving applications.

Figure 5.6: Configuring allowed TCP/IP ports.

Figure 5.7 shows another file server-specific option of the SCW. The wizard prompts you to find out whether the server has sufficient extra processor capacity that can be devoted to digitally signing file and print traffic. By indicating that the server does, SCW will configure the resulting policy template to enable Server Message Blocks (SMB) signing, a feature that can help eliminate spoofing and other forms of attack on your network.


Security Configuration Wizard

Require SMB Security Signatures
The following information determines whether Server Message Block (SMB) security signatures are enabled or required.

The selected server has the following attributes:

☑ All computers that connect to it satisfy the following minimum operating system requirements:

- Windows NT 4.0 Service Pack 6a or later
- Windows 95 with the Directory Services Client Pack installed
- Windows 98 or Windows Millennium Edition
- Windows CE .NET 4.2 (for example Windows Mobile 2003 Second Edition) or later

☑ It has surplus processor capacity that can be used to sign file and print traffic

This option digitally signs all file and print traffic. This signing is processor intensive, so it is recommended only if the server does not normally exceed 70% processor utilization.

These settings affect the RequireSecuritySignature value in HKLM\System\CurrentControlSet\Services\LanManServer\Parameters.

Learn more about SMB security signatures.

Figure 5.7: SCW options that enable file and print traffic signing.

Why bother locking down ports and services to begin with? Because Windows has bugs. With millions of lines of code, the OS will probably *always* have bugs. By disabling unused ports, you can prevent anything from accessing portions of the OS—primarily services—that aren't in use and potentially may contain bugs. By restricting the services that are running (a concept I'll cover in more detail in the next chapter), you prevent code from running which isn't necessary and which might contain bugs. The SCW is, in fact, a tacit acknowledgement on Microsoft's part that Windows probably contains undiscovered bugs, that not every feature of Windows is needed on every server, and that disabling and preventing access to unused features will help mitigate the fact that they probably contain undiscovered vulnerabilities.

📖 The SCW has applications beyond file servers, so the next chapter will examine it in more detail.

Data Resilience

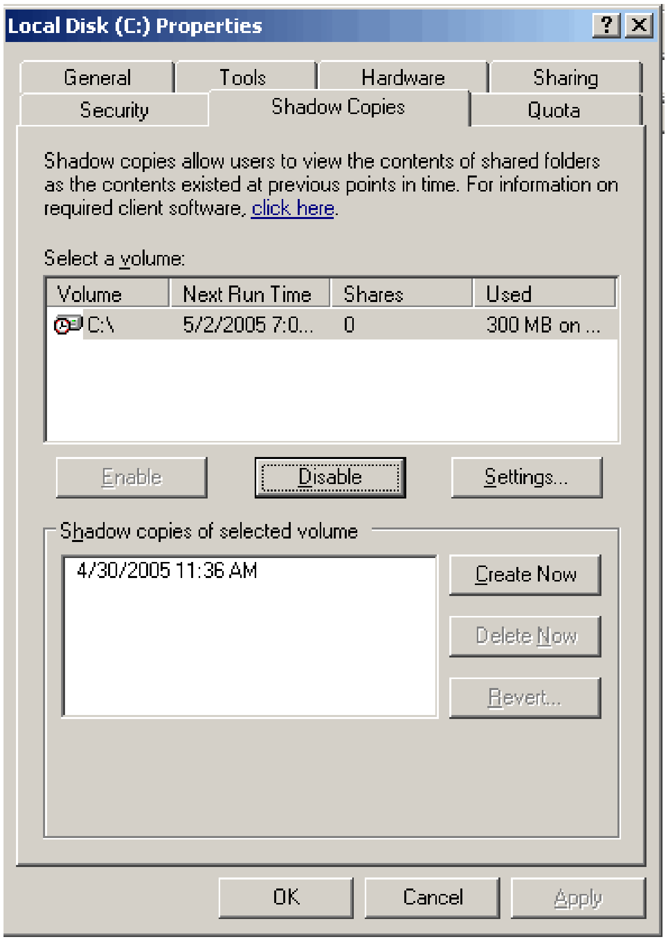
Data resilience—the ability for an administrator or a server to deal with data loss—is often seen as a purely operational issue. However, lost or corrupted data can also be a security issue. For example, if an attacker is able to gain access to network configuration documentation and modify it, the attacker might be able to convince an administrator to reconfigure the network according to the modified documentation (convincing someone to do something they shouldn't is a technique often referred to as *social engineering*, playing off the human weak point in the network's security). That's just one example; there are a number of ways in which illegally modified or deleted data can result in a security problem. Thus, data resilience has a clear security application as well as the more traditional, operational application.

Volume Shadow Copy

Other than the time-honored practice of making frequent backups of your data, Windows includes some nice features to help improve data resiliency and make data recovery easier and more convenient. One of those features is Windows' Volume Shadow Copy service capabilities.

As Figure 5.8 shows, VCS is enabled on a per-volume basis. Once enabled, all files located within a shared folder will be *shadowed*, meaning Windows will retain old versions of files for faster recovery. These old versions are retained in a shadow copy area, which can be located on the same volume or on a separate volume (which is more appropriate for high-volume file servers). Windows doesn't create a shadow copy for every change made to a file; instead, snapshots are taken on a schedule that you can set (the default is two per day).

> ✎ Hidden administrative shares—such as the default C$ share—aren't counted by the Shadow Copy panel, as Figure 5.8 illustrates. In the figure, the number of shares is zero, even though we know there's a default C$ share present.



Shadow copies allow users to view the contents of shared folders as the contents existed at previous points in time. For information on required client software, click here.

Select a volume:

Volume	Next Run Time	Shares	Used
C:\	5/2/2005 7:0...	0	300 MB on ...

Shadow copies of selected volume

4/30/2005 11:36 AM

Figure 5.8: Configuring the Volume Shadow Copy service on the C volume.

Some recommendations regarding the Volume Shadow Copy service:

- Enable it on all file servers, but only on the volumes that contain user share folders (for example, those shares that contain user-accessible files).
- Set a size limit for the shadow copy storage area based on how many files tend to change per day and how frequently you're taking shadow copy snapshots. When the storage area is full, older shadow copies are deleted, so setting the storage area too small will result in too few copies being retained.

  During a Volume Shadow Copy snapshot, only files that have changed since the last snapshot are backed up into the shadow copy storage area, so the rate at which that storage area fills up depends on how frequently files change on the server.
- Don't schedule more than one snapshot per hour, and schedule fewer for especially busy file servers.
- Configure the shadow copy storage area for a separate volume. Ideally, this volume might be a non-RAID volume (because the data is just backup data, anyway) dedicated to the Volume Shadow Copy storage.

Clients will need to install a client component—which comes on the Windows Server CD-ROM—in order to access shadow copies. This client, called the Previous Versions Client, allows Windows Explorer to access the inventory of shadow copies for any given file, and allows users to retrieve past versions of a file (which can be saved to a different location, to avoid overwriting the current version of the file). You can reserve this functionality for administrators by simply not installing the client software on your users' client computers.

The Volume Shadow Copy service performs essentially the same task as a traditional disk- or tape-based backup but makes the backed-up files more readily accessible. Microsoft's intention with the Volume Shadow Copy service was to make it possible for users to retrieve recent versions of files without having to contact an administrator; this same functionality, however, has a useful security application because it can be used to protect sensitive files and quickly retrieve older versions in case an unauthorized change (or deletion) occurs.

Storage Management, Hierarchical Storage, and Antivirus

WS2K3 (and Win2K, for that matter) includes Remote Storage services, a basic hierarchical storage management system. You can read more about it at http://support.microsoft.com/?kbid=816588; essentially its job is to monitor the free space available on a server's local drives. When the free space drops below a designated point, Remote Storage locates infrequently used files and moves them to an attached tape or optical drive. The moved files retain a pointer in the main NTFS file system, meaning that users can continue to see the files when browsing the network. When a user attempts to access a moved file, Remote Storage locates it on tape (or optical disk, or whatever) and moves it back into the main file system of the server. There is a delay while the file is accessed, but the process is automatic.

> ✎ Remote Storage is only available on the Advanced (or Enterprise) and Datacenter editions of Win2K and WS2K3.

This process is called hierarchical storage management (HSM) because it creates a hierarchy of storage capabilities: *Online* storage (local disks), which are fast but generally more expensive; *near-line* storage (such as tapes) which are slower but cheaper; and even *offline* storage, where data is moved off the server completely and an administrator is required to retrieve it when needed. Third-party vendors such as Legato and VERITAS offer more robust HSM solutions, helping to further automate and streamline the process of moving data between online, near-line, and offline storage systems. Figure 5.9 illustrates the various levels of storage usually included in a full HSM system.

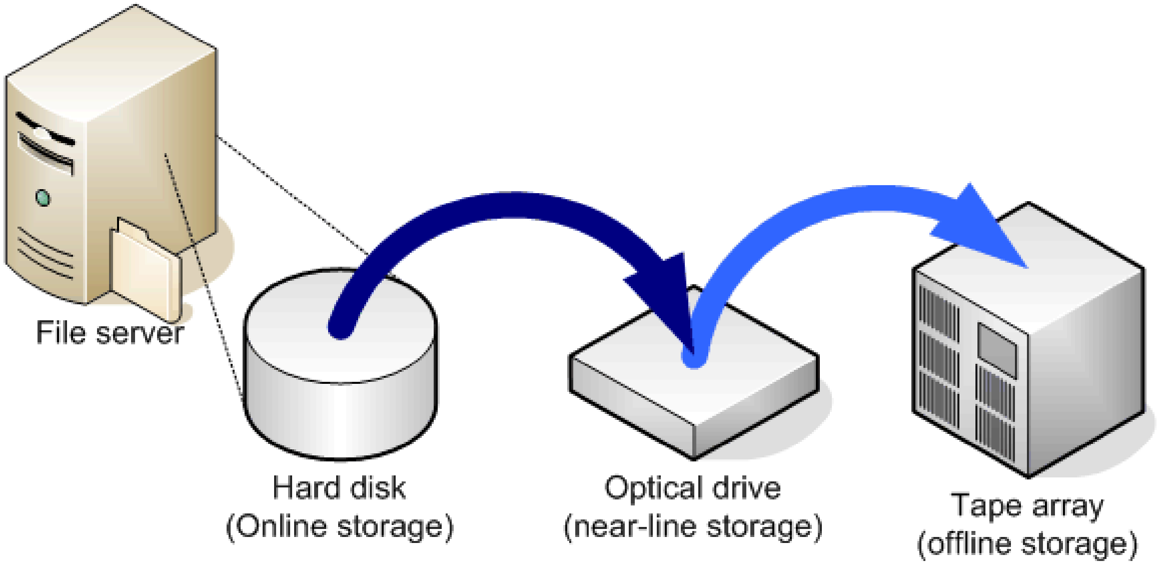


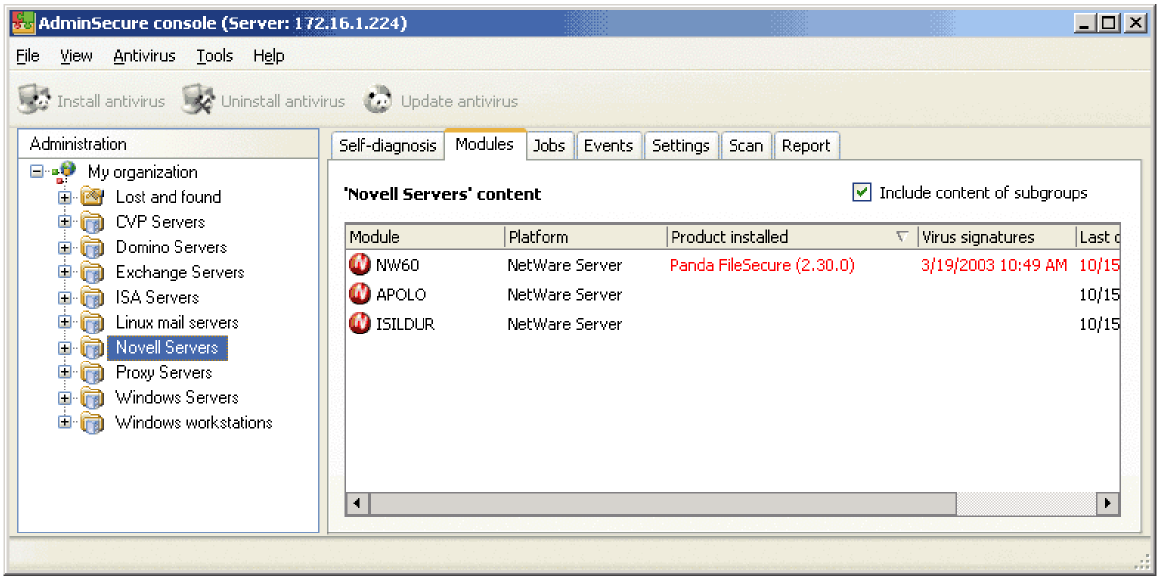
Figure 5.9: HSM includes various levels of storage.

So what does HSM have to do with security? HSM helps security in a number of ways:

- Because HSM can migrate data off expensive file server storage, data doesn't need to be deleted, therefore reducing the risk that critical data will be deleted by accident.
- HSM can also help prevent file servers from becoming filled and unavailable, because older data is moved offline or near-line, ensuring that the file server can continue to function.
- Because third-party HSM solutions are often integrated as part of an overall backup and recovery package, disaster recovery becomes an easier, more automatic operation, helping to guard against the loss of critical data.

Although the security implications might not be obvious, storage management in general—including HSM as well as traditional backup and restore—is really all about security—the security (that is, the safety) of your data. Other forms of storage management can play an important role in securing file servers, too. For example, VERITAS Storage Exec can help ensure that unwanted files stay off file servers, which helps to guard against operationally problematic files (such as copyrighted MP3 files or inappropriate graphic files), as well as outright dangerous files (such as file types known to be associated with viral attack vectors, such as VBS files).

Finally, one last and perhaps more obvious storage management category is antivirus software, which plays a crucial role in helping to secure file servers. Virus scanning should occur at every possible level of your enterprise. Client computers may all have antivirus software, but it is difficult to ensure that the software is always kept up-to-date. By adding antivirus scanning to each file server, you can help ensure that viruses don't propagate through the file servers' centralized storage resources. Most major antivirus manufacturers offer solutions specifically for file servers: Panda Software offers FileSecure, Trend Micro offers ServerProtect Antivirus, McAfee offers VirusScan Enterprise, and so forth. Most of the enterprise-level solutions are more easily managed from a central console than per-client antivirus software. For example, Figure 5.10 shows Panda Software's AdminSecure console, which provides management of all server-based antivirus software including Exchange servers, Novell file servers, Windows file servers, and even Windows workstations.



'Novell Servers' content

☑ Include content of subgroups

Module	Platform	Product installed	Virus signatures	Last c
NW60	NetWare Server	Panda FileSecure (2.30.0)	3/19/2003 10:49 AM	10/15
APOLO	NetWare Server			10/15
ISILDUR	NetWare Server			10/15

Figure 5.10: Panda antivirus software console.

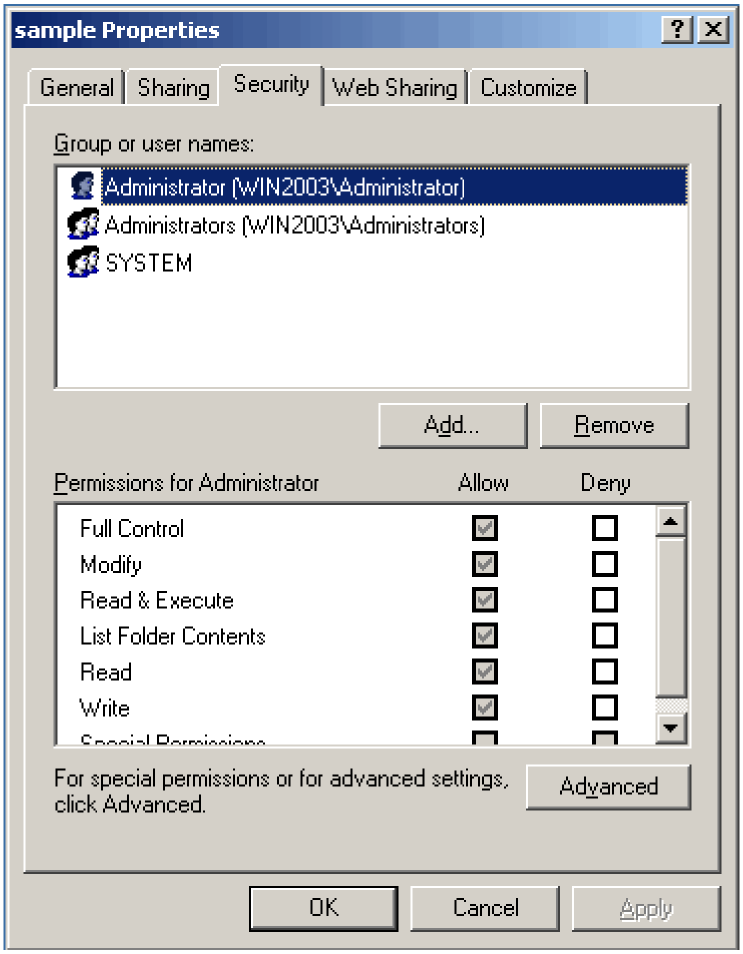
Of course, server-based anti-spyware scanning—available from most of the same third-party vendors—is another critical piece of security for file servers, as spyware can not only damage data but also help deliver it off your network to unauthorized individuals.

☞ One industry best practice is to use different manufacturers' virus and spyware scanning solutions at different levels. For example, if you've adopted Symantec (Norton) software on your client computers, select a different vendor for server-based scanning, a different one for firewall-based scanning, and so forth. The theory is that no one solution catches everything, so by using a variety, you're more likely to have fewer holes through which malicious software can slip.

Thus, while storage management—including Volume Shadow Copy, antivirus scanning, anti-spyware scanning, and HSM—plays a sometimes less-than-obvious role in file server security, it is nonetheless an important role. Proper storage management can help keep critical data safe, undamaged, unmodified, and uninfected, all of which helps contribute to a more secure Windows-based enterprise.

Applying Proper File Permissions

I've saved the biggest and best for last—file permissions. Perhaps the most obvious portion of file server security, file permissions are also one of the most complex. Although Windows offers exceedingly complex and granular file permissions capabilities, complete with permissions inheritance, it also offers a relatively poor GUI through which these complex permissions are managed. For example, Figure 5.11 shows the basic Windows file and folder permissions dialog box. Notice that the check boxes, used to assign permissions are unavailable (grayed out). This element visually indicates that the permissions have been inherited from a parent folder, and that they therefore can't be changed directly on this folder without first disabling inheritance and copying the existing inherited permissions directly onto the folder. A simple, grayed-out check box carries a lot of hidden, less-than-intuitive meaning!



Group or user names:

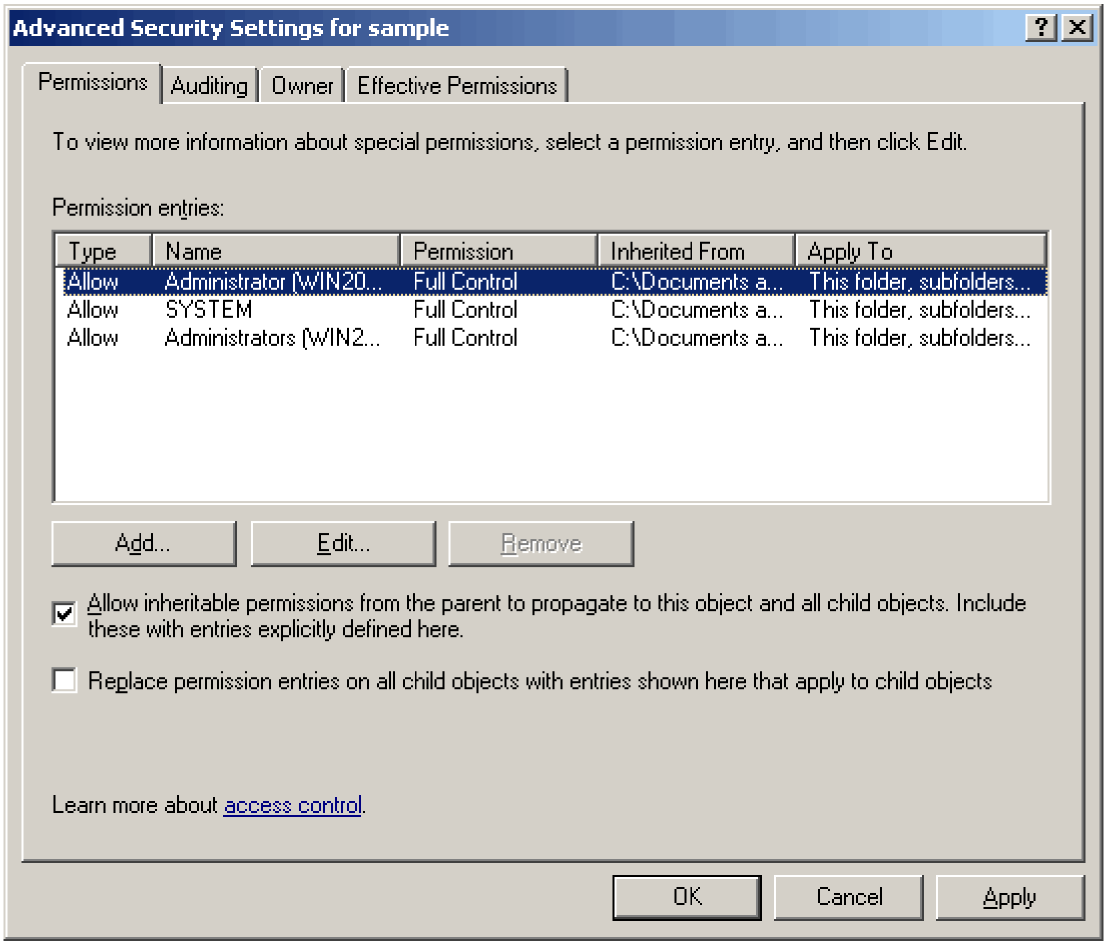
- Administrator (WIN2003\Administrator)
- Administrators (WIN2003\Administrators)
- SYSTEM

Permissions for Administrator	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

Figure 5.11: Basic file and folder permissions in Windows.

Even worse, many permissions are *special*, meaning they're not fully displayed in this simplified dialog box. Figure 5.12 shows the advanced permissions dialog box, which lists in greater detail the permissions applied to this folder.



Advanced Security Settings for sample

Permissions | Auditing | Owner | Effective Permissions

To view more information about special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Administrator (WIN20...	Full Control	C:\Documents a...	This folder, subfolders...
Allow	SYSTEM	Full Control	C:\Documents a...	This folder, subfolders...
Allow	Administrators (WIN2...	Full Control	C:\Documents a...	This folder, subfolders...

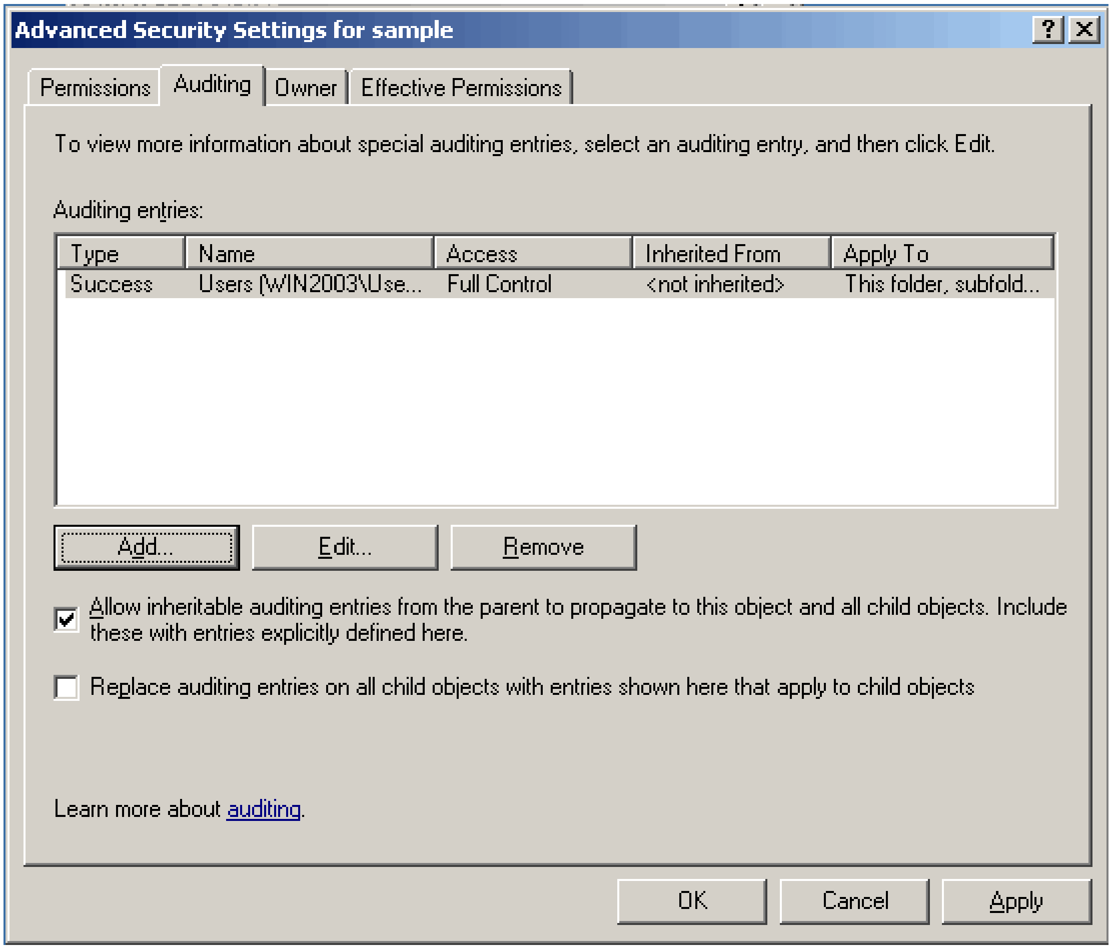
☑ Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.

□ Replace permission entries on all child objects with entries shown here that apply to child objects

Learn more about access control.

Figure 5.12: Examining special permissions on a folder.

This screen helps you determine where inherited permissions are coming from (in the Inherited From column) as well as enables you to control the more detailed and granular permissions that can be associated with this particular object. Auditing—a key portion of any secure enterprise, especially those dealing with legislative auditing and accounting requirements—is also configured from this dialog box, on the Auditing tab, which Figure 5.13 shows.



To view more information about special auditing entries, select an auditing entry, and then click Edit.

Auditing entries:

Type	Name	Access	Inherited From	Apply To
Success	Users (WIN2003\Use...	Full Control	<not inherited>	This folder, subfold...

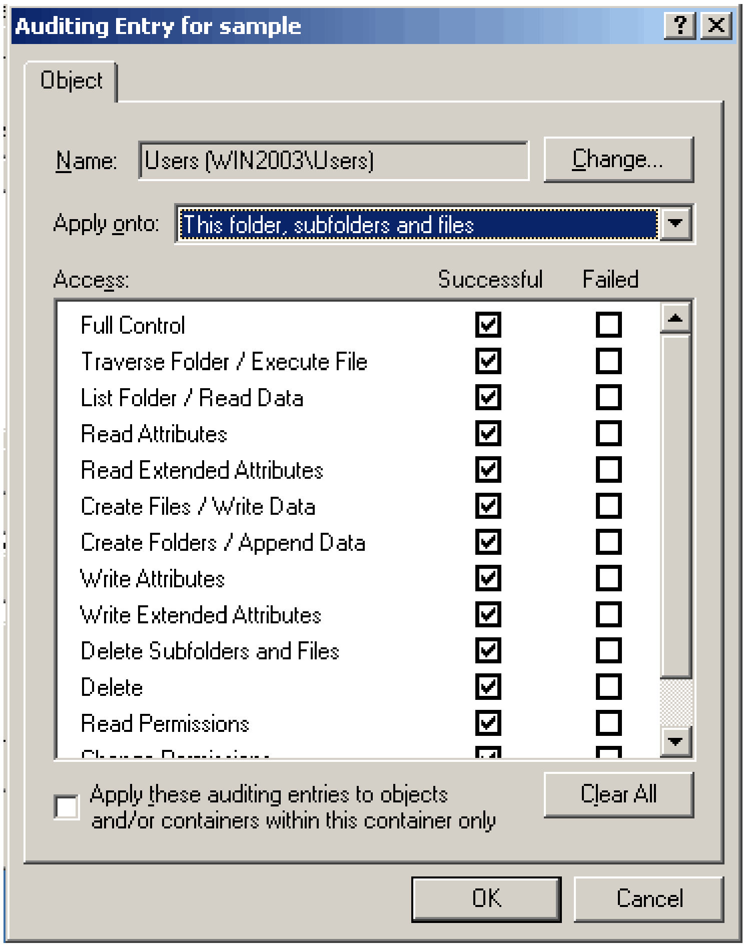
☑ Allow inheritable auditing entries from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.

□ Replace auditing entries on all child objects with entries shown here that apply to child objects

Learn more about auditing.

Figure 5.13: Auditing entries applied to a folder.

Unfortunately, even this dialog box doesn’t always display the full complexity of what has been applied to the folder. Figure 5.14 shows the dialog box used to add an auditing entry to the folder, and you can see that it offers several choices that aren’t as easy to see in the summary dialog box that Figure 5.13 shows.



Name: Users (WIN2003\Users)

Apply onto: This folder, subfolders and files

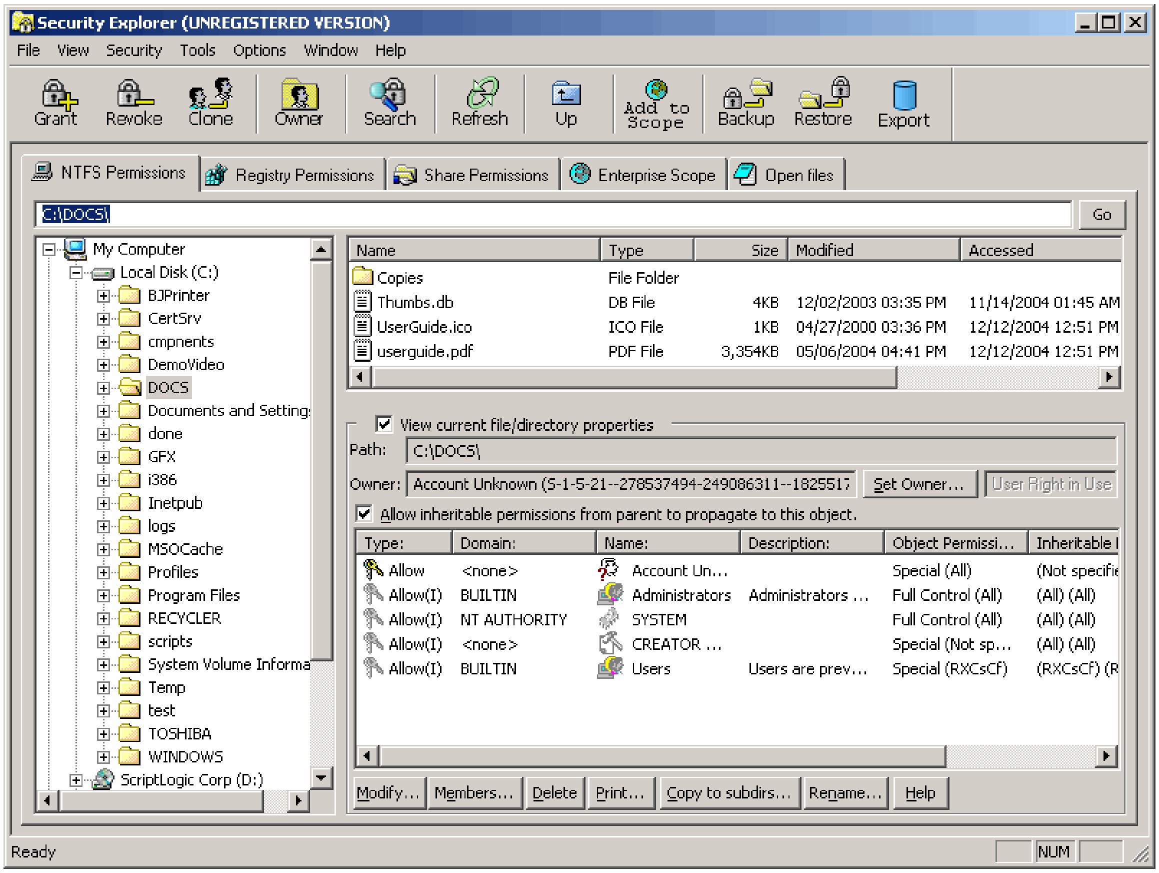
Access:	Successful	Failed
Full Control	☑	□
Traverse Folder / Execute File	☑	□
List Folder / Read Data	☑	□
Read Attributes	☑	□
Read Extended Attributes	☑	□
Create Files / Write Data	☑	□
Create Folders / Append Data	☑	□
Write Attributes	☑	□
Write Extended Attributes	☑	□
Delete Subfolders and Files	☑	□
Delete	☑	□
Read Permissions	☑	□

□ Apply these auditing entries to objects and/or containers within this container only

Figure 5.14: Adding an auditing entry to a folder.

The point is to demonstrate that Windows' user interface (UI) for managing permissions seems easy-to-use at first, but in fact can be less then intuitive and overly complicated when managing complicated file permissions. In fact, I blame this UI for many of the file server security issues I've run across—the interface just doesn't make clear what is going on, making it easier for administrators to make mistakes when applying permissions and auditing entries to files and folders. It is also frustrating that Windows has no built-in searching functionality for permissions. In other words, strictly using Windows' built-in tools, there is no way to discover which permissions a particular user has across all the files on a server—or across multiple servers.

So what is the solution? Obviously, a third-party tool with a better interface. Several exist, in fact, and many offer an interface that is comfortingly similar to the Windows interface, making the solution somewhat more intuitive (see Figure 5.15). Such products offer an Explorer-like folder hierarchy and the security information in one view, making it infinitely easier to browse folders' security. Inheritance is more clearly displayed, and a form of shorthand is used so that most special permissions can be seen right on the main screen (notice the last permission entry, which lists RXCsCf for Read, eXecute, Create subfolder, and Create file).



C:\DOCS\

Name	Type	Size	Modified	Accessed
Copies	File Folder			
Thumbs.db	DB File	4KB	12/02/2003 03:35 PM	11/14/2004 01:45 AM
UserGuide.ico	ICO File	1KB	04/27/2000 03:36 PM	12/12/2004 12:51 PM
userguide.pdf	PDF File	3,354KB	05/06/2004 04:41 PM	12/12/2004 12:51 PM

☑ View current file/directory properties

Path: C:\DOCS\

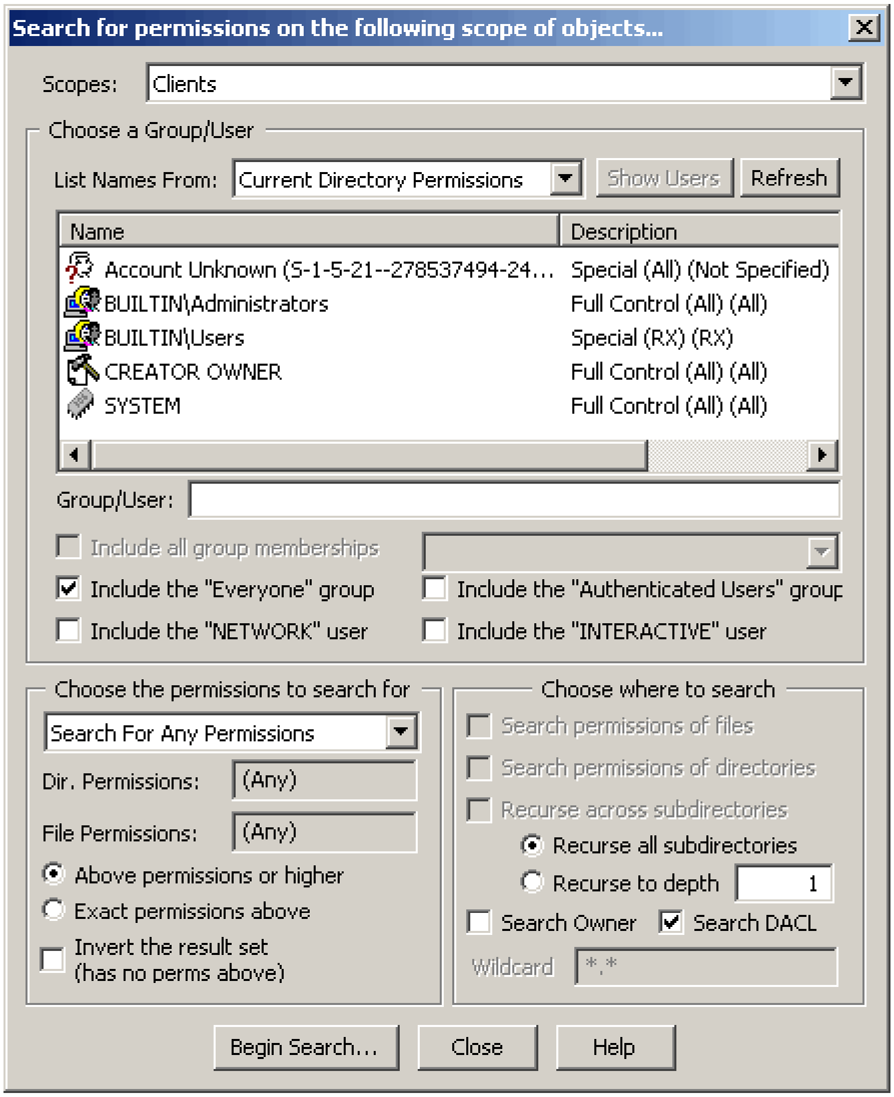
Owner: Account Unknown (S-1-5-21--278537494-249086311--1825517

☑ Allow inheritable permissions from parent to propagate to this object.

Type:	Domain:	Name:	Description:	Object Permissi...	Inheritable I
Allow	<none>	Account Un...		Special (All)	(Not specifie
Allow(I)	BUILTIN	Administrators	Administrators ...	Full Control (All)	(All) (All)
Allow(I)	NT AUTHORITY	SYSTEM		Full Control (All)	(All) (All)
Allow(I)	<none>	CREATOR ...		Special (Not sp...	(All) (All)
Allow(I)	BUILTIN	Users	Users are prev...	Special (RXCsCf)	(RXCsCf) (R

Figure 5.15: ScriptLogic Security Explorer.

In addition, these tools can provide built-in search functionality, as Figure 5.16 shows, allowing you to quickly locate specific permissions across specified objects. This functionality is sorely needed in Windows, especially on file servers with tens of thousands of objects.



Search for permissions on the following scope of objects...

Scopes: Clients

Choose a Group/User

List Names From: Current Directory Permissions

Name	Description
Account Unknown (S-1-5-21--278537494-24...	Special (All) (Not Specified)
BUILTIN\Administrators	Full Control (All) (All)
BUILTIN\Users	Special (RX) (RX)
CREATOR OWNER	Full Control (All) (All)
SYSTEM	Full Control (All) (All)

Group/User:

□ Include all group memberships
☑ Include the "Everyone" group
□ Include the "Authenticated Users" group
□ Include the "NETWORK" user
□ Include the "INTERACTIVE" user

Choose the permissions to search for

Search For Any Permissions

Dir. Permissions: (Any)

File Permissions: (Any)

● Above permissions or higher
○ Exact permissions above
□ Invert the result set (has no perms above)

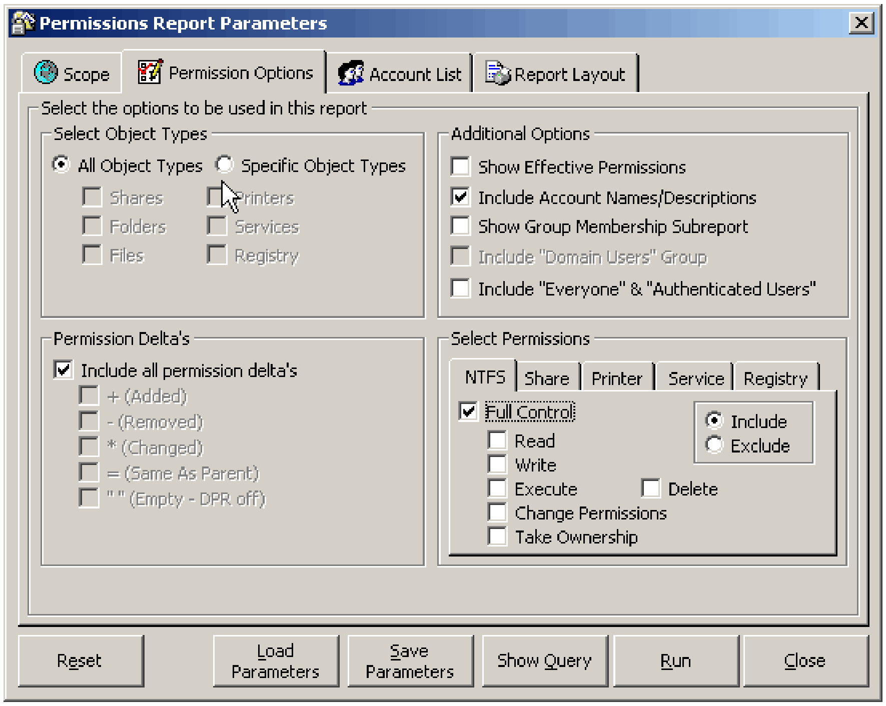
Choose where to search

□ Search permissions of files
□ Search permissions of directories
□ Recurse across subdirectories
● Recurse all subdirectories
○ Recurse to depth 1
□ Search Owner
☑ Search DACL

Wildcard *.*

Figure 5.16: Searching for permissions in Security Explorer.

If you need more robust reporting capabilities, there are third-party tools that offer the functionality you need. Such tools collect security information into a centralized database, allowing faster reporting on that data. Figure 5.17, for example, shows a file permissions search for all objects that have explicit Full Control permissions applied.



Select the options to be used in this report

Select Object Types

● All Object Types ○ Specific Object Types

□ Shares □ Printers
□ Folders □ Services
□ Files □ Registry

Additional Options

□ Show Effective Permissions
☑ Include Account Names/Descriptions
□ Show Group Membership Subreport
□ Include "Domain Users" Group
□ Include "Everyone" & "Authenticated Users"

Permission Delta's

☑ Include all permission delta's
□ + (Added)
□ - (Removed)
□ * (Changed)
□ = (Same As Parent)
□ " " (Empty - DPR off)

Select Permissions

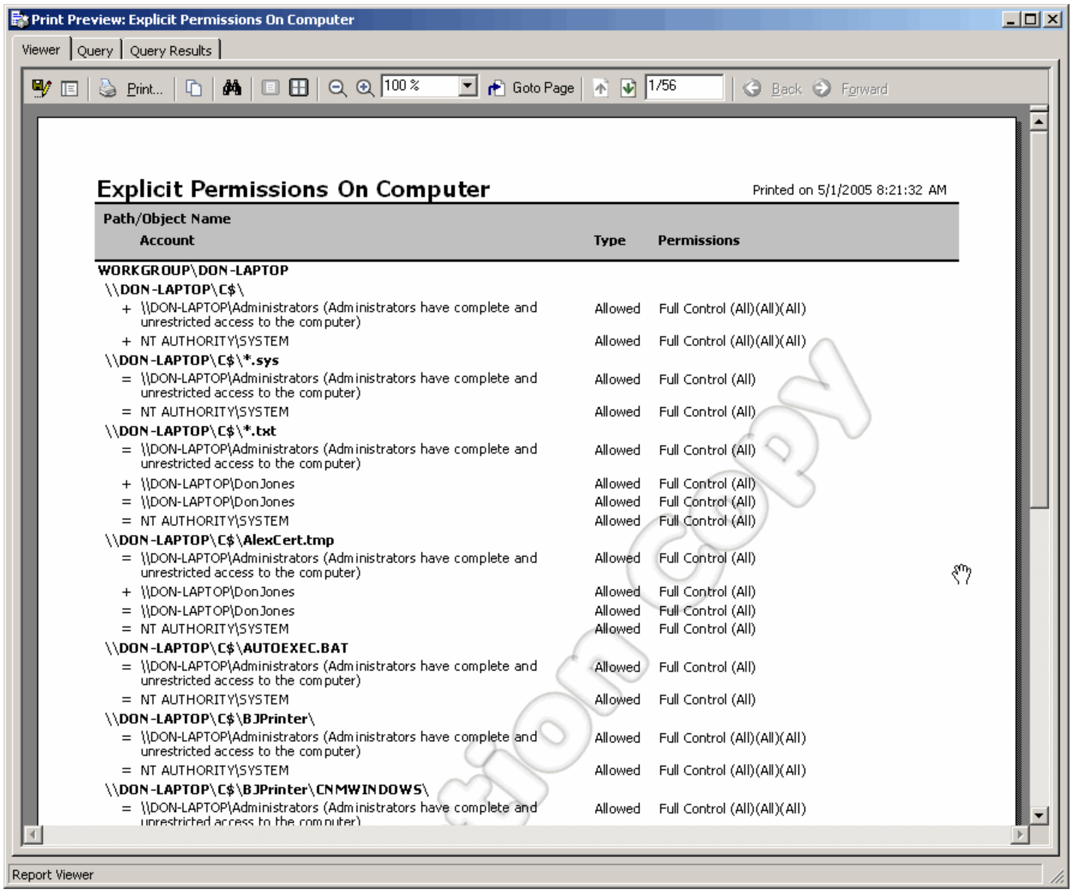
NTFS | Share | Printer | Service | Registry

☑ Full Control
□ Read
□ Write
□ Execute □ Delete
□ Change Permissions
□ Take Ownership

● Include
○ Exclude

Figure 5.17: Configuring a permissions search in ScriptLogic Enterprise Security Reporter.

Figure 5.18 shows the results of the search, which took only a few seconds to run because all the security information had already been collected into a central database.



Explicit Permissions On Computer

Printed on 5/1/2005 8:21:32 AM

Path/Object Name Account	Type	Permissions
WORKGROUP\DON-LAPTOP		
\\DON-LAPTOP\C$		
+ \\DON-LAPTOP\Administrators (Administrators have complete and unrestricted access to the computer)	Allowed	Full Control (All)(All)(All)
+ NT AUTHORITY\SYSTEM	Allowed	Full Control (All)(All)(All)
\\DON-LAPTOP\C$*.sys		
= \\DON-LAPTOP\Administrators (Administrators have complete and unrestricted access to the computer)	Allowed	Full Control (All)
= NT AUTHORITY\SYSTEM	Allowed	Full Control (All)
\\DON-LAPTOP\C$*.txt		
= \\DON-LAPTOP\Administrators (Administrators have complete and unrestricted access to the computer)	Allowed	Full Control (All)
+ \\DON-LAPTOP\DonJones	Allowed	Full Control (All)
= \\DON-LAPTOP\DonJones	Allowed	Full Control (All)
= NT AUTHORITY\SYSTEM	Allowed	Full Control (All)
\\DON-LAPTOP\C$\AlexCert.tmp		
= \\DON-LAPTOP\Administrators (Administrators have complete and unrestricted access to the computer)	Allowed	Full Control (All)
+ \\DON-LAPTOP\DonJones	Allowed	Full Control (All)
= \\DON-LAPTOP\DonJones	Allowed	Full Control (All)
= NT AUTHORITY\SYSTEM	Allowed	Full Control (All)
\\DON-LAPTOP\C$\AUTOEXEC.BAT		
= \\DON-LAPTOP\Administrators (Administrators have complete and unrestricted access to the computer)	Allowed	Full Control (All)
= NT AUTHORITY\SYSTEM	Allowed	Full Control (All)
\\DON-LAPTOP\C$\BJPrinter		
= \\DON-LAPTOP\Administrators (Administrators have complete and unrestricted access to the computer)	Allowed	Full Control (All)(All)(All)
= NT AUTHORITY\SYSTEM	Allowed	Full Control (All)(All)(All)
\\DON-LAPTOP\C$\BJPrinter\CNMWINDOWS		
= \\DON-LAPTOP\Administrators (Administrators have complete and unrestricted access to the computer)	Allowed	Full Control (All)(All)(All)

Figure 5.18: Viewing an Enterprise Security Reporter security report.

> ☞ Remember the worst nightmare I opened this chapter with? Enterprise Security Reporter is a tool that can help solve it, by showing you every file and folder in your organization that has permissions assigned directly to a user, rather than to a group, allowing you to get your NTFS and other permissions properly reassigned to groups.

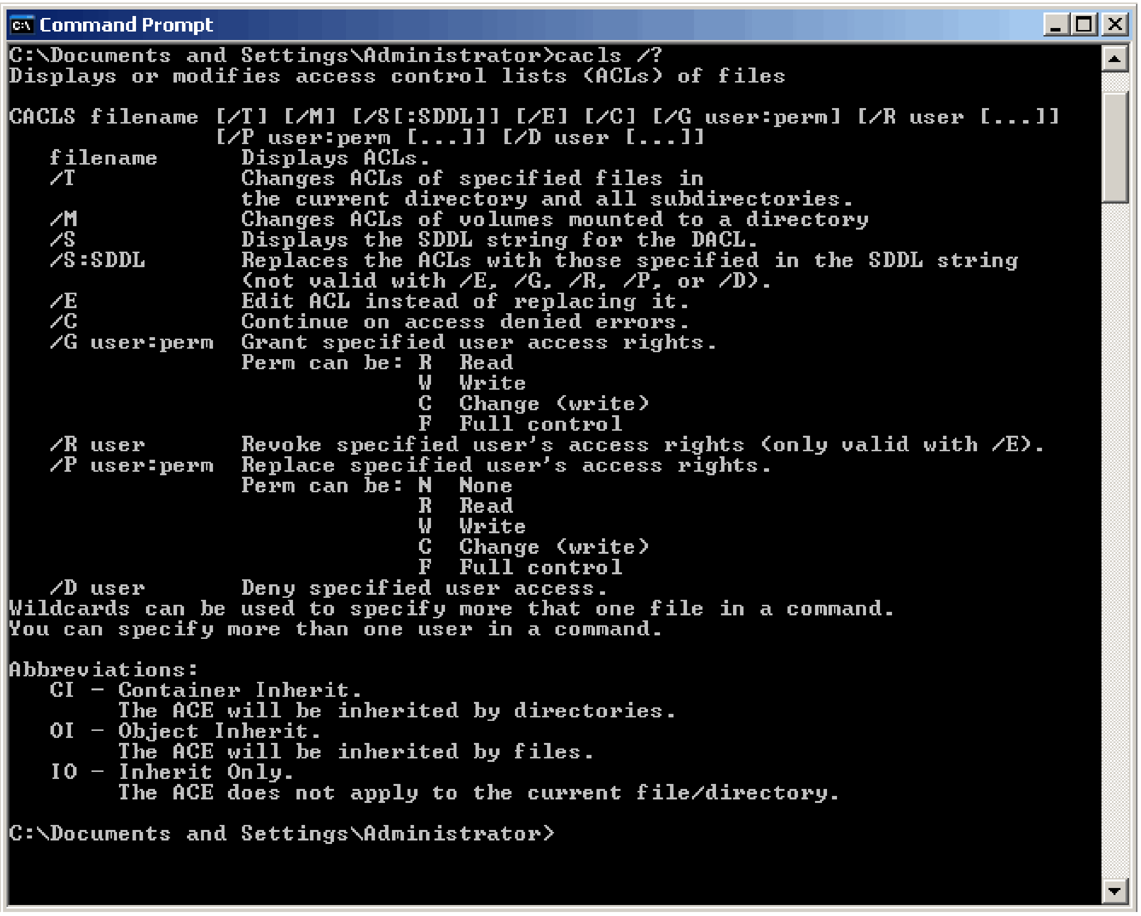
Companies that make tools with these capabilities include ScriptLogic, which offers Security Explorer and Enterprise Security Reporter (ESR). In addition, Quest Software offers Quest Reporter, which includes share permission reporting from a centralized database, similar to the way in which ESR works. Companies such as BindView and NetIQ also offer solutions that ease enterprise-level file and folder permissions management. All of these solutions are intended to help make permissions management clearer and easier so that you can get the right permissions on the right files and folders. Of course, once you have the right permissions in place, the trick lies in *keeping* them right.

Maintaining Proper File Permissions

Understanding how to properly maintain file permissions requires an understanding of how they can get messed up to begin with. Once in place, properly applied file permissions don't usually require a lot of maintenance. After all, they don't get old and stale and require occasional refreshing; file permissions stick around for the life of the file. Where permissions can get messed up, however, is when the file gets moved or copied. When moving a file to another location on the same volume, Windows will retain the file's permissions. When copying a file or moving the file to *another* volume, however, the permissions are reset to whatever permissions can be inherited from the new parent folder. This change is rarely what you want to do, however, so you will have to take special steps to ensure that file permissions remain in place.

One way to do so is to use the command-line Xcopy tool, which provides an /O command-line argument that copies file ownership and permissions. You can also specify the /X argument, which includes not only permissions and ownership but also auditing settings. Unfortunately, Xcopy can be a bit tedious if you're copying a lot of files and folders, and it's of no use when copying files and folders *between* servers.

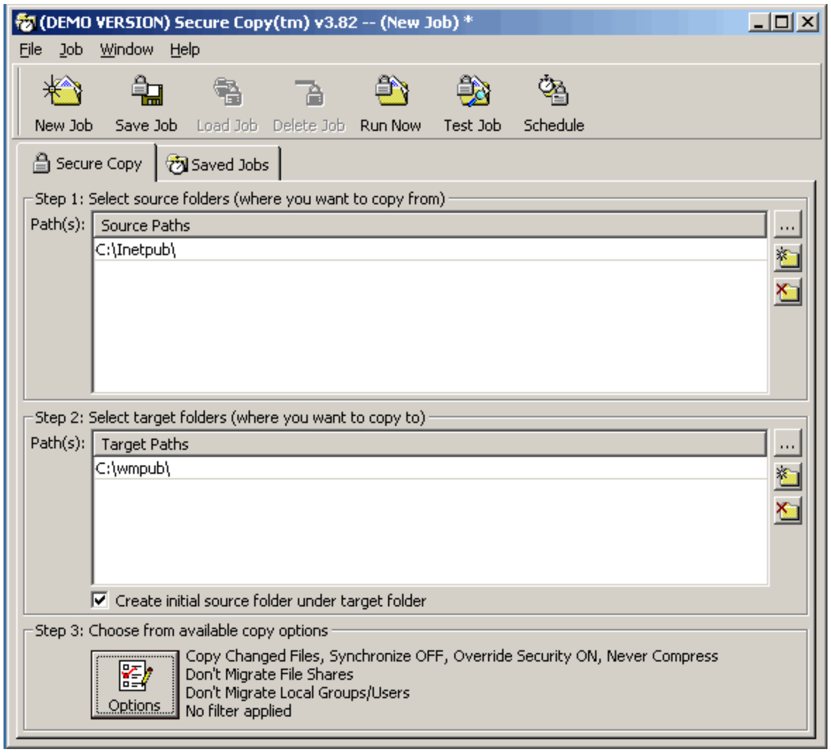
Some administrators choose not to worry about it. Instead, they just copy the files and let the permissions get messed up, then either manually fix the permissions using Windows' UI (or a third-party tool), or they use a command-line tool such as Cacls or Xcacls. Both of these tools allow you to replace or edit the file permissions on a file; Cacls—shown in Figure 5.19—is the simpler of the two.



```
C:\Documents and Settings\Administrator>cacls /?
Displays or modifies access control lists (ACLs) of files

CACLS filename [/T] [/M] [/S[:SDDL]] [/E] [/C] [/G user:perm] [/R user [...]]
               [/P user:perm [...]] [/D user [...]]
   filename      Displays ACLs.
   /T            Changes ACLs of specified files in
                 the current directory and all subdirectories.
   /M            Changes ACLs of volumes mounted to a directory
   /S            Displays the SDDL string for the DACL.
   /S:SDDL       Replaces the ACLs with those specified in the SDDL string
                 (not valid with /E, /G, /R, /P, or /D).
   /E            Edit ACL instead of replacing it.
   /C            Continue on access denied errors.
   /G user:perm  Grant specified user access rights.
                 Perm can be: R  Read
                              W  Write
                              C  Change (write)
                              F  Full control
   /R user       Revoke specified user's access rights (only valid with /E).
   /P user:perm  Replace specified user's access rights.
                 Perm can be: N  None
                              R  Read
                              W  Write
                              C  Change (write)
                              F  Full control
   /D user       Deny specified user access.
Wildcards can be used to specify more that one file in a command.
You can specify more than one user in a command.

Abbreviations:
   CI - Container Inherit.
        The ACE will be inherited by directories.
   OI - Object Inherit.
        The ACE will be inherited by files.
   IO - Inherit Only.
        The ACE does not apply to the current file/directory.

C:\Documents and Settings\Administrator>
```

Figure 5.19: Using the Cacls command-line tool.

And, simple as it is, Cacls is actually pretty complicated and somewhat limited in what it can do. Xcacls is more flexible and capable, but its command-line syntax is *really* complex. The bottom line is that, while both tools do a great job, they're both pretty tough to use (I always have to look up some examples before using them) and they're easy to make mistakes with. Enter a third-party tool to make the task a bit easier. As Figure 5.20 shows, a third-party tool lets you specify multiple files and folders to copy. By default, it copies permissions, auditing entries, and everything else, making the copy a simple operation whether you're copying files to a new location on the same server or to an entirely different server.



Step 1: Select source folders (where you want to copy from)

Path(s): Source Paths

C:\Inetpub\

Step 2: Select target folders (where you want to copy to)

Path(s): Target Paths

C:\wmpub\

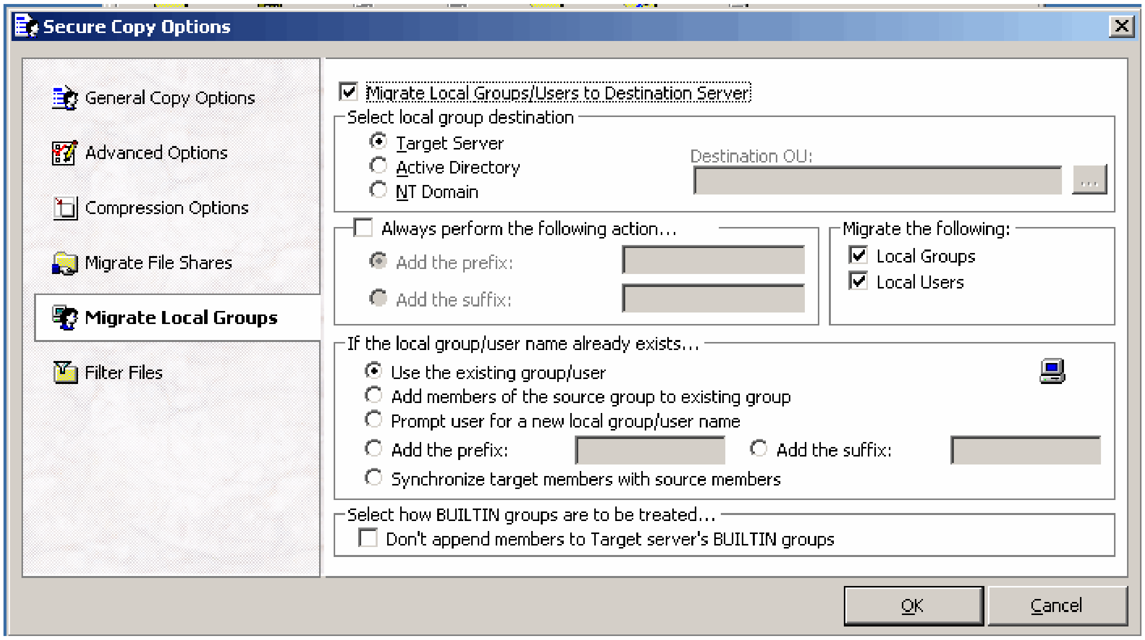
☑ Create initial source folder under target folder

Step 3: Choose from available copy options

Copy Changed Files, Synchronize OFF, Override Security ON, Never Compress
Don't Migrate File Shares
Don't Migrate Local Groups/Users
No filter applied

Figure 5.20: Using ScriptLogic Secure Copy to copy files.

One problem you can run into when copying files between servers, however, is the possibility that a user group that has permissions on the original server doesn’t exist on the target server. If you’re following one version of permissions-assignment best practices—that is, assigning permissions to servers’ *local* groups, and placing domain user groups into those local groups—this practice creates problems when copying files across servers. A third-party tool can deal with this problem by first checking to see whether the group exists on the target server and then, if you desire, creating it for you if it doesn’t exist (see Figure 5.21).



☑ Migrate Local Groups/Users to Destination Server

Select local group destination

● Target Server
○ Active Directory
○ NT Domain

Destination OU:

□ Always perform the following action...

● Add the prefix:
○ Add the suffix:

Migrate the following:

☑ Local Groups
☑ Local Users

If the local group/user name already exists...

● Use the existing group/user
○ Add members of the source group to existing group
○ Prompt user for a new local group/user name
○ Add the prefix: ○ Add the suffix:
○ Synchronize target members with source members

Select how BUILTIN groups are to be treated...

□ Don't append members to Target server's BUILTIN groups

Figure 5.21: Migrating local groups and users to the destination server.

Obviously, this difficulty is one reason I prefer to simply always assign permissions directly to domain user groups (which is really the best practice; assigning to local groups is often either a misunderstanding of the domain-best best practice or a political necessity often based on departmental, rather than central, control of a file server). Once you've gotten file copying fixed—that is, you're able to routinely copy files as needed without losing their permissions—you'll have closed the loop on file server management, helping to ensure a more secure Windows enterprise.

Summary

File serving is one of the most common uses of Windows in any enterprise, making file servers worth special attention when it comes to security. This chapter covered how to make file permissions management easier and more efficient as well as how to keep file permissions intact during routine file maintenance and copying. I've discussed the role of storage management in helping to make file servers more secure, and we've explored key techniques that can help protect file servers from attacks. You'll see many of these concepts again in the next chapter, applied more broadly (and covered in more detail) to securing Windows servers in general.

Content Central

Content Central is your complete source for IT learning. Whether you need the most current information for managing your Windows enterprise, implementing security measures on your network, or deploying new enterprise software solutions, Content Central offers the latest instruction on the topics that are most important to the IT professional. Browse our extensive collection of eBooks and video guides and start building your own personal IT library today!

Download Additional eBook Chapters!

If you found this eBook chapter to be informative, please visit Content Central and download other eBook chapters from this publication. If you are not already a registered user of Content Central, please take a moment to register in order to gain free access to this and many other great IT eBooks and video guides. Please visit: http://www.realtimepublishers.com/contentcentral/.