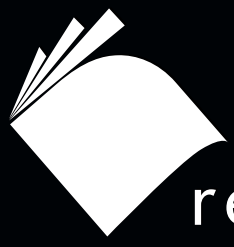


realtimepublishers.com™

The Definitive Guide™ To

Windows 2003 Storage Resource Management

VERITAS™

Evan Morris

Copyright Statement

Chapter 2: Analyzing Your Storage

In Chapter 1, we took a quick look at Windows Server's storage offerings. In this chapter, I'll show you how to make the most of the new WS2K3 product using the built-in features and a healthy portion of resource kit and support tools to analyze your storage requirements. There are many new tools and they are often free for download, so I'll show you where to get them and what they do.

In addition, I'll discuss the *process* of analyzing your current storage environment. First, detailing the levels or hierarchy of auditing: organization, network, domain, servers, storage systems, shares, folders, and files. I'll then provide templates for the types of information that you'll want to gather, including determining storage utilization (used and available disk space) and identifying the storage users.

Finally, we'll explore what you can and can't do with Windows Server's native analysis tools, such as Performance Monitor, as well as with tools in the Windows Server resource kit. We'll set the stage for taking a first-hand look at the need for third-party SRM tools to show how they can improve the audit process and prepare you for the next phase—planning your SRM deployment.

Phase 1: Analyzing Storage Requirements

Analyzing storage requirements is an ongoing process, especially in a dynamically changing environment. Table 2.1 shows this phase in the overall SRM deployment methodology. The first step in the analysis process will be to take a snapshot of where you're at today. The next step will be to perform a *gap analysis* to determine where you want to be and what's missing.

Phase	Process	Storage Resource Management
Analyze	Gather usage information	How storage is being used—What types of information are being stored and where. Is storage space and performance adequate? Prepare to use storage reporting tools to gather this information.
	Gather business information	Understand the need for storage at the business level—not just for file sharing but also for collaboration on business functions.

Table 2.1: Phase 1 of an SRM deployment methodology.

The challenge is that SRM is a moving target. You must observe and take time to gather information about the current situation before you can take action. So start your SRM deployment by printing out some storage analysis reports and taking them with you to your next extra-long meeting. Spend some extra time observing and asking whether the actions that you intend to take are really the best possible.

Storage Analysis Activities

The following list defines the activities that your storage analysis will entail:

- Gather storage tools—Why start gathering information before you know which tools are available? For example, I'll list some inexpensive resource kit utilities, but if your company has already purchased an SRM product, you'll be much better off using that. Prepare to use the storage reporting tools to gather information.
- Gather storage-management information—In addition to knowing which tools are being used, determine which storage-management processes have already been established. How can you tap into those processes rather than reinvent them?
- Gather storage information—Which types of storage are available and in what quantity? What are the storage devices and how are they configured? What are the storage applications commonly in use?
- Gather storage-usage information—How is storage being used? What types of information are being stored and where? Where are the hot spots in which you're running out of room and cold spots in which you have excess capacity? Identify the storage space that isn't being used to its full potential.
- Gather user-usage information—Identify the users, groups, and departments that are using storage and how they're using it. This activity is usually a requirement when performing charge-back analysis to bill users or departments for the cost of providing the storage resources (including administration in addition to hardware). Nevertheless, it is a foundation of storage management to understand how storage is being consumed.
- Gather performance information—Is the storage performance adequate? Where does it need to be improved? Identify current hardware configurations to determine which configurations need to be refreshed or phased out. In addition, analyze the environment to ensure that it can support newer technologies such as NAS.
- Gather data-protection information—Is the data adequately protected against hardware faults, operator error, malicious intent, physical access, natural disaster, and so on? Identify which forms or techniques of data protection are in use. Identify business-critical and even mission-critical data and how it is protected.
- Gather business information—What types of storage benefit the business? Try to understand the need for storage at the business level; that is, not just for file sharing but also for collaboration on business functions and workflow. Are there limitations in the storage or applications that can be addressed to improve storage functionality?

Storage Analysis Goals

Despite the many possible types of information you can gather, I prefer to keep this phase of an SRM deployment simple. Doing so makes your chance of success much greater. That said; let's keep the following goals in mind for an SRM deployment:

- Reduce the cost of ownership—Reduce capital expenditures for new hardware as well as the cost of managing storage resources. Part of this goal includes the effort of server consolidation, reducing the number of systems that need to be managed. You can accomplish this goal only by making the larger, consolidated systems easier to administer with the same or fewer resources. By managing storage effectively, you also reduce the effort and cost associated with maintaining files that don't need to be part of your critical data-protection strategy (fault-tolerant hardware and backup). The sum of these costs is known as the total cost of ownership (TCO).
- Improve end-user experience—Improve both the perception of performance and system availability. Although this goal isn't directly quantifiable, the SRM deployment should provide some assistance in making users' daily tasks easier to accomplish rather than interfere with their business functions and make their lives miserable.
- Improve protection of business-critical and mission-critical data—This goal ties in directly with the TCO, as a hit to storage-system availability can have a devastating effect on business profit and loss.
- Develop a sound organizational policy—Out of an SRM-deployment effort, you should gain a well-developed policy that defines storage best practices for your organization.
- Develop qualified personnel—Let's not forget that the SRM-deployment process will let you identify the necessary tools to proactively manage storage resources, and it will give employees knowledge about how to accomplish SRM. Also, administrators will become aware of storage-management solutions and tools and how to use them.

Levels of Auditing

Now that you know what type of information you need and why, you can take action. As you pick up the technical details of the SRM-deployment process, be sure to relate them back to the business environment.

The different levels, or hierarchy, of auditing include the organization, network, servers, storage subsystems, domains, users and groups, shares, machine accounts, OSs, storage applications, logical drives, folders, controllers, interconnects, physical disks, and files, as Figure 2.1 shows. To start organizing your collection of information, let's start at the top—the organizational level.

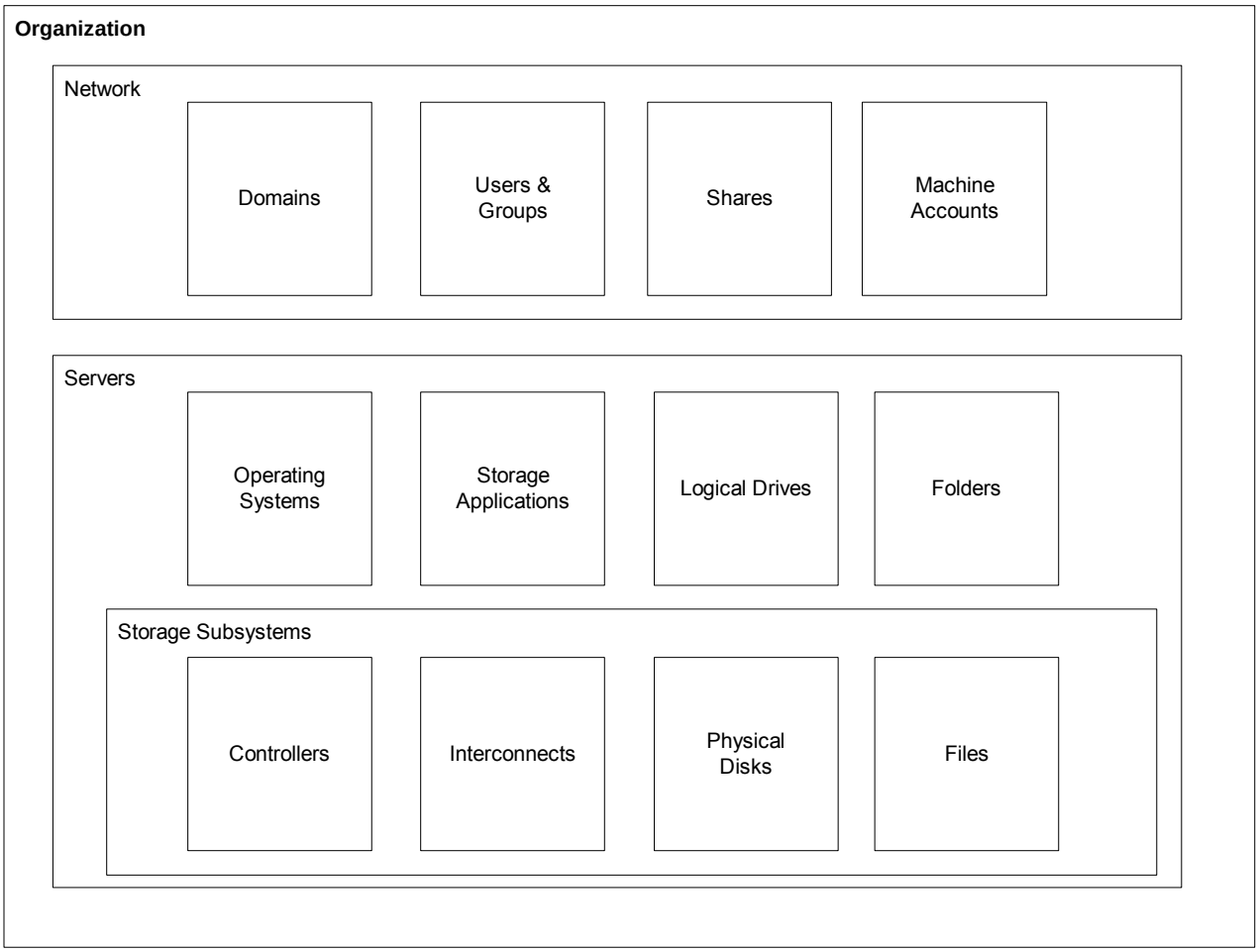


Figure 2.1: Levels of auditing.

Most organizations consist of many pools of storage as well as a variety of directory services. In the NT world, you have any number of domains that can contain storage resources. The idea behind AD is to centralize the directory services and publish storage resources, such as file shares, in the directory. You'll see later how well this system works (or doesn't work), but for now, you'll most likely need to deal with groups, users, and server accounts that aren't integrated into a single directory. You might also deal with other OSs and storage applications, but for this guide, I'll focus on Windows Server storage applications.

The storage subsystems layer contains storage controllers, storage interconnects, physical disks and their logical representation, and the folders and files on those disks. Your method of accessing this information is most likely dependent on the equipment vendor or manufacturer; that is, there is such a variety of hardware-specific information that you'll require a reporting tool from the server or storage maker. There are a few products available for managing SAN equipment that attempt to report on all devices in the SAN, but this task is difficult. For the information to be specific enough to be of value, it typically must come from the hardware manufacturer. For the purpose of SRM, our concern is the presentation and usage of the storage resources at a higher level—as storage from which the end-user can benefit. This storage is typically in the form of shares, folders, and the files they contain, as Figure 2.1 illustrates.

Types of Audit Information

There is quite a wide variety of information that you can acquire from a storage audit, and it corresponds to the levels of auditing. You can identify who the storage users are in your organization and can audit file and folder access at the server level. You can perform security auditing to make sure that file and folder access is set properly and is being used as planned. This type of network audit has become increasingly important as we have been hit by viruses that take advantage of network share permissions allowing write access to unauthenticated users (for example, the Everyone group).

You can conduct a performance analysis to measure how well your storage systems are performing at different levels. You can also gather information such as the level of data protection (for example, RAID and other fault-tolerance measures) and whether backups are completing successfully. For SRM, we're most interested in assessing disk space used and available (storage utilization) on both a per-server and per-user or group level, and we'll take an in-depth look at how to use certain tools to accomplish this mission.

Auditing File and Folder Access

WS2K3 makes auditing file and folder access on NTFS volumes fairly easy. First, you or another member of the Administrators group define which files and folders, whose actions, and what types of actions to audit. In WS2K3, auditing is enabled through Group Policy, as Figure 2.2 shows. (To navigate to this Group Policy console, select Start, Programs, Administrative Tools, Local Security Policy.) As you can see, the Group Policy interface for auditing is much simpler in WS2K3 than it was in Win2K, in which you had to expand several levels.

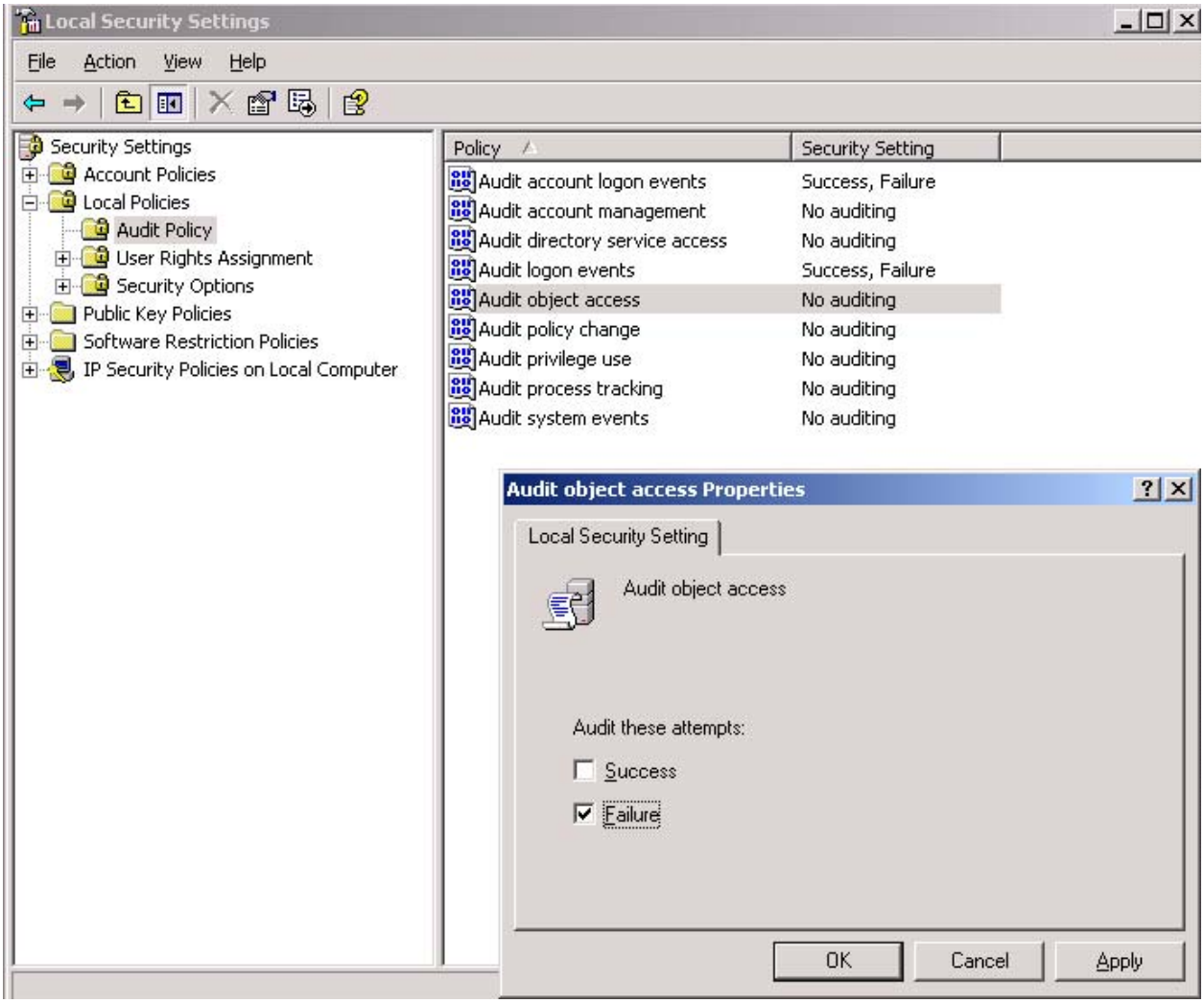


Figure 2.2: Enabling auditing for object access in WS2K3.

Once the auditing policy is enabled, you can then apply it to specific folders and files using the Windows Explorer interface. An entry is then written to the Event Viewer Security Log whenever the file or folder matching your criteria is accessed. Then another entry is written to the Security Log, and then another, and so on.

The problem is that this type of information can create overload fairly easily unless used carefully. For example, auditing successful file access can indicate normal business usage, which can occur quite frequently. Instead, what you should be looking for are the rare occurrences of failed file or directory access attempts, which might signal a problem. Let's explore the tools you can use to help you accomplish this task.

Storage Tools

In this section, we'll look at the tools that you can use to manage—including analyze—your storage, starting with the tools that you've already paid for: the tools included in Windows Server, including both the graphical consoles and the powerful command-line utilities.

Native Windows Server Tools

Some useful tools are available immediately when you install WS2K3. These tools had previously been available only for purchase as resource kit utilities or for download (sometimes only within Microsoft). Most of the built-in tools will be listed when you type

```
HELP
```

at a command prompt, although there are a few exceptions, such as Eventcreate (discussed later). The best starting point for Windows Server storage auditing is to see what the built-in tools—such as Performance Monitor and the Computer Management console—are capable of.

File Server Management MMC

As Figure 2.3 shows, the Manage Shared Folders MMC is different than the one in Win2K. In the WS2K3 version, there are task commands that can be launched by a single mouse-click, including the new task, Configure Shadow Copies. You can access this console by selecting Start, Run, and typing

```
filesvr.msc
```

Alternatively, if you have configured the file server role in the Manage Your Server Wizard, you will see this console available from the Administrative Tools menu. (Note that Fsmgmt.msc brings up the simpler Shared Folders MMC).

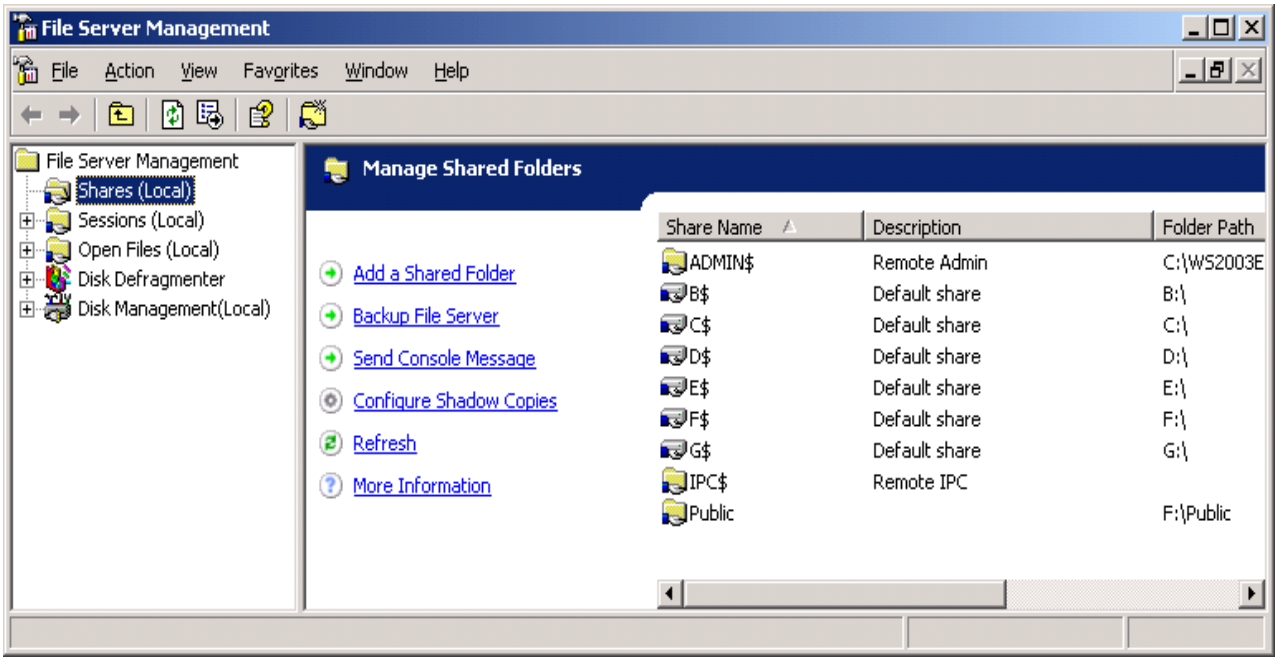


Figure 2.3: The Manage Shared Folder MMC in WS2K3 Administrative Tools.

As you use the Manage Shared Folders MMC in WS2K3, you might notice changes in the default security permissions. As Figure 2.4 shows, the new default permissions no longer allow write access to unauthenticated users (for example, the Everyone group). This security setting is a result of the recent viruses that have taken advantage of network share permissions.

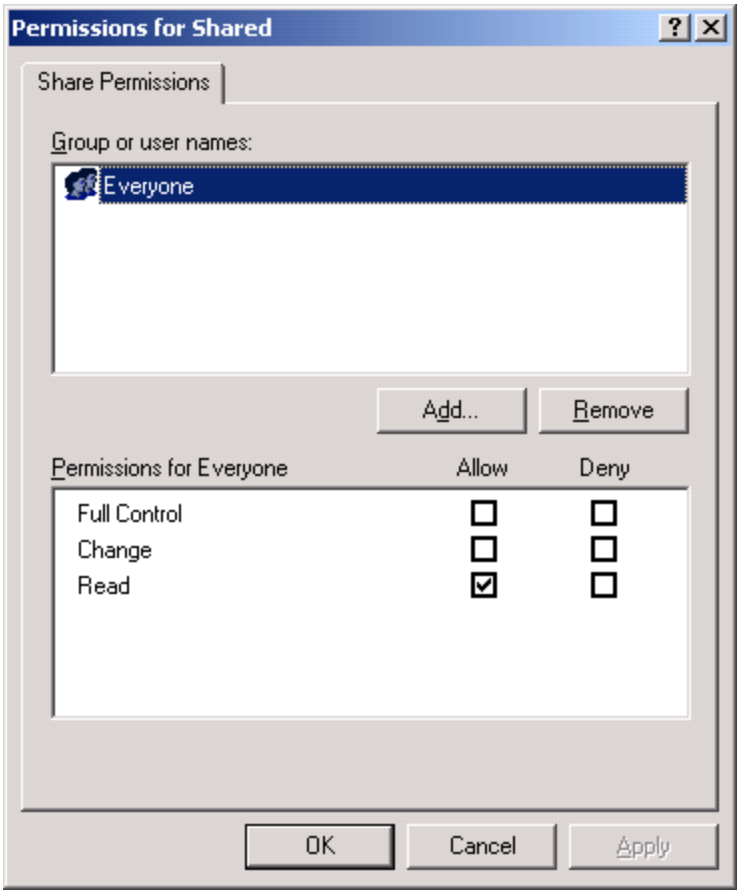


Figure 2.4: WS2K3's default network share permissions.

The Logical Disk Manager provides the Disk Management view that Figure 2.5shows. This Disk Management view of drive information includes important information about unallocated storage. The big news about WS2K3 is that the Logical Disk Manager is kinder, gentler than it was in previous versions. We'll explore the Logical Disk Manager in more detail in later chapters; for now, you should know simply that the underlying storage mounting mechanism is improved in WS2K3. One of the big improvements of Win2K over NT 4.0 was how Win2K handled mounting disks without the need to reboot. WS2K3 takes a step back and says "Do you really want me to mount that disk?" The reason is to make it less disruptive and friendlier to SAN environments—it will no longer grab every disk that it sees.

Another change in WS2K3 is that the option to upgrade a basic disk to a dynamic disk is turned off by default. When you mount new disks, the Initialize and Convert Disk Wizard has only the option to write a signature selected.

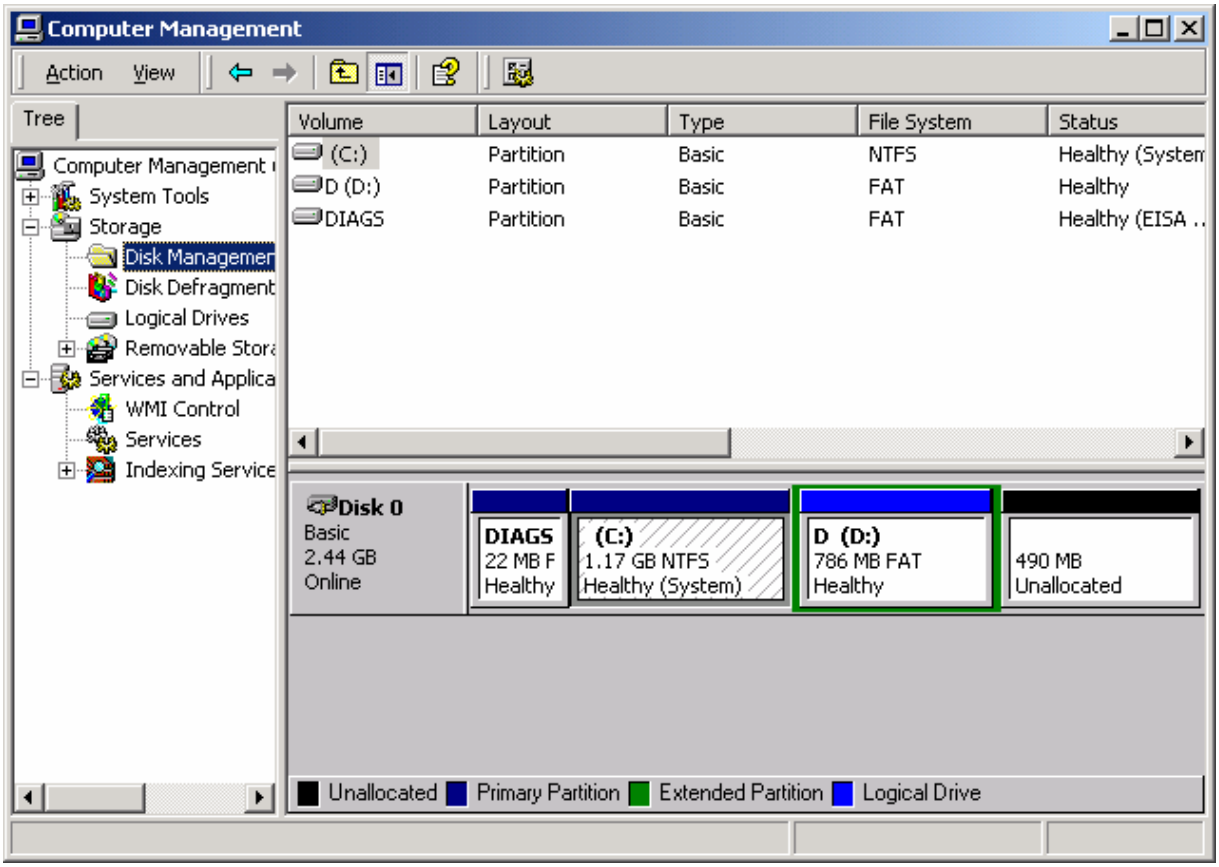


Figure 2.5: Disk Management view of drive information including unallocated storage.

The Windows Server Event Viewer performs storage management functions such as warning you when a disk is nearly full (see Figure 2.6). However, depending on the level of activity, you might already be in trouble by the time you get this message. You must be set up to get this type of message before the situation is irreparable. To do so, you need to use an application—such as Microsoft Operations Manager (MOM) or Hewlett-Packard OpenView—or a resource kit utility—such as Eventquery and Eventtriggers, discussed later—to monitor the event logs and notify you of the warning. The Windows Server tool also lacks features such as being able to configure threshold settings. Thus, in this case, the native Windows Server tool alone isn't enough.

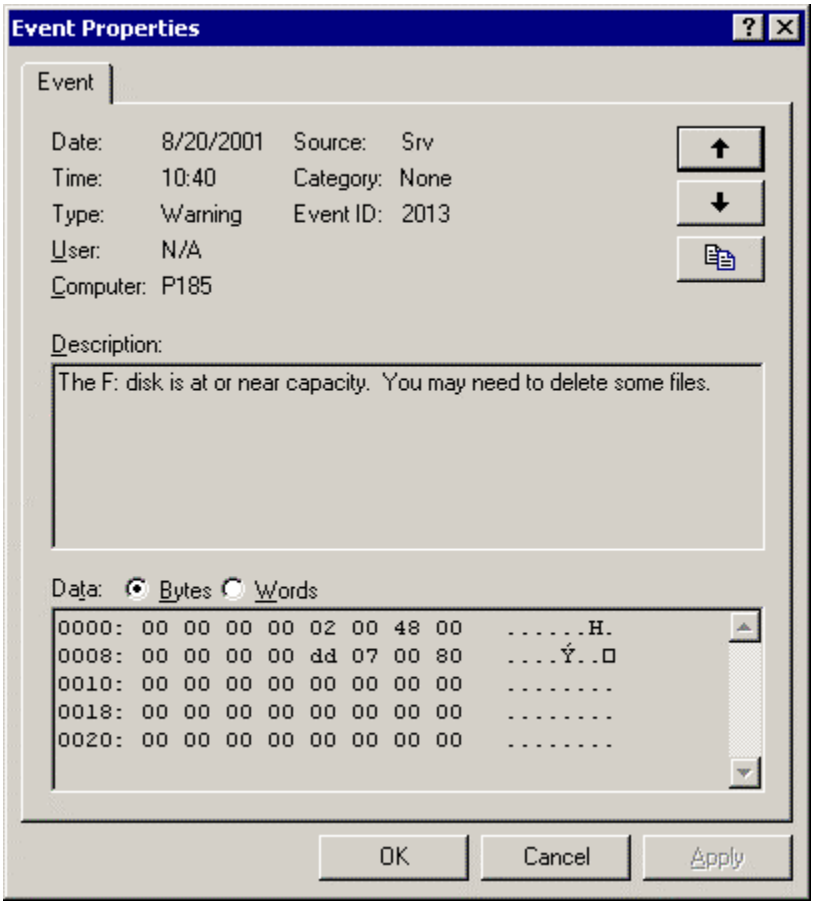


Figure 2.6: An example disk nearly full event log warning message.

Performance Monitor

Despite its name, the Windows Server Performance Monitor is designed for more than just monitoring performance. Technically, the new name for the Windows Server version of the tool is System Monitor, but it will likely always be known as Performance Monitor or PerfMon (the name of the actual executable). As Figure 2.7 illustrates, Performance Monitor can monitor the amount of free disk space on a volume or drive. As you can see, the chart view can be messy and difficult to read if you try to view too much information at once.

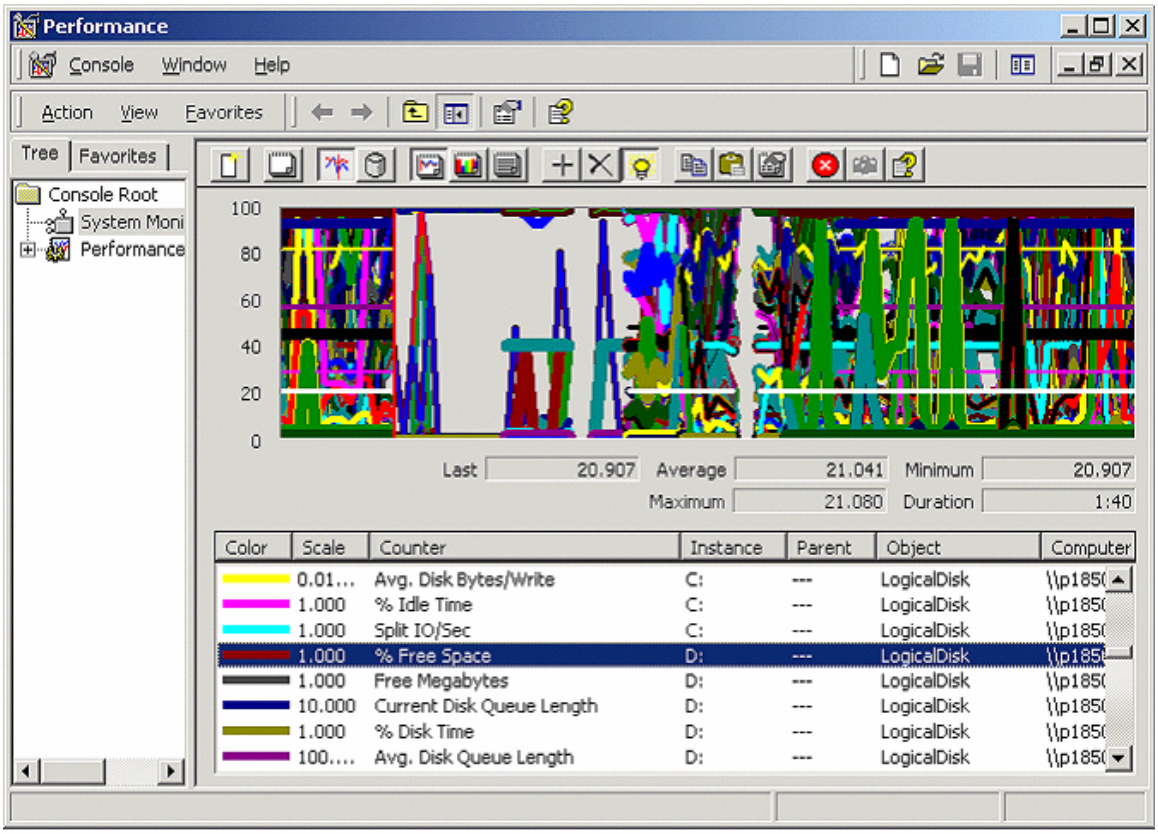


Figure 2.7: Performance Monitor chart view of % Free [Disk] Space.

When using Performance Monitor, you must know the name of the server that you want to connect with because there is no browse button. After you enter the server name, and Performance Monitor validates the name (this validation can take a bit of time), the next step is to select the object and counters to monitor, such as Current Disk Queue Length, % Disk Time, and Avg. Disk Bytes/Write. For a brief explanation of a counter, click Explain as you add the counter.

Some of the counters that Figure 2.7 shows, such as % Free Space and Free Megabytes, are more resource-management related than truly performance related. However, these counters provide useful information that you can use in your analysis. Note that the object being monitored is the LogicalDisk; however, you won't see the LogicalDisk as an object until you enable the Diskperf counters (as I explain later).

Once you add all the disk counters, you end up with a chart that is messy and difficult to read. The chart view is useful for comparing how several servers are performing for the same counter (for example, which servers have the least disk space). However, for comparing counters from different objects, the report view provides information that is much easier to read at a glance.

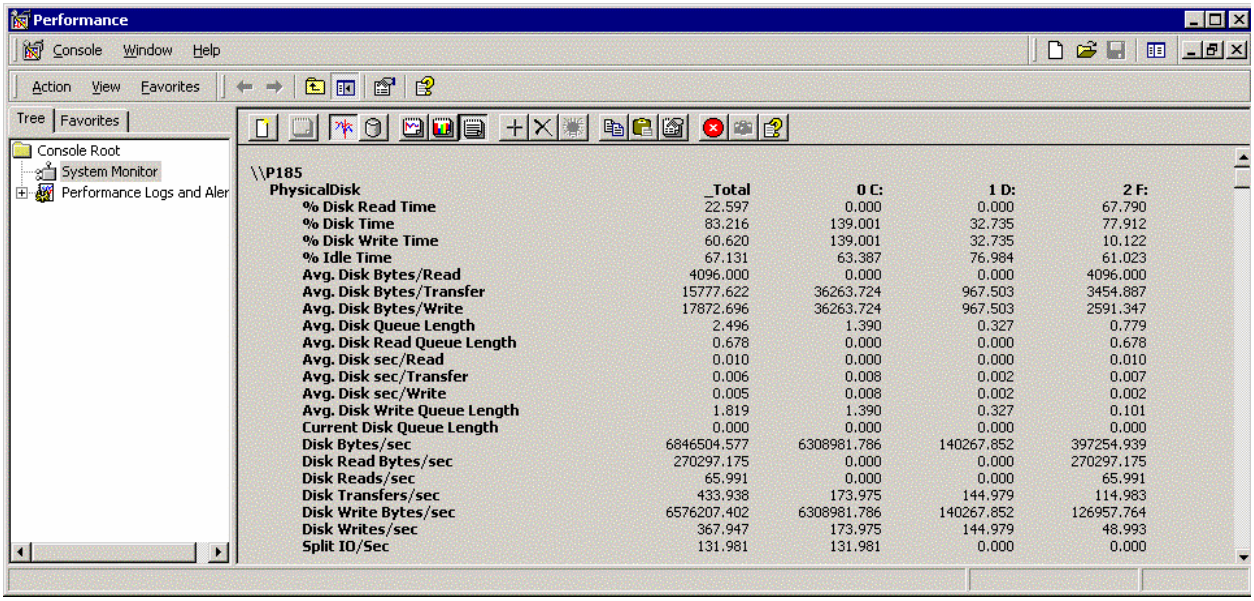
Figure 2.8 shows the report view for PhysicalDisk counters for one server. If, for example, you needed to know how much space is free on the D drive, you would look at the numbers in the middle of the screen to get that information.

> Notice that the following figure is missing the all-important LogicalDisk counters for % Free Space. To see LogicalDisk counters, I need to enable them by typing

```
diskperf -y \\computername
```

at a command prompt (you can omit the \\computername for the local computer). The option –y sets the system to start all disk performance counters when the system is restarted. In NT 4.0 and earlier, none of the disk counters are enabled by default. However, in Windows Server, the PhysicalDisk counters are enabled but not active until you start polling them using Performance Monitor.

The option diskperf –n turns off all disk counters, and the –nv option disables only the logical counter. In all cases, a reboot is required after toggling the counters. Of course, there is a very slight performance impact for monitoring the disk counters, so you might not want to leave them on all the time.



\\P185

PhysicalDisk	_Total	0 C:	1 D:	2 F:
% Disk Read Time	22.597	0.000	0.000	67.790
% Disk Time	83.216	139.001	32.735	77.912
% Disk Write Time	60.620	139.001	32.735	10.122
% Idle Time	67.131	63.387	76.984	61.023
Avg. Disk Bytes/Read	4096.000	0.000	0.000	4096.000
Avg. Disk Bytes/Transfer	15777.622	36263.724	967.503	3454.887
Avg. Disk Bytes/Write	17872.696	36263.724	967.503	2591.347
Avg. Disk Queue Length	2.496	1.390	0.327	0.779
Avg. Disk Read Queue Length	0.678	0.000	0.000	0.678
Avg. Disk sec/Read	0.010	0.000	0.000	0.010
Avg. Disk sec/Transfer	0.006	0.008	0.002	0.007
Avg. Disk sec/Write	0.005	0.008	0.002	0.002
Avg. Disk Write Queue Length	1.819	1.390	0.327	0.101
Current Disk Queue Length	0.000	0.000	0.000	0.000
Disk Bytes/sec	6846504.577	6308981.786	140267.852	397254.939
Disk Read Bytes/sec	270297.175	0.000	0.000	270297.175
Disk Reads/sec	65.991	0.000	0.000	65.991
Disk Transfers/sec	433.938	173.975	144.979	114.983
Disk Write Bytes/sec	6576207.402	6308981.786	140267.852	126957.764
Disk Writes/sec	367.947	173.975	144.979	48.993
Split IO/Sec	131.981	131.981	0.000	0.000

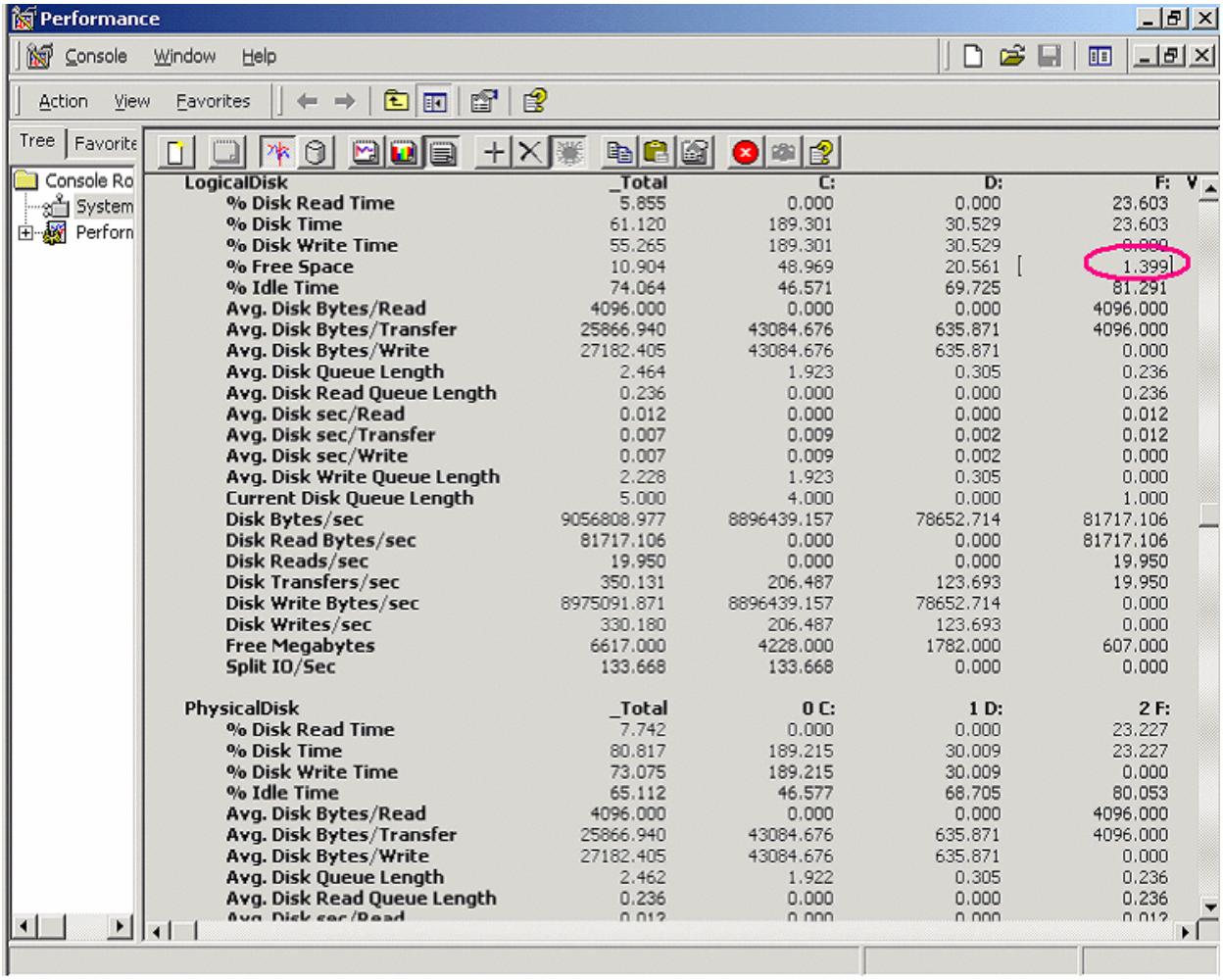
Figure 2.8: Report view of PhysicalDisk counters for a single server.

☞ If you can see the LogicalDisk object but can't add the associated counters, the problem might be that diskperf –y was set but the server wasn't rebooted.

In Win2K, to gather Performance Monitor information on one computer from another, you need to configure the Performance Logs and Alerts service (which has a short name of SysMonLog) with credentials at the domain level. By default, the Performance Logs and Alerts service is configured with the LocalSystem account, which means that it will be unable to gather performance information from remote computers. When you add the desired account and click OK, the tool will present a message stating that the account will be granted the *Log On As A Service* right, which saves you the step of performing that task manually.

By default WS2K3 adds credentials (the NT Authority\NetworkService account) that allow the service to access remotely over the network. If you check your WS2K3 Performance Logs and Alerts service, you will see that the change has already been made for you. The NetworkService account presents the computer's credentials to remote servers with a token containing the security IDs (SIDs) for the Everyone and Authenticated Users groups. Oddly, Windows XP still uses the Local System Account for log on when starting the service.

Let's take a look at the Performance Monitor reports in several views; first, at the single server view of both LogicalDisk and PhysicalDisk counters. As you can see in Figure 2.9, the circled number for % Free [Disk] Space is a bit low for the comfort zone of most administrators.



LogicalDisk	_Total	C:	D:	F:
% Disk Read Time	5.855	0.000	0.000	23.603
% Disk Time	61.120	189.301	30.529	23.603
% Disk Write Time	55.265	189.301	30.529	0.000
% Free Space	10.904	48.969	20.561	1.399
% Idle Time	74.064	46.571	69.725	81.291
Avg. Disk Bytes/Read	4096.000	0.000	0.000	4096.000
Avg. Disk Bytes/Transfer	25866.940	43084.676	635.871	4096.000
Avg. Disk Bytes/Write	27182.405	43084.676	635.871	0.000
Avg. Disk Queue Length	2.464	1.923	0.305	0.236
Avg. Disk Read Queue Length	0.236	0.000	0.000	0.236
Avg. Disk sec/Read	0.012	0.000	0.000	0.012
Avg. Disk sec/Transfer	0.007	0.009	0.002	0.012
Avg. Disk sec/Write	0.007	0.009	0.002	0.000
Avg. Disk Write Queue Length	2.228	1.923	0.305	0.000
Current Disk Queue Length	5.000	4.000	0.000	1.000
Disk Bytes/sec	9056808.977	8896439.157	78652.714	81717.106
Disk Read Bytes/sec	81717.106	0.000	0.000	81717.106
Disk Reads/sec	19.950	0.000	0.000	19.950
Disk Transfers/sec	350.131	206.487	123.693	19.950
Disk Write Bytes/sec	8975091.871	8896439.157	78652.714	0.000
Disk Writes/sec	330.180	206.487	123.693	0.000
Free Megabytes	6617.000	4228.000	1782.000	607.000
Split IO/Sec	133.668	133.668	0.000	0.000

PhysicalDisk	_Total	0 C:	1 D:	2 F:
% Disk Read Time	7.742	0.000	0.000	23.227
% Disk Time	80.817	189.215	30.009	23.227
% Disk Write Time	73.075	189.215	30.009	0.000
% Idle Time	65.112	46.577	68.705	80.053
Avg. Disk Bytes/Read	4096.000	0.000	0.000	4096.000
Avg. Disk Bytes/Transfer	25866.940	43084.676	635.871	4096.000
Avg. Disk Bytes/Write	27182.405	43084.676	635.871	0.000
Avg. Disk Queue Length	2.462	1.922	0.305	0.236
Avg. Disk Read Queue Length	0.236	0.000	0.000	0.236

Figure 2.9: Single server with LogicalDisk counters for % Free Space circled.

The key is that the report view makes it much easier to review multiple counters of information at a glance. Figure 2.10 shows another example through the multiple server view of LogicalDisk counters.

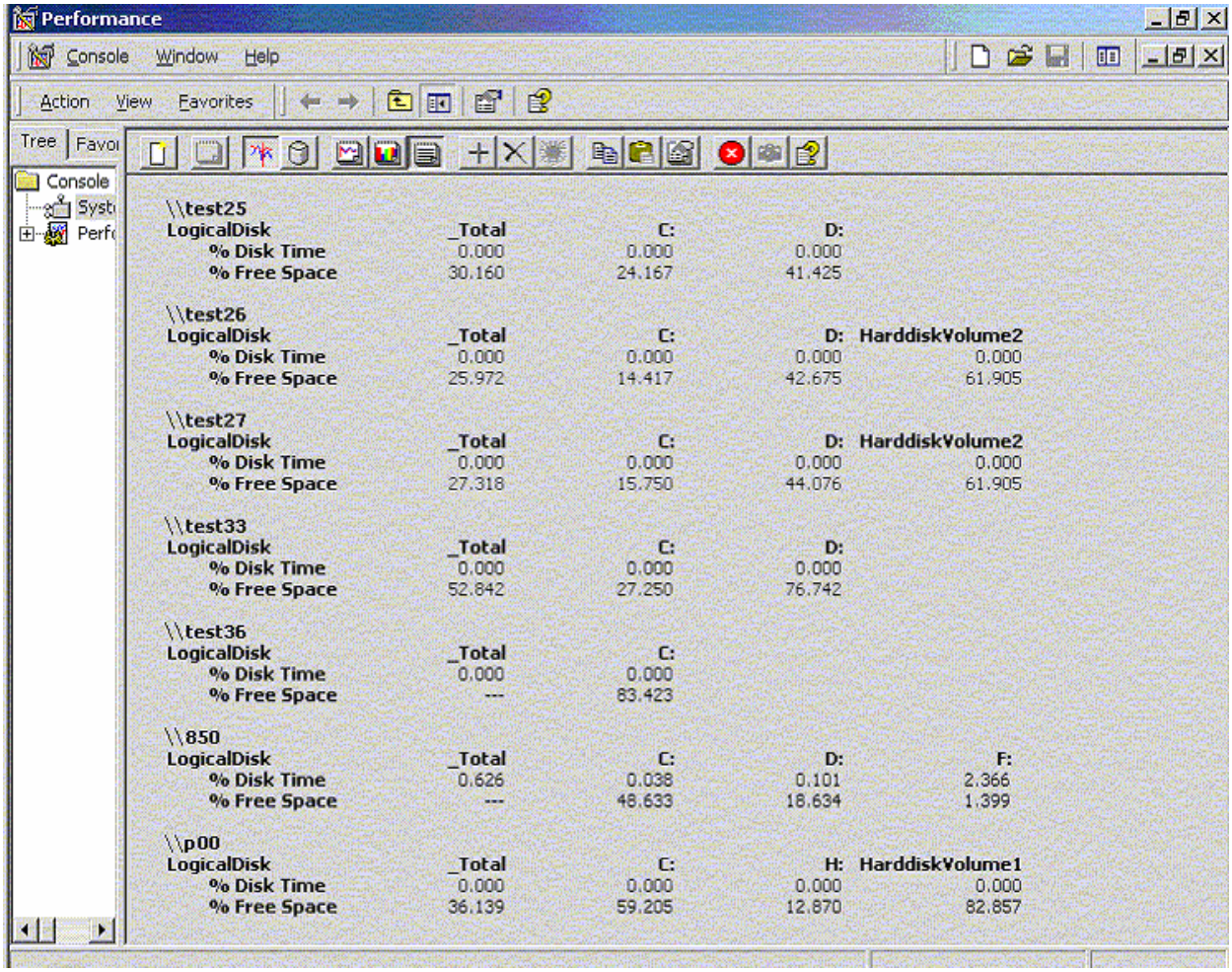


Figure 2.1: Multiple server report of LogicalDisk counters.

In Figure 2.10, you might notice that the % Free Space counter shows no value under some counters. The reason is that the counter wasn't selected for that computer. Although adding counters for multiple systems can be a tedious process, you will benefit from learning how to edit the Performance Monitor settings files. To do so, simply right-click in the monitoring area of the console, and select Save As from the resulting menu. This action will create an HTML file. Next, edit the HTML (you can use a program as simple Notepad), and add servers or replace the current server name with a new one, then save the file with a new name. When you want to start capturing or logging performance data, simply right-click in Performance Monitor, select New Log Settings From, and open the .htm file you just created.

> ☞ Does the % Free Space counter really provide useful information? What good does 20 percent free space on each of five partitions do you? To gain more from the information provided, you could use volume mount points to combine them under one share. We'll explore this solution in detail later.

File Properties

Have you ever saved a downloaded file only to return to it weeks or months later with no idea what the file was for or what the application did? Have you ever wondered where you downloaded the file in the first place because you could not find it by searching the Internet? You can make use of the file metadata information (stored in the properties fields) and store the relevant information in the Summary Properties, as Figure 2.11 shows. This figure provides an example of a file that is somewhat difficult to find and that has a somewhat misleading name (VCD commonly stands for Video Compact Disc). Although difficult to find, this tool is a very handy utility that I can now recognize using file properties.

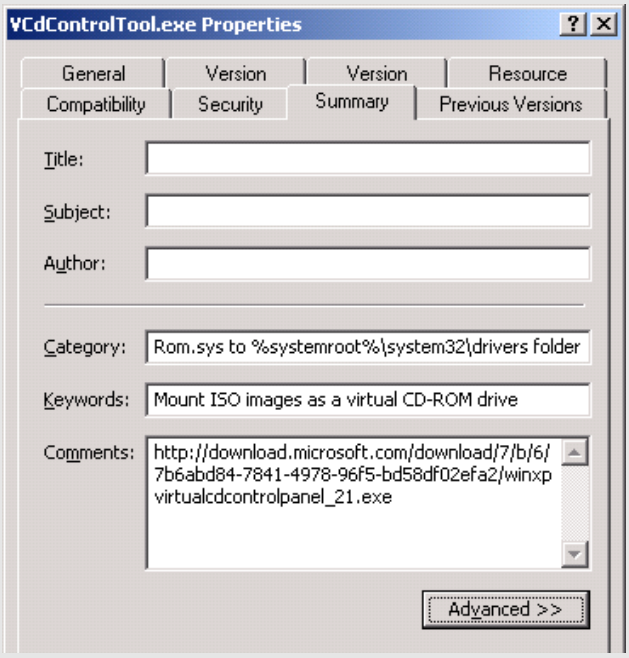


Figure 2.11: Using file properties to store metadata information.

Figure 2.12 illustrates a simple change in applying file properties in either Windows XP or WS2K3. This dialog box reflects the fact that Microsoft is responding to feedback about the need to make its OSs easier to use. When you are changing file properties, the default option is now to *Apply changes to this folder, subfolders and files*. How often do you copy files from a CD-ROM (without using Xcopy, which would reset the read-only bit) or want to compress an entire subfolder tree? With this slight change, it is much easier to administer larger numbers of files. I remember in the NT days, you had to run a search without any specific criteria (essentially for *.*) just to highlight all files and apply the same properties (or attributes).

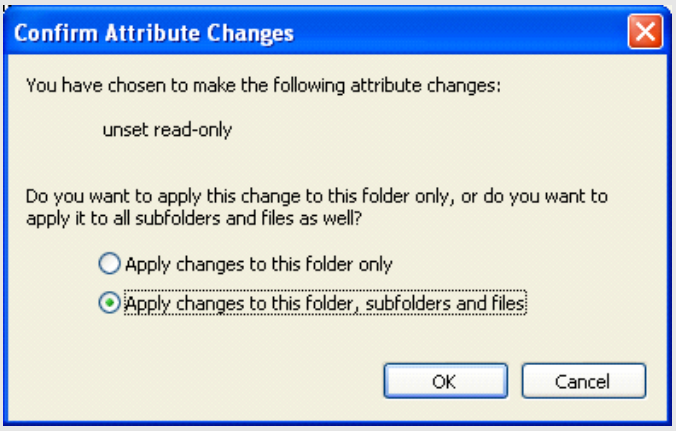


Figure 2.12: The default option in Windows XP and WS2K3 is to apply changes to subfolders.

Storage-Management Utilities

The following Windows Server utilities will make disk and storage management easier. These utilities are available for download and installation; you simply need to know where to find them. In addition, the new WS2K3 product ships with many additional command-line tools and utilities that were previously available only in the resource kits. Many of these utilities are disk- and storage-related.

Here comes the good stuff: the powerful tools that remain hidden until you discover them, perhaps by reading this chapter. I'll run through these utilizes alphabetically, weaving in related tools as they become applicable. I hope that you will be impressed by what you find here.

You must be logged on as an Administrator or a member of the local Administrators group to use these utilities. Ideally, use Run As to escalate your privileges to this level only when necessary. For example, because Run As works on executables, I find it easiest to bring up a command prompt as Administrator, then launch compmgmt.msc (the computer management console, which I can then use to add an account to the local administrators group if necessary). Simply right-click on the Start menu item Command Prompt, which is found under Accessories.

DiskPart

You can use DiskPart to manage disks, partitions, and volumes, including the all-important extending of volumes (for example, volumes that are grown through storage virtualization on a SAN). DiskPart runs in interactive mode, essentially bringing up its own command line. For example, you would enter

```
diskpart
```

then enter

```
list volume
```

to make sure you are operating on the correct volume. Next you would enter

```
select volume #
```

where # is the volume number. Then you would enter

```
extend size (MB)
```

and finally

```
exit
```

When you receive a message that DiskPart successfully extended the volume, your new space is added to the existing drive while disrupting the data already on the volume.

You can use DiskPart only to extend volumes that were created on a dynamic disk. If the disk was originally a basic disk when the volume was created and then converted to a dynamic disk, you will receive an error and DiskPart will fail.

DiskPart lets you manage disks, for example, by extending a disk volume while the storage is online to the OS. DiskPart is fully scriptable, using the syntax

```
Diskpart /s <script>
```

Figure 2.13 shows the commands for using DiskPart. This utility is also useful for rescanning the server to detect any devices that have been presented from a SAN. For example, after breaking off a Business Continuance Volume (BCV—such as a clone) and presenting it to the host, you can use DiskPart to detect the new drive and mount it.

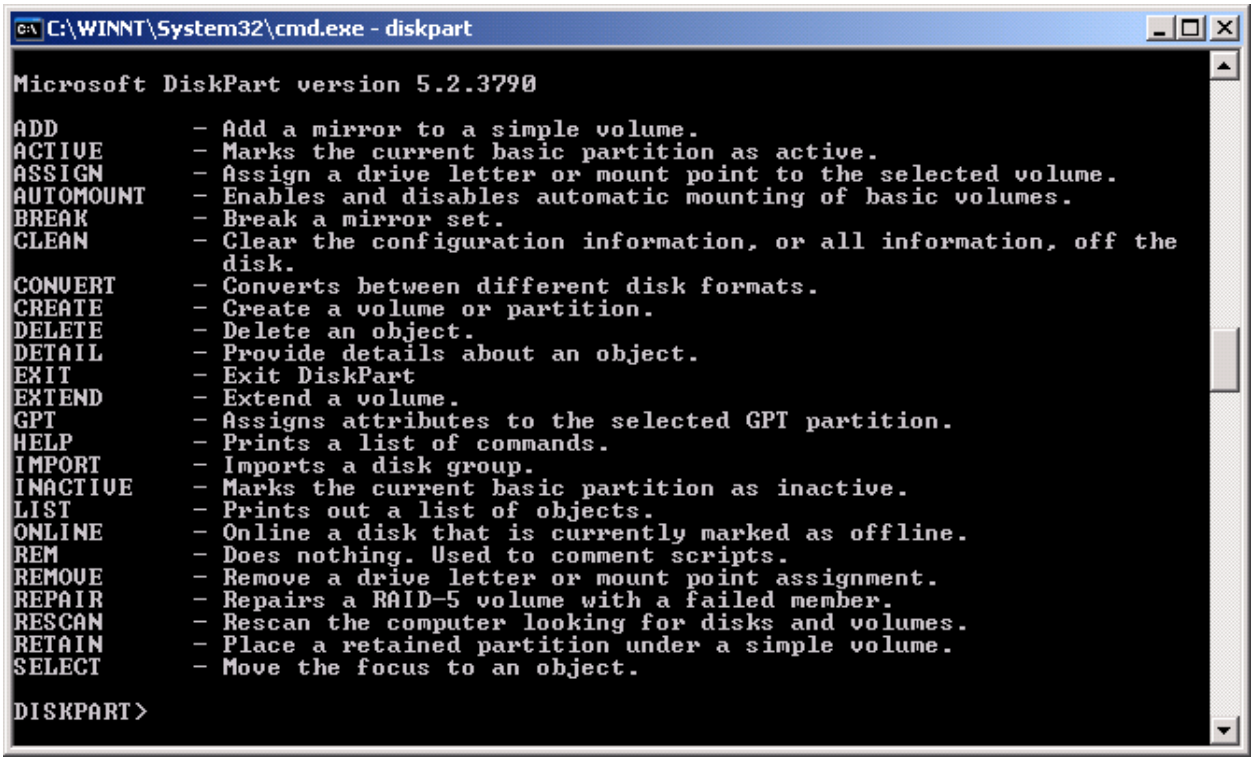


Figure 2.13: DiskPart commands for managing a disk volume (WS2K3 version).

DiskPart is available for Win2K both by download and as part of the Recovery Console as well as in the default installation of Windows XP and WS2K3. Make sure that you are using the appropriate OS version, as there are differences in how they operate (see the following note). As Figure 2.14 illustrates, in Win2K, the DiskPart command is only available when you are using the Recovery Console, so most of the benefit in a production environment for changing disks will be to WS2K3 systems.

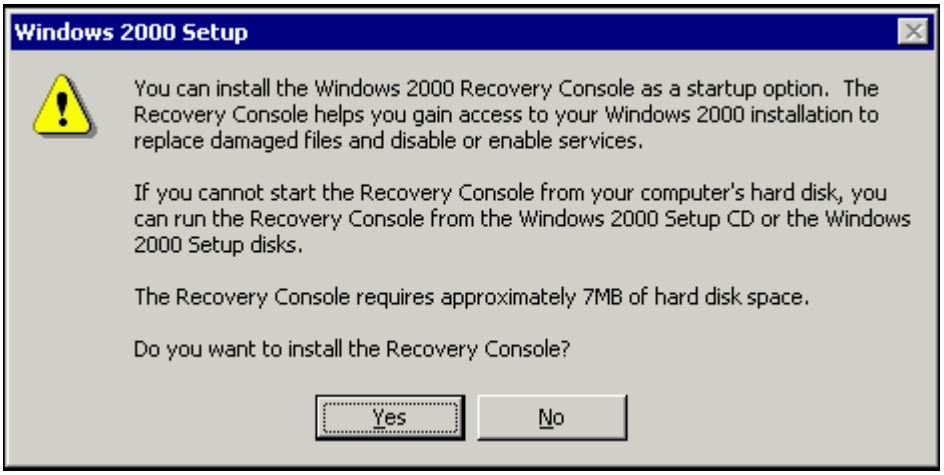


Figure 2.14: Installing the Recovery Console.

☞ To install the Recovery Console as a startup option in Win2K, insert the Win2K CD-ROM, and hold down the Shift key to prevent the CD-ROM auto-run feature from running, or wait for the auto-run feature to bring up the installation options. Close the installation wizard, run a command prompt, and type the following

```
x:\i386\winnt32.exe /cmdcons
```

where x is your CD-ROM drive letter. If you have the bits copied to disk, you can run the installation directly from the hard drive. Answer Yes to the prompt, and installation will begin.

The installation won't prompt you to reboot your system, but the Recovery Console will be available as a boot option the next time you reboot your system. The installation did not prompt me for the SP2 source location, so I recommend running the installation from a Win2K source that has had SP2 slipstreamed in (by running

```
\i386\update>update –s <dir>
```

where <dir> is the location of your Win2K source files).

DiskPart can also add or break mirrors, assign or remove a disk's drive letter, create or delete partitions and volumes, convert basic disks to dynamic disks, import disks and bring offline disks and volumes online, and convert master boot record (MBR) disks to GUID Partition Table (GPT) disks. The options under CONVERT for DiskPart are as follows:

- BASIC—Converts a disk from dynamic to basic
- DYNAMIC—Converts a disk from basic to dynamic
- GPT—Converts a disk from MBR to GPT
- MBR—Converts a disk from GPT to MBR

Just because you can run it from a command line or script does not mean that it will not destroy your data! Always test your backup before you perform these types of disk operations!

Driverquery

Another built-in utility is Driverquery, which displays a list of installed device drivers and can be run remotely against a server. This utility is useful for checking driver status, especially using the verbose mode, as the sample in Listing 2.1 shows. As you can see, the driver list is quite long (it was truncated for brevity for this example). However, Driverquery *cannot* be used for driver-management tasks such as stopping, starting, or removing.

```
Module Name  Display Name           Description            Driver Type   Start Mode State
Status     Accept Stop Accept Pause Paged Pool Code(bytes BSS(by Link Date              Path
Init(bytes

ACPI         Microsoft ACPI Driver  Microsoft ACPI Driver  Kernel        Boot       Running    OK
TRUE         FALSE         45,056     106,496     0       3/24/2003 11:16:21 PM
C:\WS2003EE\system32\DRIVERS\ACPI.sys            8,192

ACPIEC       ACPIEC                 ACPIEC                 Kernel        Disabled   Stopped    OK
FALSE        FALSE         4,096      8,192       0       3/24/2003 11:16:26 PM
C:\WS2003EE\system32\drivers\ACPIEC.sys          4,096

aec          Microsoft Kernel Acous Microsoft Kernel Acous Kernel        Manual     Stopped    OK
FALSE        FALSE         67,968     5,632       0       8/28/2002 6:09:10 AM
C:\WS2003EE\system32\drivers\aec.sys             2,176

AFD          AFD Networking Support AFD Networking Support Kernel        Auto       Running    OK
TRUE         FALSE         139,264    12,288      0       3/24/2003 11:40:50 PM
C:\WS2003EE\system32\drivers\afd.sys             16,384

AsyncMac     RAS Asynchronous Media RAS Asynchronous Media Kernel        Manual     Stopped    OK
FALSE        FALSE         0          12,288      0       3/24/2003 11:11:27 PM
C:\WS2003EE\system32\DRIVERS\asyncmac.sys        4,096

...

USBSTOR      USB Mass Storage Drive USB Mass Storage Drive Kernel        Manual     Running    OK
TRUE         FALSE         12,288     8,192       0       3/24/2003 11:10:50 PM
C:\WS2003EE\system32\DRIVERS\USBSTOR.SYS         4,096

usbuhci      Microsoft USB Universa Microsoft USB Universa Kernel        Manual     Running    OK
TRUE         FALSE         0          15,744      0       3/24/2003 11:10:43 PM
C:\WS2003EE\system32\DRIVERS\usbuhci.sys         640

vga          vga                    vga                    Kernel        Manual     Running    OK
TRUE         FALSE         20,480     4,096       0       3/24/2003 11:08:03 PM
C:\WS2003EE\system32\DRIVERS\vgapnp.sys          4,096

VgaSave      VGA Display Controller VGA Display Controller Kernel        System     Stopped    OK
FALSE        FALSE         20,480     4,096       0       3/24/2003 11:08:03 PM
C:\WS2003EE\system32\drivers\vga.sys             4,096

ViaIde       ViaIde                 ViaIde                 Kernel        Boot       Running    OK
TRUE         FALSE         0          4,096       0       3/24/2003 11:04:49 PM
C:\WS2003EE\system32\DRIVERS\viaide.sys          4,096

VIAudio      VIA AC'97 Audio Contro VIA AC'97 Audio Contro Kernel        Manual     Running    OK
TRUE         FALSE         25,344     30,336      0       10/19/2003 8:37:04 PM
C:\WS2003EE\system32\drivers\viaudio.sys         1,408

VolSnap      Storage volumes        Storage volumes        Kernel        Boot       Running    OK
TRUE         FALSE         86,016     8,192       0       3/24/2003 11:05:47 PM
C:\WS2003EE\system32\DRIVERS\volsnap.sys         8,192

VPCNetS2     Virtual Machine Networ Virtual Machine Networ Kernel        Manual     Running    OK
TRUE         FALSE         0          36,864      0       12/3/2003 5:36:34 PM
C:\WS2003EE\system32\DRIVERS\VMNetSrv.sys        4,096

Wanarp       Remote Access IP ARP D Remote Access IP ARP D Kernel        Manual     Running    OK
TRUE         FALSE         4,096      24,576      0       3/24/2003 11:11:22 PM
C:\WS2003EE\system32\DRIVERS\wanarp.sys          4,096

WLBS         Network Load Balancing Network Load Balancing Kernel        Manual     Stopped    OK
FALSE        FALSE         0          122,880     0       3/25/2003 12:41:10 AM
C:\WS2003EE\system32\DRIVERS\wlbs.sys            12,288
```

Listing 2.1: Sample output of the Driverquery utility (in verbose mode).

WMIC

Windows Management Instrumentation Command-line (WMIC) is an interactive command shell for WMI and can do amazing things. WMIC is only available on Windows XP and WS2K3 (Microsoft has stated that the company cannot make WMIC available for Win2K—the coding effort would be too great). The first time you run WMIC by typing

```
WMIC
```

the utility kicks off a self-installation. You are then at the WMIC command prompt. WMIC can be used for remote management of multiple computers with a single command. For example, the following command lists logical disk information, such as file system (FAT, NTFS, and so on), and other driver parameters, such as free disk space, for the servers that you list following the /node switch:

```
WMIC /Node:Server1,Server2,Server3 logicaldisk
```

Note that node in the WMIC context is any server and not specifically a cluster node, as the term often means. WMIC introduces a term called aliases, which can be thought of either as commands or objects on which actions are performed. Using WMIC is such a huge topic that it cannot be covered in entirety here. To illustrate this point, take a look at the list of aliases that Listing 2.2 shows.

```
ALIAS                   –Access to the aliases available on the local
system
BASEBOARD               –Base board (also known as a motherboard or
system board) management.
BIOS                    –Basic input/output services (BIOS) management.
BOOTCONFIG              –Boot configuration management.
CDROM                   –CD-ROM management.
COMPUTERSYSTEM          –Computer system management.
CPU                     –CPU management.
CSPRODUCT               –Computer system product information from
SMBIOS.
DATAFILE                –DataFile Management.
DCOMAPP                 –DCOM Application management.
DESKTOP                 –User's Desktop management.
DESKTOPMONITOR          –Desktop Monitor management.
DEVICEMEMORYADDRESS     –Device memory addresses management.
DISKDRIVE               –Physical disk drive management.
DISKQUOTA               –Disk space usage for NTFS volumes.
DMACHANNEL              –Direct memory access (DMA) channel management.
ENVIRONMENT             –System environment settings management.
FSDIR                   –Filesystem directory entry management.
GROUP                   –Group account management.
IDECONTROLLER           –IDE Controller management.
IRQ                     –Interrupt request line (IRQ) management.
JOB                     –Provides  access to the jobs scheduled using
the schedule service.
LOADORDER               –Management of system services that define
execution dependencies.
LOGICALDISK             –Local storage device management.
LOGON                   –LOGON Sessions.
MEMCACHE                –Cache memory management.
MEMLOGICAL              –System memory management (configuration layout
and availability of memory).
MEMORYCHIP              –Memory chip information.
MEMPHYSICAL             –Computer system's physical memory management.
```

```
NETCLIENT               –Network Client management.
NETLOGIN                –Network login information (of a particular
user) management.
NETPROTOCOL             –Protocols (and their network characteristics)
management.
NETUSE                  –Active network connection management.
NIC                     –Network Interface Controller (NIC) management.
NICCONFIG               –Network adapter management.
NTDOMAIN                –NT Domain management.
NTEVENT                 –Entries in the NT Event Log.
NTEVENTLOG              –NT eventlog file management.
ONBOARDDEVICE           –Management of common adapter devices built
into the motherboard (system board).
OS                      –Installed Operating System/s management.
PAGEFILE                –Virtual memory file swapping management.
PAGEFILESET             –Page file settings management.
PARTITION               –Management of partitioned areas of a physical
disk.
PORT                    –I/O port management.
PORTCONNECTOR           –Physical connection ports management.
PRINTER                 –Printer device management.
PRINTERCONFIG           –Printer device configuration management.
PRINTJOB                –Print job management.
PROCESS                 –Process management.
PRODUCT                 –Installation package task management.
QFE                     –Quick Fix Engineering.
QUOTASETTING            –Setting information for disk quotas on a
volume.
RDACCOUNT               –Remote Desktop connection permission
management.
RDNIC                   –Remote Desktop connection management on a
specific network adapter.
RDPERMISSIONS           –Permissions to a specific Remote Desktop
connection.
RDTOGGLE                –Turning Remote Desktop listener on or off
remotely.
RECOVEROS               –Information that will be gathered from memory
when the operating system fails.
REGISTRY                –Computer system registry management.
SCSICONTROLLER          –SCSI Controller management.
SERVER                  –Server information management.
SERVICE                 –Service application management.
SHADOWCOPY              –Shadow copy management.
SHADOWSTORAGE           –Shadow copy storage area management.
SHARE                   –Shared resource management.
SOFTWAREELEMENT         –Management of the  elements of a software
product installed on a system.
SOFTWAREFEATURE         –Management of software product subsets of
SoftwareElement.
SOUNDDEV                –Sound Device management.
STARTUP                 –Management of commands that run automatically
when users log onto the computer system.
SYSACCOUNT              –System account management.
SYSDRIVER               –Management of the system driver for a base
service.
SYSTEMENCLOSURE         –Physical system enclosure management.
```

```
SYSTEMSLOT              –Management of physical connection points
including ports,  slots and peripherals, and proprietary connections
points.
TAPEDRIVE               –Tape drive management.
TEMPERATURE             –Data management of a temperature sensor
(electronic thermometer).
TIMEZONE                –Time zone data management.
UPS                     –Uninterruptible power supply (UPS) management.
USERACCOUNT             –User account management.
VOLTAGE                 –Voltage sensor (electronic voltmeter) data
management.
VOLUME                  –Local storage volume management.
VOLUMEQUOTASETTING      –Associates the disk quota setting with a
specific disk volume.
VOLUMEUSERQUOTA         –Per user storage volume quota management.
WMISET                  –WMI service operational parameters management.
```

Listing 2.2: Complete WMIC alias listing.

As you can see from the listing, WMI provides access to the storage volume management and quota settings. We will cover the built-in WS2K3 quota feature later, as it has some limitations and difficulties (for example, in being able to include or exclude certain users or groups). For now, you can see where it fits in for the storage analysis phase.

If you bring up the properties for a volume and click on the quota tab, you will see a Quota Entries button in the lower right corner. Clicking this button brings up the quota report that Figure 2.15 shows. This report is somewhat useful for storage analysis as it shows the amount of disk space used by each user (or technically, SID; as you can see, there are some SIDs that are not resolved in the figure).

Note that the BUILTIN\Administrators are excluded from the Quota Limit—but be warned that disk utilities will be affected by the quota limit. Thus, if you enable a 40GB quota, as the example shows, don't be alarmed when your disk defragmenter reports a 40GB drive. Also note the Warning Level is set at 40KB, which should be 40GB.

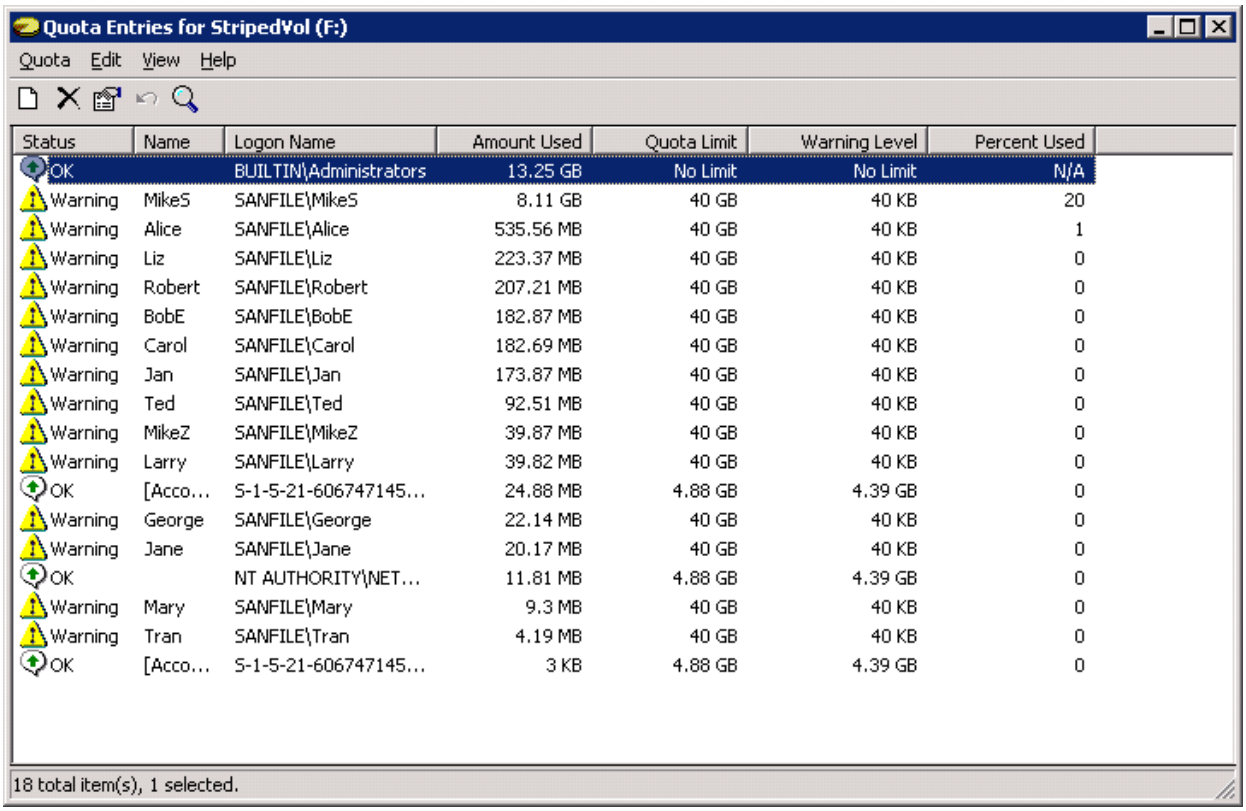


Figure 2.15: Using the quota entries table as a simple volume report.

Cleanmgr

The Disk Cleanup manager offers the option to compress files older than a certain number of days, as Figure 2.16 shows. Of course, this setting only applies for NTFS volumes, and you should use this option with caution to ensure that you know which files you are compressing (some files are not worth compressing because doing so offers little gain and others—such as system files—should be left alone).

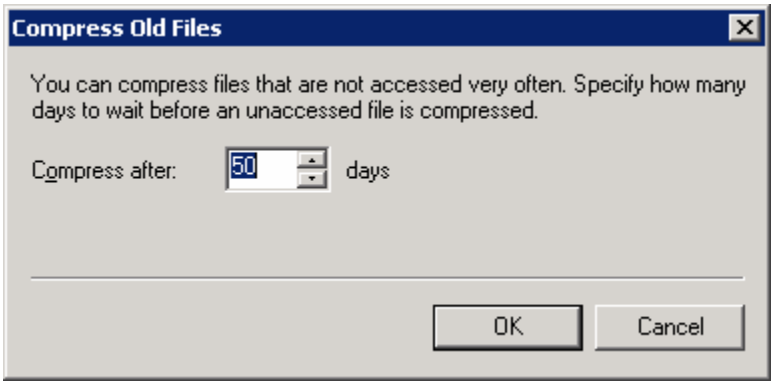


Figure 2.16: The Disk Cleanup tool (Cleanmgr) option to compress files.

Type

```
cleanmgr /d x:
```

to launch the dialog box, and select the x drive.

> Note that most of the information on the Disk Cleanup tool in Windows XP applies to WS2K3 *except* the references to System Restore Points.

The Disk Cleanup tool option that Figure 2.17 shows launches the Add/Remove programs applet. I have included it here as a reminder to watch that 200MB free space threshold for Windows.

Figure 2.17: The Disk Cleanup tool option to launch the Add/Remove programs applet.

Defrag

The Windows Disk Defragmenter now offers a command-line option

```
Defrag -f
```

that will automate defragmentation and force it to run even if free space is low. However, as with the GUI version (dfrg.msc), the volume should have at least 15 percent free space for defragmentation to work properly.

How Important is Disk Defragmentation?

The concept of disk defragmentation makes great sense when dealing with a single spindle, but does it make sense for drive arrays with RAID striping? There have been many studies that claim improved performance as a result of disk defragmentation, but many of them have been funded by the software company selling the product (http://www1.execsoft.com/pdf/NSTL-XP_mddvdk.pdf and http://www.raxco.com/products/perfectdisk2k/whitepapers/benefits_of_defragmentation.pdf).

An odd side effect of disk defragmentation to watch out for is excessive replication of FRS files. For more information about this potential problem, see the Microsoft article "FRS: Disk Defragmentation Causes Excessive FRS Replication Traffic," which states that you should not run defragmentation utilities on volumes that contain FRS replicated files. In addition, see the Microsoft article "Shadow Copies May Be Lost When You Defragment a Volume," which basically states that you should avoid defragmenting these volumes or use a 16KB or larger cluster allocation unit size when you format the volume if you plan to use shadow copies of shared folders and defragment the volume. However, you cannot change the cluster size on the fly—you must reformat, so, hopefully, this information is not too late.

An indication that defragmentation is beneficial is that it is called internally by a new process available only in WS2K3—the logical prefetcher. What prefetch can do is provide faster boot and application launch by running when a WS2K3-based system is booted, saving the information about all logical disk read operations. On the following reboots, the files that are loaded will be optimized on disk by running the defragmentation mentioned earlier. This feature can help your server boot faster—which, hopefully, does not happen too often—as well as help any applications that load after boot—such as your antivirus and SRM applications. The system organizes disk reads that need to be done to start the system in parallel with device initialization delays, providing faster boot and logon performance.

Prefetch is enabled for system boot by default. In order to enable the prefetch feature for applications, you need to set the following registry key (simply search for a key value of prefetch with the value and data check boxes cleared as you search): HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters. Set the value name to EnablePrefetcher (DWORD) and the value to

- 0x00000001= application launch prefetching
- 0x00000002= boot prefetching
- 0x00000003=both application and boot prefetching

The parameters use AND, so to enable both boot and application EnablePrefetcher would be set to 0x00000003. The setting takes effect immediately and does not require a reboot, but, of course, the prefetch process takes advantage of each reboot, so it is a good idea.

Every 3 days or so, during system idle periods, the Task Scheduler organizes a list of files and directories in the order that they are referenced during boot or application start, and stores the list in the prefetch directory. Then the defragmenter (mentioned earlier) is launched with a command-line option to defragment based on the contents of this prefetch file instead of performing a full defragment. The defragmenter finds a contiguous area on each volume large enough to hold the listed files and directories, then moves them in their entirety to that area so that they are stored contiguous. As a result, future prefetch operations will be more efficient because the data to be read is stored physically on the disk in the order it will be needed.

Event Utilities

You can use a trio of utilities—Eventquery, Eventcreate, and Eventtriggers—to read, write, and respond to Windows events, respectively. For example, suppose you're watching for Event ID 2013 (disk is at or near capacity) and you launch a system cleanup utility such as the built-in cleanmgr.exe (which, unfortunately, has no automated options). Alternatively, you can use a different cleanup utility or a custom script that you have written. Some companies place a large file (a gigabyte or two) as a buffer against the disk filling up—the automated script would then delete this file, which is very safe, and notify the administrator. This gives you some time to assess your disk cleanup instead of immediately being in panic mode. To enable this scenario, simply enter the following text at t a command line and it will create the event:

```
eventtriggers /create /tr "my TriggerName" /l application /eid
2013 /tk c:\mycleanup.cmd
```

You will then be prompted for the Run As password for the account with which you are logged on. You can then see the scheduled tasks listing by using the built-in utility schtasks or the scheduled tasks under Control Panel in Windows Explorer. If the event fails to execute, check the log file %systemroot%\system32\wbem\logs\cmdTriggerConsumer.log.

Forfiles

Forfiles selects files in a folder or tree for batch processing (for example, you can use it to select files older than a certain date to move them to an archive location). Forfiles is more powerful in its options than other commands such as xcopy; it allows you to specify a certain number of days from today, which is handy for scheduling a cleanup or reporting script. For example, to list all files on drive x older than 365 days:

```
forfiles /p x:\ /s /m*.* /dt-365 /c"cmd /c echo @file : date >=
365 days and next command will archive it"
@echo on
pause Hit any key to continue with archive process
pause !Warning! This will move old files to z:\archive!
@echo off
forfiles /p x:\ /s /m*.* /dt-365 /c"cmd /c move @file z:\archive"
```

Freedisk

Freedisk checks whether the specified amount of disk space is available before continuing with an installation process. You can even use this utility in a logon script to check available disk space set on a volume by a disk quota before running logon commands, because Freedisk runs under the user context. You can use this utility to check quotas on a volume for specific users, and you can provide it with username and password by using the /U and /P options.

Fsutil

Fsutil is another command-line utility that eases file–system–management tasks, such as managing reparse points, managing sparse files, dismounting a volume, or extending a volume. Figure 2.18 shows sample Fsutil commands and usage for the quota command.

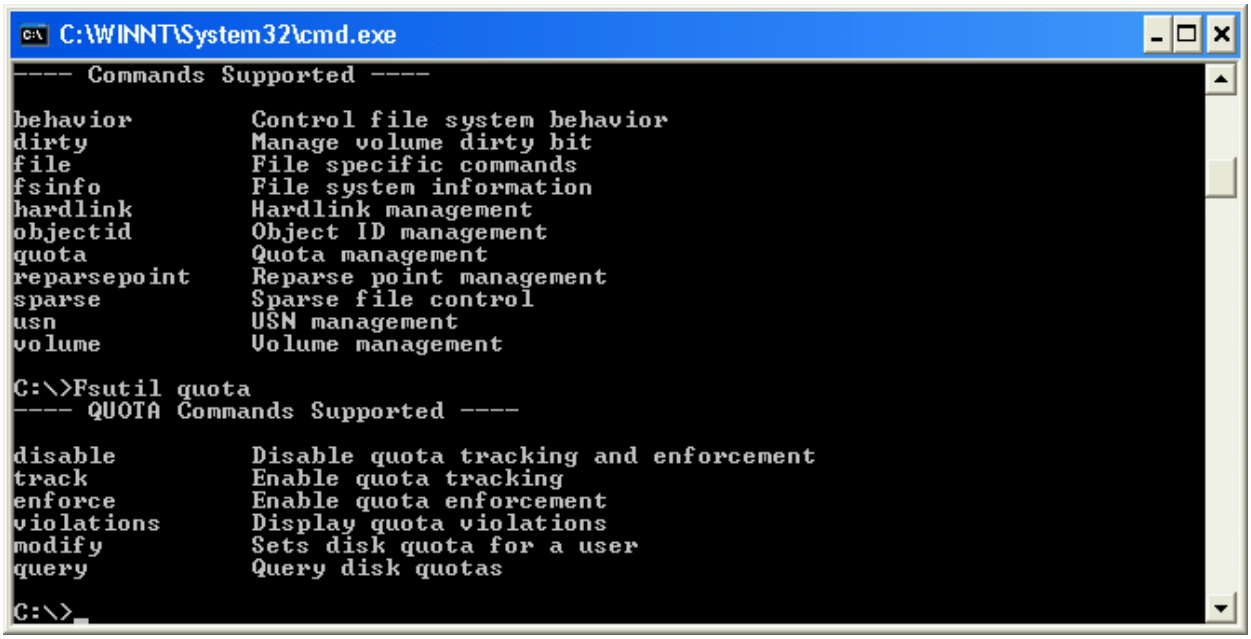


Figure 2.18: Fsutil quota commands.

You can also use Fsutil to check for a dirty bit by running

```
fsutil dirty query x:
```

where x is the volume you want to check.

> 🕮 For more information about the powerful options available through Fsutil, see http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/fsutil.asp

Openfiles

Openfiles lists the open files and folders on a system and allows you to force a disconnect (using the /Disconnect parameter). In order to list opened local files, the system global flag 'maintain objects list' needs to be enabled via openfiles /local on and requires a reboot to take effect.

RSS

RSS helps manage disk space by automatically copying infrequently used files from a volume to a tape or disk library. When the amount of free disk space falls below the defined level on the volume, RSS kicks into action. You can use the command-line RSS utility to manage RSS, but be aware that you must first install RSS. To do so, navigate to the Add/Remove Windows Components Control Panel applet to the Remote Storage option. Select this option, and make sure that you have your WS2K3 installation media handy. You will also need to restart your computer.

> 🕮 We will look at RSS in more detail in the next chapter.

Systeminfo

Systeminfo is one of many ways to get a listing of system information. A useful feather of this utility is that it includes such items as Original Install Date, system uptime, and a list of hotfixes—plus it is guaranteed to be on every WS2K3 machine because it is a built-in tool.

TakeOwn

TakeOwn lets administrators take ownership of files, which allows you to recover access to a file orphaned through incorrect file ownership. To use this utility, you must be a member of the local Administrators group, which is automatically assigned on a member server to the Domain Admins group. This utility can also come in handy if you install WS2K3 on a computer that had a previous WS2K3 installation on it, as the files in the \Installer folder may be locked and require System permissions to delete them. Using TakeOwn can reset the ownership (you might also need to use Windows Explorer or another utility, cacls, to reset all permissions).

Additional Windows Server Resources

A great starting point for discovering additional Windows Server resources is the WS2K3 Downloads page at http://www.microsoft.com/windowsserver2003/downloads/default.mspx. Microsoft has split the available resources into several areas, including WS2K3 Feature Packs and Tools.

On the WS2K3 Tools page, you'll find the downloadable tools that help you support WS2K3 systems. After installing a new WS2K3 Server using the original installation media (CD-ROM), I immediately install the Administration Pack Tools, the Support Tools, and the Resource Kit Tools.

Administration Pack Tools

The Administration Pack Tools contains Active Directory Tools, Terminal Services Tools, and other tools such as the Distributed File System console. This pack is installed by running the Adminpak.msi found in the \i386 folder of the WS2K3 CD-ROM. It is also available on the Web at http://download.microsoft.com/download/c/7/5/c750f1af-8940-44b6-b9eb-d74014e552cd/adminpak.exe.

Support Tools

The WS2K3 Support Tools provides more than 40 tools installed by running the Suptools.msi found in the support\tools folder of the WS2K3 CD-ROM. Table 2.2 offers examples of the support tools that are relevant to storage management.

Utility	Description	Example Usage
Devcon.exe	Device Console Utility—Command prompt alternative to hardware device manager	List or disable problematic devices from the command line
Diruse.exe	Displays a list of disk usage for a directory tree with additional options	An alert can be generated if folders exceed specified sizes
Dmdiag.exe	Lists disk volume configuration	Does a complete dump of disk and storage information (can be overwhelming, but also useful as input to other tools)
Efsinfo.exe	Displays information of encrypted files on NTFS partitions	/T option can be used to 'touch' all files in a given folder or subfolder, forcing an update to their EFS information
Ftonline.exe	Mounts NT 4.0 fault tolerance disk sets	Forces mounting of an existing NT 4.0 disk volume after the upgrade to WS2K3
Remote.exe	Run a command line on a remote computer	Useful when remote access has not been enabled and you need to run a utility
Rsdiag.exe and Rsdir.exe	Remote storage diagnostics and reporting	Requires remote storage to be installed on system
Topchk.cmd	DFS and SYSVOL Replication Topology Analysis Tool	Shows the FRS replication topology
Xcacls.exe	Displays or modifies access control lists (ACLs) of files	The X stands for Extended, as it can change Special Access rights

Table 2.2: WS2K3 Support Tools that are relevant to storage management.

WS2K3 Resource Kit Tools

The Resource Kit Tools have always been valuable and worth having. They are now available for download for WS2K3. You can find them at http://download.microsoft.com/download/8/e/c/8ec3a7d8-05b4-440a-a71e-ca3ee25fe057/rktools.exe. Table 2.3 lists some of the WS2K3 Resource Kit Tools that may be of interest for SRM.

Utility	Description
Cdburn.exe	Burn ISO images to CD-ROM
Cleanspl.exe	Flush print spoolers
Clusdiag.msi	Cluster diagnostics and verification tool
Clusterrecovery.exe	Server cluster recovery utility
Cmdhere.inf	Adds menu item in Explorer to launch a command prompt
Compress.exe	Compress files
Confdisk.exe	Disk configuration tool
Creatfil.exe	Create file
Csccmd.exe	Client-side caching command-line options
Diskraid.exe	RAID configuration tool
Diskuse.exe	User disk usage tool
Dvdburn.exe	ISO DVD burner tool
Fcopy.exe	File copy utility for message queuing
Gpmonitor.exe	Group Policy Monitor
Gpotool.exe	Group Policy Objects (GPOs)
Hlscan.exe	Hard link display tool
Iniman.exe	Initialization files manipulation tool
Moveuser.exe	Move users
Nlsinfo.exe	Locale information tool
Ntrights.exe	Grant or revoke NT rights to a user/group
Permcopy.exe	Copy file- and share-level permissions between shares
Perms.exe	Display a user's access permissions for a file or directory
Rcontrolad.exe	Active directory remote control add-on
Robocopy.exe	Copy files between two locations
Showacls.exe	Show ACL for subdirectories
Showperf.exe	Performance data block dump utility
Sleep.exe	Batch file wait
Srvcheck.exe	Server share check
Srvinfo.exe	Remote server information
Srvmgr.exe	Server Manager
Subinacl.exe	Move security information between objects
Tcmon.exe	Traffic Control Monitor
Usrmgr.exe	User Manager for Domains
Vfi.exe	Retrieve and generate detailed information about files
Volperf.exe	Shadow copy performance counters
Volrest.exe	Shadow copies for shared folders restore tool
Vrfydsk.exe	Verify disk
Winpolicies.exe	Policy spy

Table 2.3: Storage-related WS2K3 Resource Kit Tools.

WS2K3 Feature Packs

The WS2K3 downloadable Feature Packs provide new functionality and extend the capabilities of WS2KS:

- Automated Deployment Services (ADS)
- Identity Integration Feature Pack (part of the Metadirectory System for integrating Directory Services)
- Software Update Services
- Windows SharePoint Services
- Windows System Resource Manager (WSRM)

> WSRM is only available for use with WS2K3 Enterprise Edition and Datacenter Edition.

> We'll touch upon some of these feature packs as they relate to storage management in later chapters.

Win2K Server Resource Kit

The Win2K Server resource kit is available for purchase from Microsoft and is well worth the investment.

> If you haven't already purchased the resource kit, check out the following Web links, as some of these tools are available for free download. You can find a list of free Win2K Server resource kit tools at http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp and a complete list of tools at http://www.microsoft.com/windows2000/techinfo/reskit/rktour/server/S_tools.asp.

The resource kit includes about 300 tools; Table 2.4 provides a list of some storage-related tools that can help you in your SRM deployment.

Utility	Description	Example Usage	Free Download	Notes for 2003
Diskmap.exe	Displays information about a disk and the contents of its partition table.	Reports disk signature as well as cylinder, head, and sector information.	Yes	
Dmdiag.exe	Saves disk volume configuration to a text file and writes a signature to a disk partition.	Does a complete dump of disk and storage information. (This much information can be overwhelming!)	Yes	Updated version in 2003 kit
Dumpcfg.exe	Reads and writes disk information such as signatures.	Can be used for disk-signature repair. (This utility is very useful for cluster disks).	No	Replaced on 2003 by the built-in DiskPart

Utility	Description	Example Usage	Free Download	Notes for 2003
Efsinfo.exe	Displays information about EFS NTFS partitions.	Lists encrypted files, the user, and the recovery agent.	Yes	Updated version in 2003 kit
Forfiles.exe	Enables batch processing of files in a directory or tree.	Automated operation to find and clean up a directory tree or an entire drive.	No	Updated version in 2003 kit
Freedisk.exe	Checks for free disk space, returning a 0 if there is enough space for an operation and a 1 if there isn't enough space.	One method to ensure that a disk doesn't run out of room.	No	Updated version in 2003 kit
Linkd.exe	Links an NTFS directory to a target object.	I'll discuss this utility when I discuss volume mount points and junction points later in this book.	No	
Netcons.exe	Displays current network connections.	Monitor or determine status on connections to a file server	No	
Permcopy.exe	Copies file- and share-level permissions from one share to another.	Duplicate ACL permissions from one directory tree to another	No	
Perms.exe	Displays a user's access permissions for a file or directory.	Handy for clean up or migrations	Yes	
Robocopy.exe	Robust File Copy Utility	Create and maintain multiple mirror images of large folder trees on network servers.	No	Updated version in 2003 kit
Rsm_dbic.exe	Removable Storage Integrity Checker	Checks the integrity of the RSM database for media and removable media drives and libraries.	No	
Rsm_dbutil.exe	Removable Storage Database Utility	Steps through the RSM database and inspects each database object attribute for valid values and referential integrity.	No	
Rsmconfg.exe	Removable Storage Manual Configuration Wizard	Aids in manually configuring (from a command prompt) libraries that RSM autoconfiguration can't configure.	No	

Utility	Description	Example Usage	Free Download	Notes for 2003
Subinacl.exe	Move security information between objects (users, groups, domains, printers, files, and services).	Changes the account used in service startup properties, as I previously mentioned.	No	Updated version in 2003 kit
Vfi.exe	Retrieves and generates detailed information about files, such as attributes, version, and flags.	Allows you to find duplicate files and do a size as well as a cyclical redundancy check (CRC) comparison.	No	Updated version in 2003 kit
Xcacls.exe	Displays and modifies security options for system folders.	More powerful than Perms.exe in that it lets you set the ACLs.	Yes	

Table 2.4: Win2K Server Resource Kit storage-related tools.

Windows Server Resource Kit Security Tools

In addition to the storage-related tools, the resource kit provides security tools that can help you during your SRM deployment. Do not overlook security, as recent virus outbreaks and network-based attacks have affected storage servers. What we've learned from the recent outbreaks is:

- Systems must be secured from the start—deployed from a secure baseline image (or built off the main network). The Security Readiness Kit (SRK) can be used for offline builds and preparation (http://www.microsoft.com/technet/security/readiness/232.mspx).
- Establish an escalation response team and communication procedures. It might become necessary to disable certain network services (or block certain types of attachments temporarily).
- All systems must be managed (for example, using Software Update Services for patch management). Scanning tools must be used to probe the network for unmanaged at-risk systems. Systems can be scanned with the Microsoft Baseline Security Analyzer (MBSA) and HFNetChk, which I'll discuss shortly.
- Corporate security must be proactively managed. Studies have shown that staying current on threats and patch management and actively filtering for malicious code reaps substantial rewards (in terms of reduced cost associated with outbreaks).

For additional reading and guidelines to assist you in securing Windows Server, the National Security Agency (NSA) publishes about 20 Security Recommendation Guides that you can download from http://nsa1.www.conxion.com/win2k/index.html. Many of the security guides will still be helpful for WS2K3, although some configuration directions might not be as necessary with the "secure by default" initiative of WS2K3. In fact, the NSA does not plan to publish a security guide for WS2K3 and has stated that the "high security" settings in Microsoft's "Windows Server 2003 Security Guide" are close to the security level represented in NSA guidelines. You can access the Microsoft publication at http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en.

The following list highlights additional security tools that might be of interest:

- HFNetChk—This tool is designed to check which patches have been applied to your system. HFNetChk is available via the command-line interface of MBSA.
- MBSA version 1.2—A new version of the MBSA is available to work with WS2K3. Version 1.2 includes both a graphical and command-line interface to perform local or remote scans of Windows systems. The MBSA scans for common security misconfigurations, vulnerabilities, and missing security updates, and generates security reports. It is available at http://support.microsoft.com/default.aspx?kbid=320454.
- System Scanner—System Scanner for Windows is a security-assessment tool designed for Win2K Server. It performs security checks on files, the registry, and user-account settings and can verify the configuration of virus scanners. You must install it separately by running Sysscansetup in the \Apps\Systemscanner folder of the Win2K Resource Kit CD-ROM, then click Start, Programs, ISS, and System Scanner Help.

> 🕮 For more information about the System Scanner for Windows, check out the Microsoft article "Description of the Windows 2000 Resource Kit Security Tools" at http://support.microsoft.com/support/kb/articles/Q264/1/78.asp.

Analyzing Storage Usage Tools

We've covered some great new utilities for performing disk operations and storage management, but what about analyzing storage usage? How do we know which types of files exist, how old they are, who they belong to, if they are duplicates, and whether they are being properly managed? There aren't any great tools built-in to the Windows Server products that can do all of this. Many storage administrators use rather crude methods to access such information, but a truly efficient enterprise will require the features that have defined the SRM market and products, which we'll explore later in this guide.

Summary

In this chapter, we covered the process and available tools for analyzing your current storage environment. First, I laid out the levels or hierarchy of auditing from the organization to the files level. I spelled out the types of information that you'll want to gather, showing you sample reports including storage utilization (disk space used and available) and identifying who the storage users are. Next, we looked at the built-in tools of WS2K3 for analyzing your storage requirements. We've reached the need to look at third-party SRM tools to show how they can improve the storage audit process and prepare you for the next phase, planning your SRM deployment.