realtimepublishers.com™

The Definitive Guide™ To

Windows 2003 Storage Resource Management

VERITAS™

Evan Morris

Copyright Statement

Chapter 7: Manage and Maintain the SRM Solution

In the previous chapter, we covered the deployment phase of your SRM solution. We started by reviewing the SRM goals and components, and developed an organizational view of the SRM solution. Next, we looked at the different storage management strategies and the various products, listing product selection criteria for the following types of solutions: device configuration and management, enterprise storage management, application-centered SRM, fibre-channel SAN approach to SRM, and policy-based object management. I continued to cover project-management fundamentals, such as defining the critical path, setting milestones, and performing a risk analysis. I gave you a template for risk-mitigation techniques and how to identify sources of problems such as technical issues and people issues. We also looked at change control in the context of extending AD. Finally, I gave you some sample success-measurement criteria to help you define your objectives for this phase of the project.

In this chapter, we will continue the focus on project management, as you complete the deployment by setting up systems to monitor and maintain the SRM solution. In addition, we will cover the technical aspects of what you need to monitor and which solutions are available. I will give you a complete list of systems management recurring tasks that you can use to make sure that you have all your operations—including SRM functions—in place.

The goal of this chapter is to aid you in developing a daily approach to SRM that automates the repetitive tasks—for example, monitoring disk usage by using the SRM software that we have discussed. This automation will free your time for other crucial tasks—such as maintaining your security defenses—that might be overlooked, as you only have so much time, and must continually fight to ensure that your priorities match those of the business. Table 7.1 shows Phase 6 in the overall SRM deployment methodology.

Phase	Process	SRM
Maintain	Continue to support the solution and prepare to improve as needed	Monitor disk usage; add storage as needed (hopefully, only for performance upgrades or to replace defective hardware).

Table 7.1: Phase 6 of the SRM deployment methodology.

Project Management Aspects

At this point, you should be polishing off any rough edges in your SRM deployment, and you'll find that this task is the easiest part of the deployment. You will have the opportunity to see the benefits of SRM, and to work on automating the monitoring and management process. Change of plan—this urgent message just came in—we have a security violation on our network that must be dealt with immediately!

Security Issues

When your security model is compromised, all else takes a back seat—SRM becomes less important than storage resource protection. Security should not be omitted from any deployment. Throughout this SRM discussion, security may have been given lesser priority, but in this chapter, we will increase the priority of security in the context of your SRM deployment. Recent virus outbreaks have either tested whether you have been updating your systems' security patches or given you a chance to validate your data recovery procedures. Lately, much effort has been spent just keeping systems safe from harm, and from this effort, new attention to security and a new security initiative from Microsoft will result.

There are several things that you can do to improve your security immediately. First, subscribe to the Microsoft Security Notification Service. To subscribe to this service, send an email to securbas@microsoft.com (no need to put anything in the subject line or message body). More information can be found at http://www.microsoft.com/technet/security/bulletin/notify.asp.

The next thing that you can do is to download and run several Microsoft-provided security tools. Many security flaws or problems have been found in IIS, which is a component of the default installation of WS2K3, so many of the tools focus on IIS. A good starting point is the Microsoft Security Tool Kit, as it packages several tools and recent patches to the OS, IIS, and some applications, such as Internet Explorer (IE).

Microsoft Baseline Security Analyzer

The newest version of the Microsoft Baseline Security Analyzer (MBSA) can be downloaded from the MBSA site at http://www.microsoft.com/technet/security/tools/mbsahome.mspx. The newest version scans not only for missing security updates and incorrect configurations in Windows but also in IE, IIS, SQL Server, Exchange Server, and many other Microsoft products. This tool should become a constant companion, and you should use it to run regular security checks of all your servers.

MBSA will point out any missing security updates as well as poor configurations (such as weak or missing passwords). Obviously, in order to have the most secure system possible, you should carefully review MBSA's report and consider its recommendations for hardening your servers.

In addition, Microsoft recommends uninstalling all Windows services not in active use—particularly IIS, but also services such as DNS, DHCP, and so forth. Any service not actively needed on a server should be uninstalled; merely disabling the service still presents the opportunity for an attacker to re-enable it and exploit any vulnerabilities.

Systems Management and Monitoring

Now that we've secured our systems, we can get back to the business of SRM. The challenge in managing any storage environment is how to be proactive instead of reactive to catastrophic events. What can we learn from the top professionals in enterprise organizations, the largest consumers of storage? If we follow their lead, we will already know the questions that must be asked, and how to find the answers, such as "How do I know if my storage is online and performing as well as it should?"

Anticipating Changes

Table 7.2 lists the types of events most likely to happen in your environment, and some planned responses. What you can gain from the table is seeing the importance of SRM. Perhaps you are reading this guide with the thought of maintaining SRM yourself, without a third-party application. If so, you will need the following contingency plans.

Anticipated Event	**Planned Response**
Running low on disk space	Notify users and prepare user report and administrative report about what can be removed; if space is dangerously low, block writes until files are removed
New users and home directories	Add new users to the existing storage policy (how much space allocated, which types of files are not allowed); ensure that no users exist outside of policy
New folders or subdirectories	Ensure that existing storage policies are applied to the new folders
New viral attacks	Prevent viruses from writing files by using NTFS permissions and identifying the viral files (sometimes creating a read-only pre-existing file to stop the viral action)
New storage systems and SANs	Carve out the storage and allocate to application servers and file servers; apply storage policy to allocated storage; ensure that storage systems and SANs are part of the management framework; understand how to deal with specific events, such as device failure
Disk drives added to the servers	Add the disks to existing arrays (if supported) or create new arrays and logical disks; ensure that the disks are part of the storage policy
Non-events	User accounts and files will become orphaned through long periods of inactivity; plan to identify and clean up these objects periodically
Minor service interruptions	Resolve items such as loss of power, cable damage or failure, operator error, or other service errors such as GC or domain controller failures precluding authentication
Catastrophic events	Device failure or data corruption necessitating recovery procedures; identify proper procedures and ensure that recovery hardware is on standby

Table 7.2: Anticipated storage events and planned responses.

OS Monitoring

You can monitor and measure WS2K3 stability using similar methods as you use with other applications, primarily by using an application monitor (such as Microsoft Operations Manager—MOM, which I'll discuss later) to watch event logs for the dirty shutdown event (ID 6008) followed by the system startup event (ID 6005).

> ☞ If your server is experiencing stop errors, see the following articles for information about how to use the crash dump information recorded in the Memory.dmp file
>
> "Gathering Blue Screen Information After Memory Dump" at http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q192463&
>
> "Blue Screen Preparation Before Contacting Microsoft" at http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q129845&
>
> For information about troubleshooting failed applications, see the article "How to Install Symbols for Dr Watson Error Debugging" at http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q141465&

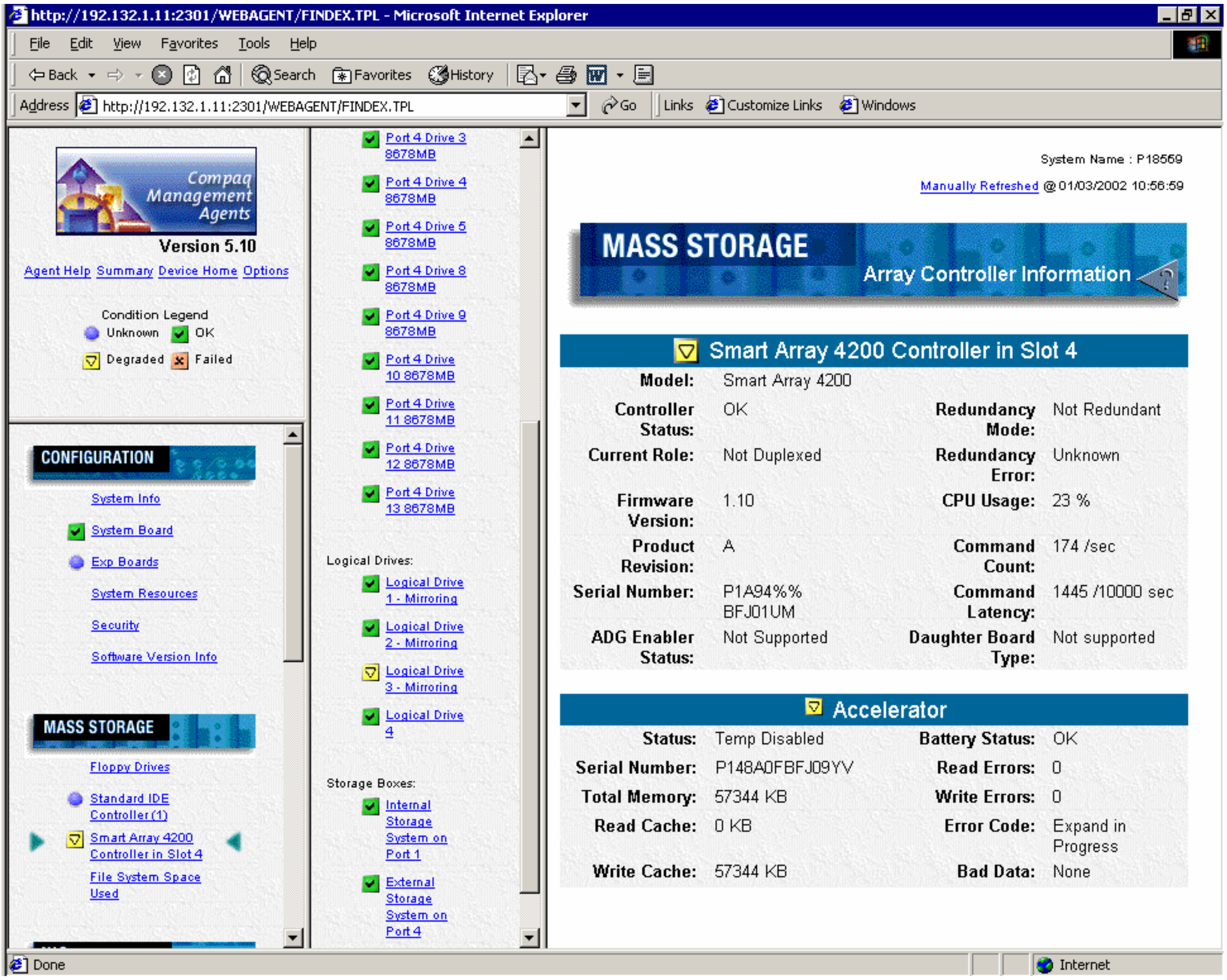
Another product that performs WS2K3 monitoring offers a visual perspective—Quest Software's Spotlight on Windows. This product's UI looks like it should also play CD-ROMs or mp3s, but it actually provides an all-in-one view of how a server is performing, including items such as free disk space and disk I/O (reads/second and writes/second). This tool offers more functionality than Windows Performance Monitor provides, featuring an analysis of performance data and an online tuning guide.

Storage Event Monitoring

When we are forced to be in reactive mode, which is inevitable as devices fail and software crashes, the key is how quickly we can find out that there is a problem and how extensive the information is that we can gather. Quite often we find that the failure was preceded by several warnings, such as several Event 9, source: scsi miniport driver, which states *The device, \Device\ScsiPortX, did not respond within the timeout period* followed by an Event 11 source: scsi miniport driver, which states *The driver detected a controller error on Device\ScsiPortX*.

The WS2K3 Performance Monitor can be set to monitor many servers with a very infrequent polling interval—just remember to change the service startup to use a domain account with sufficient credentials. You can monitor free disk space on logical drives (by enabling disk counters using the diskperf –y command, as discussed in previous chapters), or you can monitor a counter such as system uptime, just to make sure the system is online.

Another choice is a vendor-provided storage monitoring application, such as the Web-based view of a direct-attached RAID controller, which Figure 7.1 shows. The information that this figure shows is from Compaq Insight Manager, which provides information about devices attached to the server: controllers, disks, storage boxes (cabinets), and so on, and is available at http://www.compaq.com.


http://192.132.1.11:2301/WEBAGENT/FINDEX.TPL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.132.1.11:2301/WEBAGENT/FINDEX.TPL
Go Links Customize Links Windows
Compaq Management Agents
Version 5.10
Agent Help Summary Device Home Options
Condition Legend
Unknown OK
Degraded Failed
CONFIGURATION
System Info
System Board
Exp Boards
System Resources
Security
Software Version Info
MASS STORAGE
Floppy Drives
Standard IDE Controller (1)
Smart Array 4200 Controller in Slot 4
File System Space Used
Port 4 Drive 3 8678MB
Port 4 Drive 4 8678MB
Port 4 Drive 5 8678MB
Port 4 Drive 8 8678MB
Port 4 Drive 9 8678MB
Port 4 Drive 10 8678MB
Port 4 Drive 11 8678MB
Port 4 Drive 12 8678MB
Port 4 Drive 13 8678MB
Logical Drives:
Logical Drive 1 - Mirroring
Logical Drive 2 - Mirroring
Logical Drive 3 - Mirroring
Logical Drive 4
Storage Boxes:
Internal Storage System on Port 1
External Storage System on Port 4
Done
Internet

System Name : P18569

Manually Refreshed @ 01/03/2002 10:56:59

MASS STORAGE

Array Controller Information

Smart Array 4200 Controller in Slot 4

Model:	Smart Array 4200		
Controller Status:	OK	Redundancy Mode:	Not Redundant
Current Role:	Not Duplexed	Redundancy Error:	Unknown
Firmware Version:	1.10	CPU Usage:	23 %
Product Revision:	A	Command Count:	174 /sec
Serial Number:	P1A94%% BFJ01UM	Command Latency:	1445 /10000 sec
ADG Enabler Status:	Not Supported	Daughter Board Type:	Not supported

Accelerator

Status:	Temp Disabled	Battery Status:	OK
Serial Number:	P148A0FBFJ09YV	Read Errors:	0
Total Memory:	57344 KB	Write Errors:	0
Read Cache:	0 KB	Error Code:	Expand in Progress
Write Cache:	57344 KB	Bad Data:	None

Figure 7.1: Web-based view of a direct-attached RAID controller.

This type of vendor-provided application is usual for storage event monitoring as it shows degraded and failed devices, which you can see in the Condition Legend. As the figure shows, the controller is in a degraded state as an array is being rebuilt (the error code states Expand in Progress). Where this product falls short is that a view or state must be determined for each server and rolled up to a centralized hierarchy, and perhaps this model does not apply when you are dealing with multiple applications sharing a pool of storage. So, we must also consider storage monitoring from an application perspective.

Storage Application Monitoring

In the previous chapters, we have gone through the process of designing, testing, and installing your deployment of an SRM application. At this point, we must address the questions, Who will monitor the storage resource monitor? and How will we know that the SRM application is online and performing its duties? The answers lie in another layer of monitoring—in application monitoring and management. There are a wide variety of application-monitoring products, including those focused on SAN device management, which we touched on in the past chapter.

The wide variety of storage and SAN monitoring tools presents several challenges. First, it presents a variety of interfaces or methods of managing the storage, as there is little commonality between the vendors. Second, vendors must develop a product that manages a wide variety of devices that offer varying degrees of interoperability or have limited standards. Thus, the end result is a multitude of specialized management applications with little centralization. At this point in technology evolution, our best choice for centralization is a management and monitoring application that relies on gathering information from the servers (and other similar devices that include event logging, such as a SAN management appliance based on WS2K3) attached to the SAN.

What will monitor the monitoring application—how will we know that the application-monitoring application is running? Fair questions, let's take a look at one application-monitoring package, MOM, that includes management packs to monitor itself.

MOM

So much press and publicity has been focused on MOM lately that I think it is beneficial for storage architects and storage administrators to pay attention. I have heard critical reviews of MOM's difficulty and shortfalls, but as with any Microsoft product, the lessons from the field will be turned into a better and perhaps more successful product. If you are unfamiliar with MOM, it is a server- and application-monitoring product for which Microsoft bought the code from NetIQ. So, if you are familiar with the NetIQ product functionality, MOM will be familiar. If not, you might find getting started with MOM difficult and overwhelming. I'll give you a quick lesson in how to get started with MOM, and we'll look at how MOM integrates or will be integrated with storage management.

Perhaps the most difficult part of getting started with MOM is to meet the prerequisites. It is doubtful that you have all of them in place. The server on which you choose to install MOM is known as the central computer. This server will act as the database collection point and the management console. It should be a member of a domain, but not a domain controller, or MOM will refuse to install.

First, run Office Setup, and install the Office graphing component and Access 2000 (the full version of Access 2000 is required for creating or customizing reports, whereas, the run-time version of Access 2000 is required to run and view reports). The run-time version of Access 2000 is available on the MOM CD-ROM in the \Intel\Access2000RT folder.

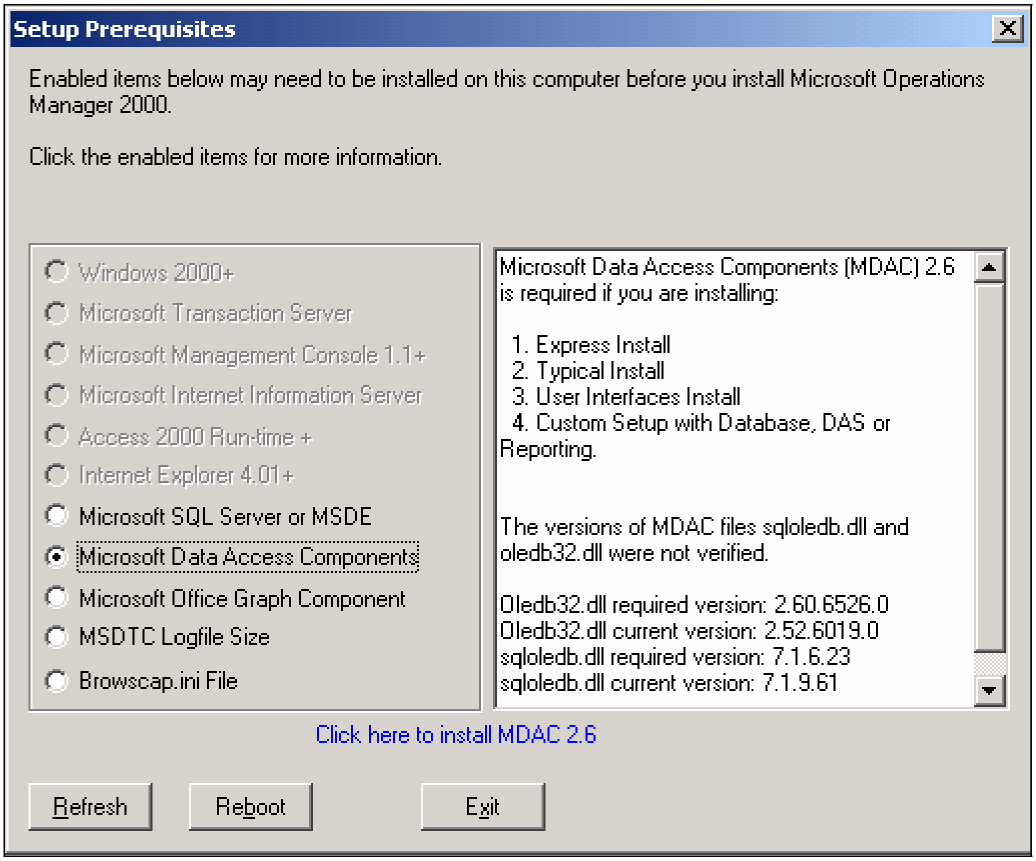
Next, update %systemroot%\system32\inetsrv\browscap.ini if you're not using IE 6.0. Supposedly (according to the MOM product documentation), this file is downloadable from the Microsoft Web site, but I couldn't find it, and the MOM setup application takes care of updating browscap.ini. Optionally, you can install Outlook 98 or later to send email notifications through Microsoft Exchange.

Next, install SQL Server 2000, and set a password on the sa account. If you're installing MOM on an existing SQL Server, run the

```
sp_helpsort
```

query to ensure that the sort order is case insensitive, and verify that the audit level of SQL Server is set to None or Failure (check the audit level on the Security tab of the server's properties page). Ensure that the MSSQLServer, MSDTC, and SQLServerAgent services are running and set to start automatically on computer startup.

MOM requires Microsoft Data Access Components (MDAC) 2.6 or later. As Figure 7.2 shows, the MOM setup program will verify this prerequisite and give you the option to install MDAC 2.6.



Setup Prerequisites

Enabled items below may need to be installed on this computer before you install Microsoft Operations Manager 2000.

Click the enabled items for more information.

○ Windows 2000+
○ Microsoft Transaction Server
○ Microsoft Management Console 1.1+
○ Microsoft Internet Information Server
○ Access 2000 Run-time +
○ Internet Explorer 4.01+
○ Microsoft SQL Server or MSDE
● Microsoft Data Access Components
○ Microsoft Office Graph Component
○ MSDTC Logfile Size
○ Browscap.ini File

Microsoft Data Access Components (MDAC) 2.6 is required if you are installing:

1. Express Install
2. Typical Install
3. User Interfaces Install
4. Custom Setup with Database, DAS or Reporting.

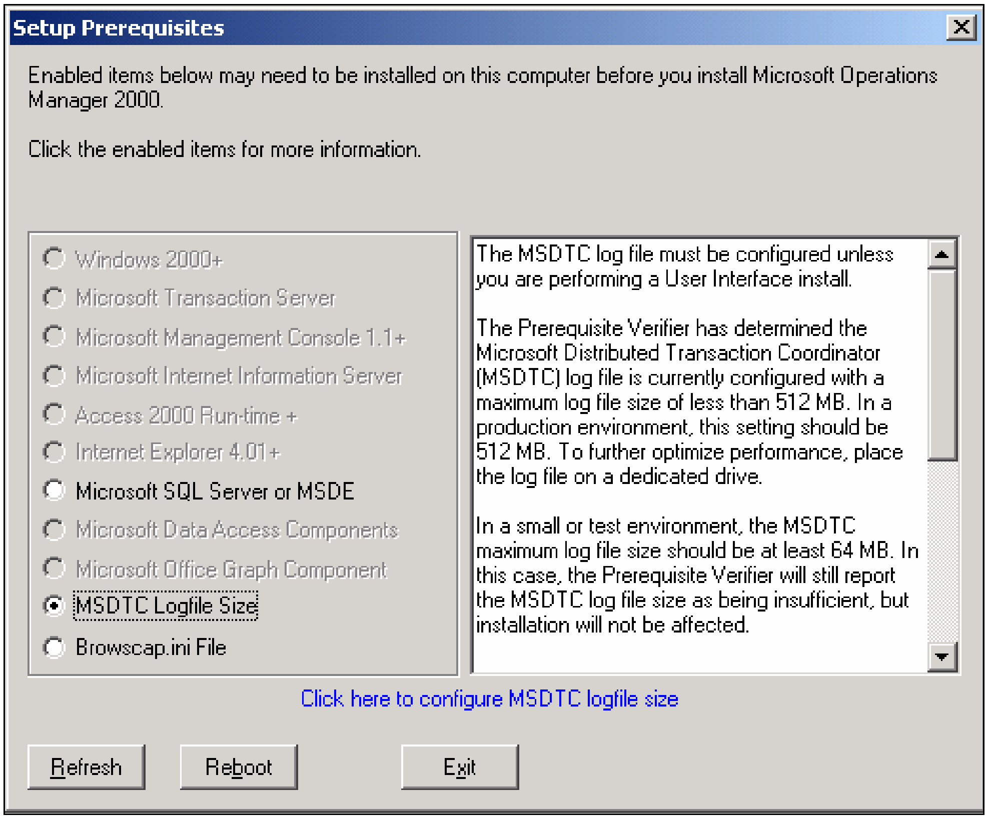
The versions of MDAC files sqloledb.dll and oledb32.dll were not verified.

Oledb32.dll required version: 2.60.6526.0
Oledb32.dll current version: 2.52.6019.0
sqloledb.dll required version: 7.1.6.23
sqloledb.dll current version: 7.1.9.61

Click here to install MDAC 2.6

Figure 7.2: MOM installation verifies prerequisites and can update MDAC.

Next, increase the log file size of the Microsoft Distributed Transaction Coordinator (MSDTC). As Figure 7.3 illustrates, the MOM installation program gives you the option to increase the MSDTC log file size, and it can launch the Component Services MMC for you. In the MMC, right-click My Computer, and select Stop MSDTC. Right-click My Computer, and select Properties to access the MSDTC log file settings. Increase the log file size as much as possible, with 512MB being a recommended minimum for production environments (possibly on its own drive array), and 64MB a recommended minimum for small or test environments. Clicking OK to confirm the changes has the same effect as clicking Reset Log. On the pop-up warning message, click Yes only if you are sure that it is OK to reset this log on your system. Finally, right-click My Computer, and select Start MSDTC.



Enabled items below may need to be installed on this computer before you install Microsoft Operations Manager 2000.

Click the enabled items for more information.

- ○ Windows 2000+
- ○ Microsoft Transaction Server
- ○ Microsoft Management Console 1.1+
- ○ Microsoft Internet Information Server
- ○ Access 2000 Run-time +
- ○ Internet Explorer 4.01+
- ○ Microsoft SQL Server or MSDE
- ○ Microsoft Data Access Components
- ○ Microsoft Office Graph Component
- ● MSDTC Logfile Size
- ○ Browscap.ini File

The MSDTC log file must be configured unless you are performing a User Interface install.

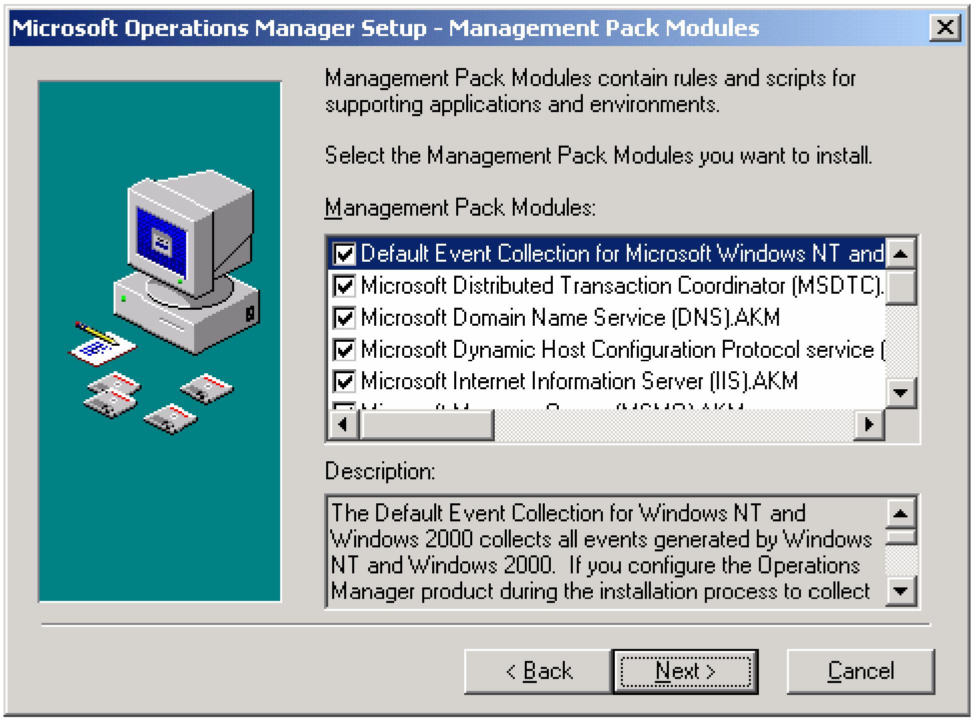
The Prerequisite Verifier has determined the Microsoft Distributed Transaction Coordinator (MSDTC) log file is currently configured with a maximum log file size of less than 512 MB. In a production environment, this setting should be 512 MB. To further optimize performance, place the log file on a dedicated drive.

In a small or test environment, the MSDTC maximum log file size should be at least 64 MB. In this case, the Prerequisite Verifier will still report the MSDTC log file size as being insufficient, but installation will not be affected.

Click here to configure MSDTC logfile size

Figure 7.3: The MOM installation program gives you the option to increase the MSDTC log file size.

During installation, you might want to add Management Pack Modules as Figure 7.4 shows.


Microsoft Operations Manager Setup - Management Pack Modules
< Back
Next >
Cancel

Management Pack Modules contain rules and scripts for supporting applications and environments.

Select the Management Pack Modules you want to install.

Management Pack Modules:

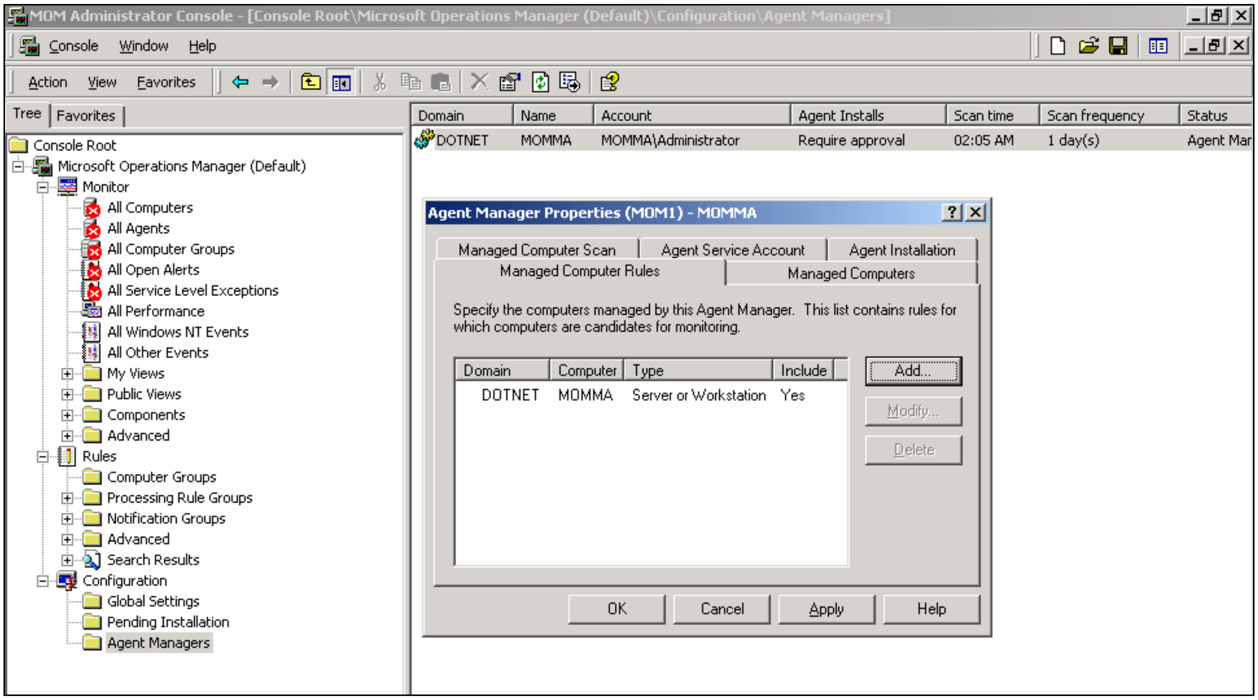
- ☑ Default Event Collection for Microsoft Windows NT and
- ☑ Microsoft Distributed Transaction Coordinator (MSDTC).
- ☑ Microsoft Domain Name Service (DNS).AKM
- ☑ Microsoft Dynamic Host Configuration Protocol service (
- ☑ Microsoft Internet Information Server (IIS).AKM

Description:

The Default Event Collection for Windows NT and Windows 2000 collects all events generated by Windows NT and Windows 2000. If you configure the Operations Manager product during the installation process to collect

Figure 7.4: Adding Management Pack Modules during MOM installation.

The next step in setting up MOM is to add the servers that will be monitored. MOM will discover the servers and push out agents to them if you authorize it. This process isn't well documented in MOM, so I have illustrated it. The first step is to right-click the Agent Managers folder in the MOM Administrator Console, and open the properties, as Figure 7.5 shows.



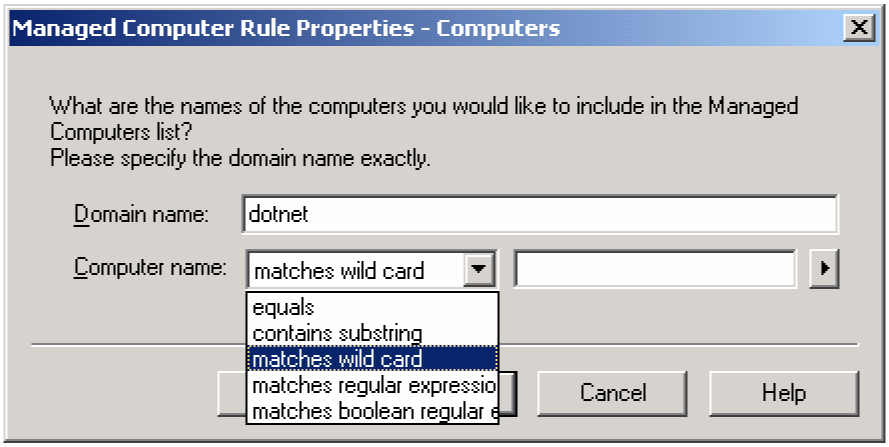
Domain	Name	Account	Agent Installs	Scan time	Scan frequency	Status
DOTNET	MOMMA	MOMMA\Administrator	Require approval	02:05 AM	1 day(s)	Agent Mar

Specify the computers managed by this Agent Manager. This list contains rules for which computers are candidates for monitoring.

Domain	Computer	Type	Include
DOTNET	MOMMA	Server or Workstation	Yes

Figure 7.5: Accessing the properties of the Agent Managers folder is the first step in selecting the computers to be managed by MOM.

Next, on the Managed Computer Rules tab, click Add, which will take you to the window that Figure 7.6 shows. This window lets you enter the domain name of the servers and a rule for matching the server names. If you want to find all computers in the domain, simply enter an asterisk (*). You can approve or reject the installation of MOM agents individually, so you don't need to worry about finding too many computers at this point (unless MOM has been previously configured to install without confirmation, but that is not the default setting).



Managed Computer Rule Properties - Computers

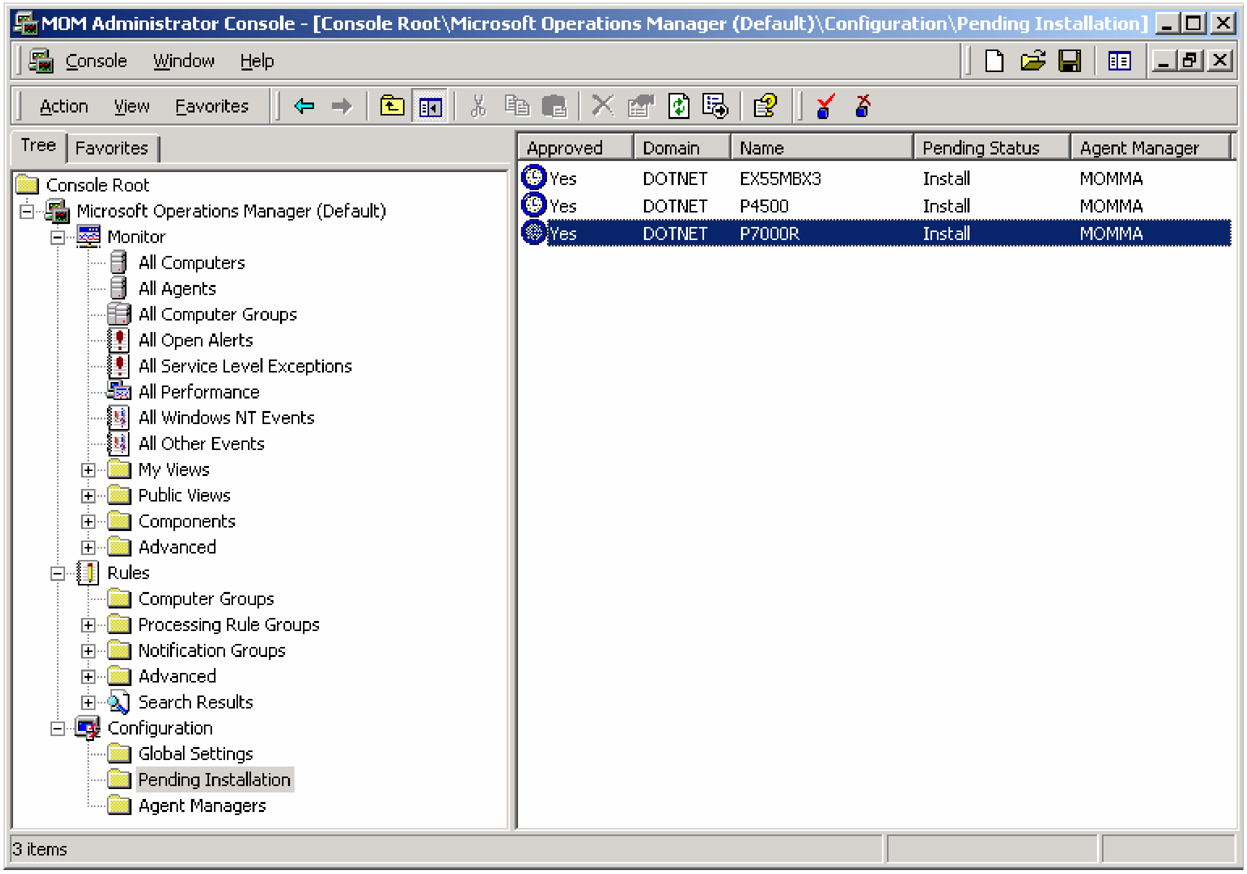
What are the names of the computers you would like to include in the Managed Computers list?
Please specify the domain name exactly.

Domain name: dotnet

Computer name: matches wild card

Figure 7.6: Selecting servers to monitor in MOM.

After MOM discovers the servers, you will see them listed in the Pending Installation folder under Configuration, as Figure 7.7 shows. In this figure, I have three new servers on which to install MOM, pending my approval.



MOM Administrator Console - [Console Root\Microsoft Operations Manager (Default)\Configuration\Pending Installation]

Approved	Domain	Name	Pending Status	Agent Manager
Yes	DOTNET	EX55MBX3	Install	MOMMA
Yes	DOTNET	P4500	Install	MOMMA
Yes	DOTNET	P7000R	Install	MOMMA

3 items

Figure 7.7: List of computers pending installation of MOM agents.

Integration with Other Applications

As Figure 7.8 shows, you can use Microsoft Visio Professional 2002 or later to diagram a SAN; a process that is made easier by an add-in called BrightStor SAN Designer from Computer Associates. This product works with Visio and allows you to create even complex SAN designs more easily, using either equipment from a specific vendor or generic SAN equipment icons.

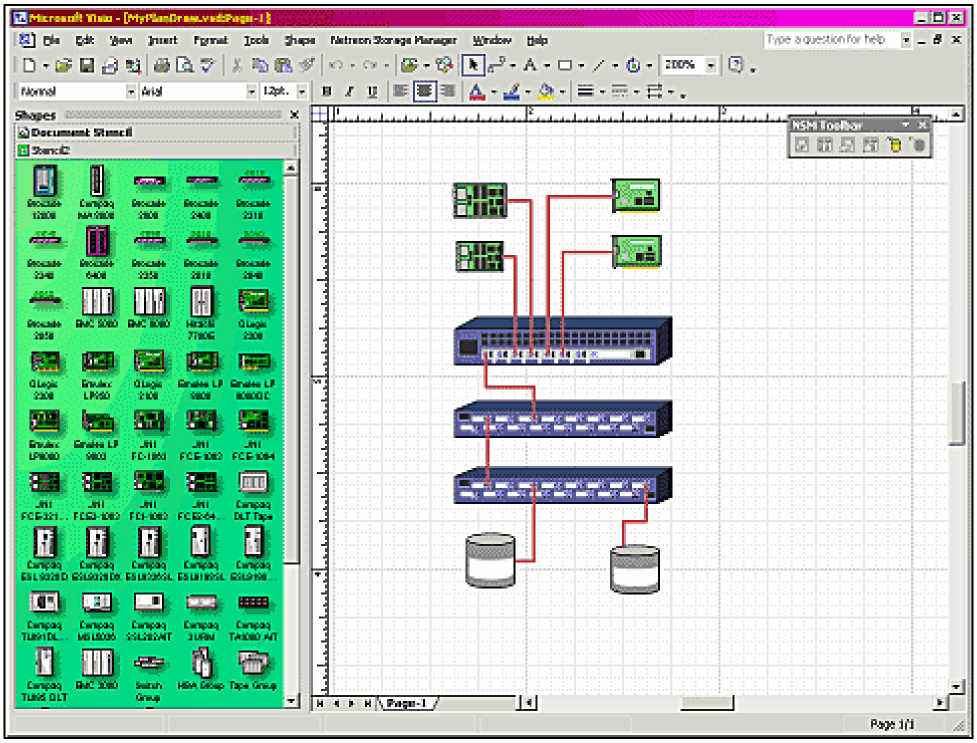


Figure 7.8: Using Microsoft Visio and BrightStor SAN Designer to diagram a SAN.

Improving the System

Although maintaining the status quo and avoiding problems is a good starting point, there is also a need to work to improve your systems. From the business standpoint, information systems are designed to give your business competitive advantage. On the horizon, there are always competitors to internal information systems departments—service providers—whose mission is to sell the same IT functions to the business as you, as a network administrator, provide, but from an external basis. For the service providers to be successful, they must provide competitive systems offerings, such as more efficient operations at a lower cost. They can also provide competitive advantages such as higher performance or guaranteed availability. If the business' internal information systems operations cannot provide these desired advantages, you are in danger of losing your job to service providers. One way to ensure job security is to maintain availability.

Maintaining Availability

In working with customers, I've determined that the key to maintaining and improving availability is to understand two components: the mean time between failures (MTBF) and the mean time to recover (MTTR). Combined, MTBF and MTTR determine the system availability.

Improving MTBF

Most studies of system downtime, especially those focused on storage systems, list the top causes of service interruptions as hardware failures, software crashes, and operator errors. So the best way to ensure availability is to implement redundant hardware systems and provide adequate operator training and change control. To protect against software crashes (in addition to change control, which can help minimize untested configurations from being deployed) and to protect against any remaining hardware faults, you can use clustering technologies.

There are many types of clustering in the Windows environment, from the Wolfpack clusters of Microsoft Cluster Server (MSCS) to devices that run multiple servers in lockstep, such as Marathon Technologies' Endurance solution (http://www.marathontechnologies.com). Both of these clustering options require specialized hardware that can add significantly to the cost. For MSCS, the storage must be on a bus that can be shared, either external SCSI (which limits both the distance and number of hosts) or fibre-channel (which is more flexible and costly).

Endurance requires a dual set of servers to separate the compute element from the I/O Processor (IOP), which maintains the storage and network connections. To connect the computer element and the IOP, the solution uses proprietary boards (Marathon Interconnects—MICs), essentially as an extension of the system bus. This setup lets the computer element and IOP pair be redundant (for a total of four physical servers acting as one logical server) and separated at a distance, up to the acceptable latency limits of the fibre-channel interconnects. In the near future, we may see these proprietary interconnect boards replaced by industry-standard InfiniBand boards.

Another option is to use servers that mirror all internal devices, including processor and memory, running all internal operations in lockstep. For any of these, the additional cost must be justified against the desired improvement in availability, or at least the improvement in MTBF; if something does go wrong on one of these specialized systems, you need to look at MTTR, and it may be more difficult to recover than on a standard server.

Improving MTTR

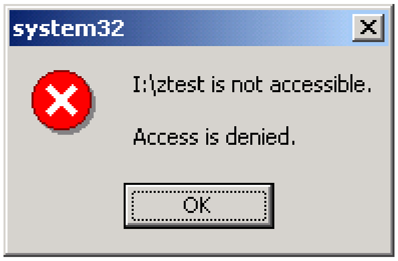
The primary method for reducing MTTR is to ensure that suitable system and information backups are being performed, and to ensure that recovery procedures are valid. The difficulty is gauging the value of these operations against the cost of performing them. The experienced IT manager or CIO knows the value of practicing recovery operations and decreasing recovery times, but you can easily let this necessity fall behind in day-to-day priorities and activities.

File Share Security

Up to this point, I have touched briefly on NTFS security, so let's consider this a final review of the subject, and perhaps a final examination to see how well you do. Recently, I worked on a project in which a shared directory was needed so that vendors and employees could place files in it, but they could not browse the directory or open the files. I was surprised at how difficult this process turned out to be for some systems administrators. Once you follow these steps, the process will make sense as you relate it to your knowledge of inheritable NTFS permissions, but if you perform the steps in the wrong order, the process will not work, which is what was preventing the systems administrators from creating the secure drop share.

Creating a Secure Drop Directory

The design goal is to have a drop folder that is available to anyone on the network to drop files into but is not available for anyone else but a select administrator (who can view the contents or execute files in that directory). For example, suppose the secure drop folder is called ztest. Two users, AB User and Secure (or groups of users instead of the individual accounts used in this scenario) can view the folder over the network. A member of the local administrators must be logged on to view the folder's properties. The share ztest should be under the Full Control of the account Secure. The share ztest should be visible to AB User over the network and allow write-only access to this user. As Figure 7.9 illustrates, if AB User attempts to open the ztest folder, access is denied.

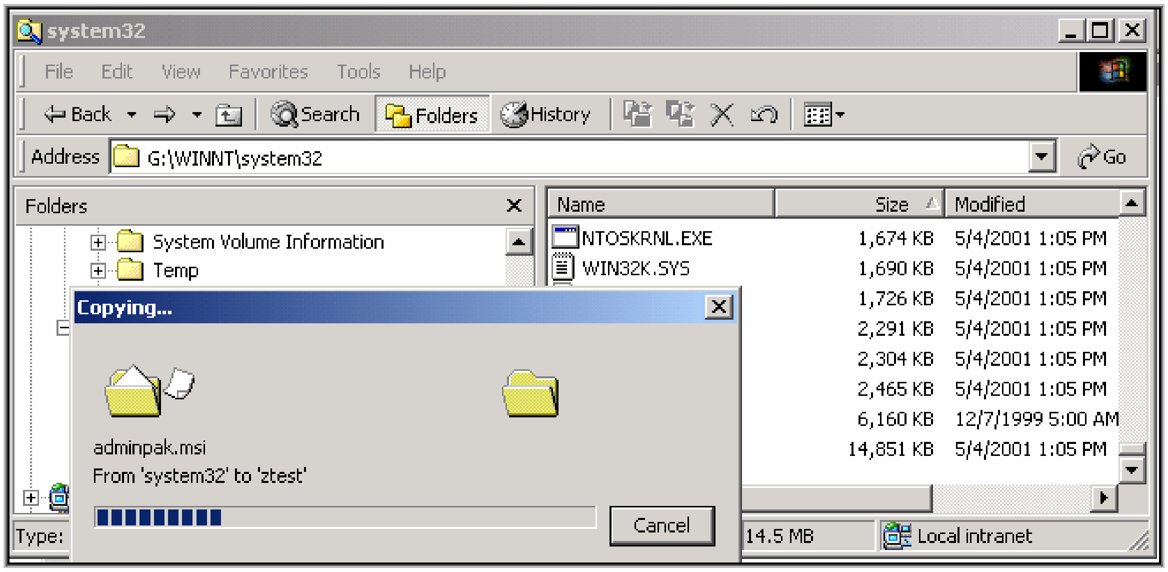

system32

I:\ztest is not accessible.

Access is denied.

Figure 7.9: Attempts by a non-administrator to open the secure drop share ztest are denied.

However, copying a file to the folder by any authenticated user does not result in access denied, as Figure 7.10 illustrates.



Address: G:\WINNT\system32

Folders: System Volume Information, Temp

Name	Size	Modified
NTOSKRNL.EXE	1,674 KB	5/4/2001 1:05 PM
WIN32K.SYS	1,690 KB	5/4/2001 1:05 PM
	1,726 KB	5/4/2001 1:05 PM
	2,291 KB	5/4/2001 1:05 PM
	2,304 KB	5/4/2001 1:05 PM
	2,465 KB	5/4/2001 1:05 PM
	6,160 KB	12/7/1999 5:00 AM
	14,851 KB	5/4/2001 1:05 PM

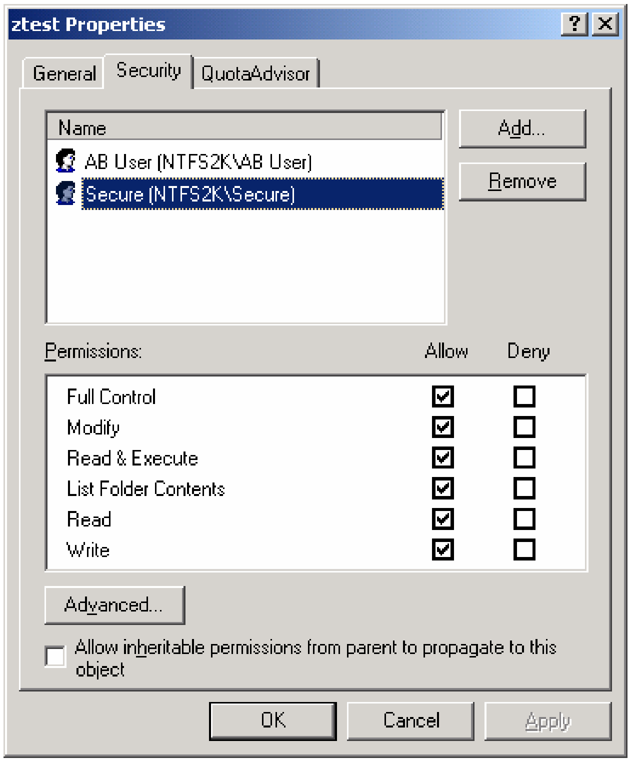
14.5 MB

Copying...

adminpak.msi
From 'system32' to 'ztest'

Figure 7.10: Non-administrator users can copy a file to the ztest folder.

The process of creating a secure drop share is not that tricky, but it has a few steps that must be done in the right order or it just won't work. Figure 7.11 shows the desired permissions for the Secure account, which will have Full Control access to the ztest folder.



ztest Properties

General | Security | QuotaAdvisor

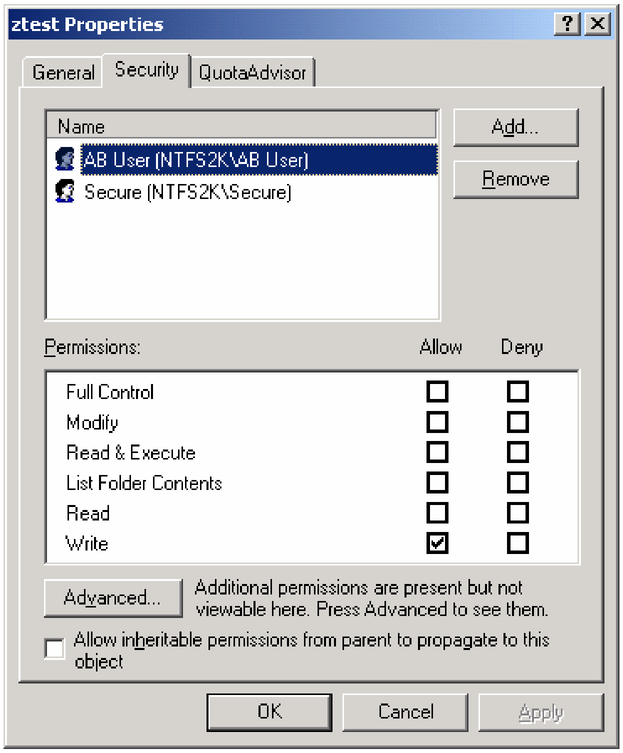
Name
- AB User (NTFS2K\AB User)
- Secure (NTFS2K\Secure)

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

□ Allow inheritable permissions from parent to propagate to this object

Figure 7.11: Desired permissions for the Secure account.

Figure 7.12 shows the correct permissions for the AB User account, which allow the user write-only permissions on the ztest folder.



ztest Properties

General | Security | QuotaAdvisor

Name
- AB User (NTFS2K\AB User)
- Secure (NTFS2K\Secure)

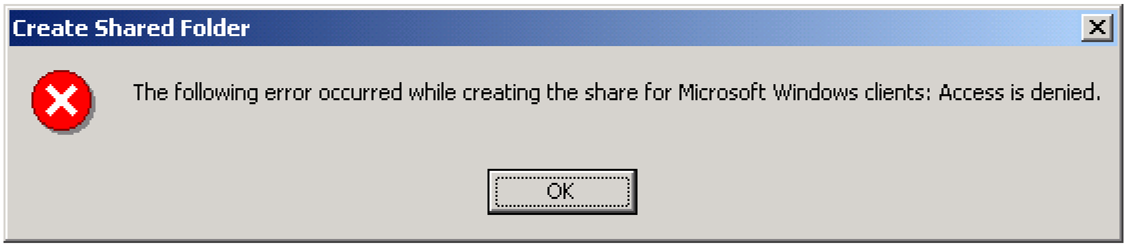
Permissions:	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	□	□
List Folder Contents	□	□
Read	□	□
Write	☑	□

Additional permissions are present but not viewable here. Press Advanced to see them.

□ Allow inheritable permissions from parent to propagate to this object

Figure 7.12: Desired permissions for AB User account.

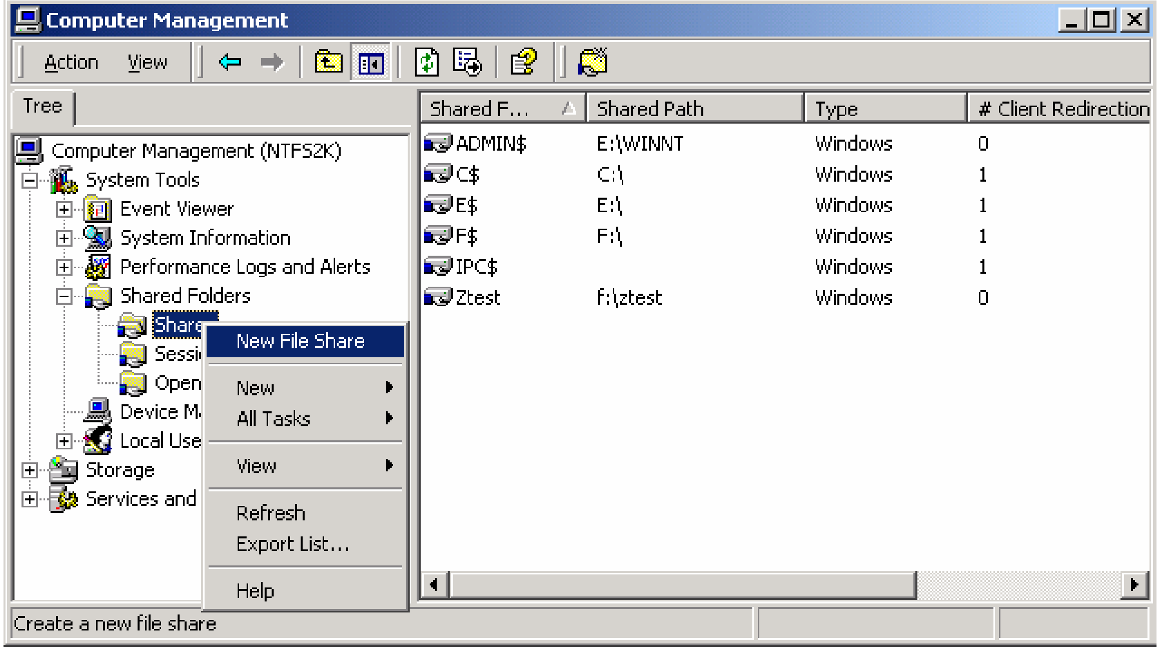
Figure 7.13 shows what happens if you attempt to set the NTFS permissions during the share-creation process. This error message can prevent some administrators from attempting to use this configuration. As the figure shows, if the process is performed in this order, you cannot even create the share!



The following error occurred while creating the share for Microsoft Windows clients: Access is denied.

Figure 7.13: The error message that results when permissions are applied during the shared folder creation.

Instead of using Windows Explorer to create shares, you can use the Computer Management MMC snap-in, which Figure 7.14 shows. Doing so has the following advantages: you can create shares on a remote computer and setting permissions on the folder is easier.



Shared F...	Shared Path	Type	# Client Redirection
ADMIN$	E:\WINNT	Windows	0
C$	C:\	Windows	1
E$	E:\	Windows	1
F$	F:\	Windows	1
IPC$		Windows	1
Ztest	f:\ztest	Windows	0

Create a new file share

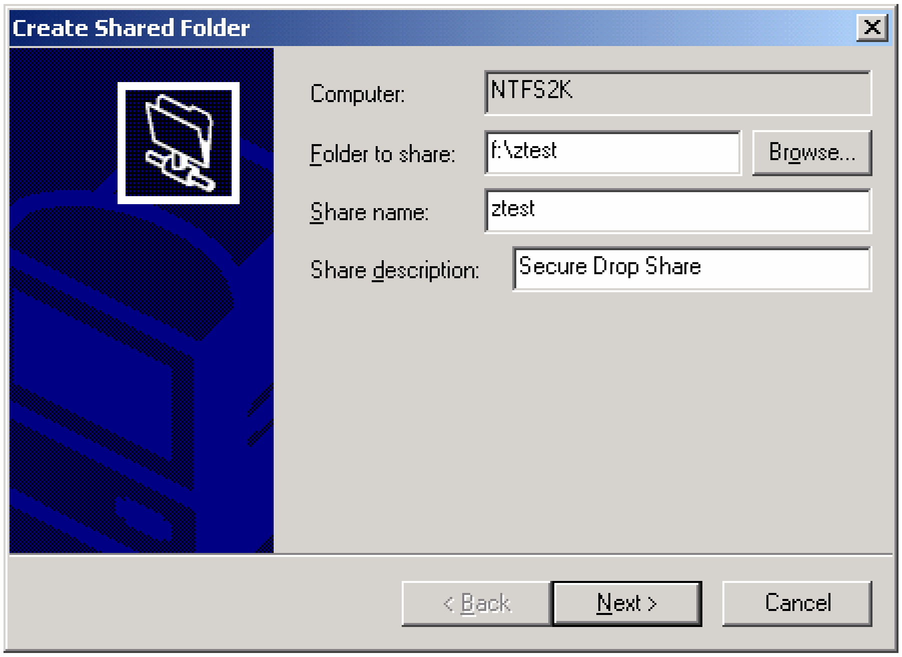
Figure 7.14: Using the Computer Management snap-in to remotely create a shared folder.

The following steps walk you through how to create and configure the ztest folder:

1. Create the folder on an NTFS partition, as Figure 7.15 shows.

> Note that the default permissions are Everyone Read for a newly-installed server, but your default permissions may be different depending on your configuration and whether or not your server was upgraded. If you have Everyone Full Control, you can leave it for now.

2. Share the folder either from the computer using Windows Explorer or remotely using the Computer Management snap-in.
3. Modify the Share Permissions to be Everyone Full Control. The default permissions provide only Read ability for the Everyone group.



Create Shared Folder

Computer: NTFS2K

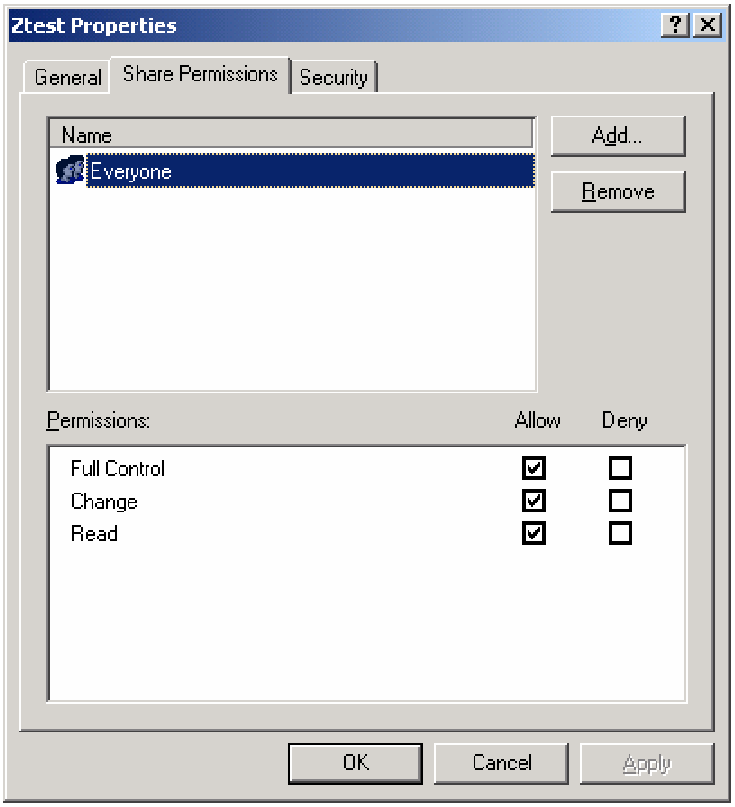
Folder to share: f:\ztest

Share name: ztest

Share description: Secure Drop Share

Figure 7.15: Creating the shared folder.

4. Open the newly created share properties and select the Security tab, as Figure 7.16 shows. Remove the Everyone group if it exists.



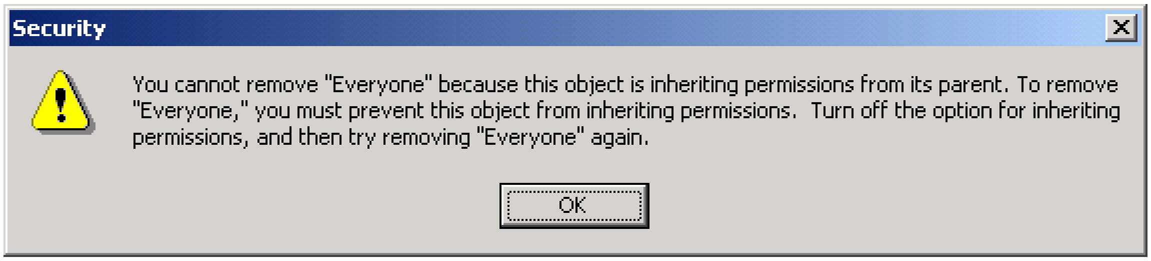
Name
Everyone

Permissions:

	Allow	Deny
Full Control	☑	☐
Change	☑	☐
Read	☑	☐

Figure 7.16: The default share permissions.

Usually you would not be able to remove the Everyone group using Windows Explorer to create shares. As Figure 7.17 shows, an error message occurs if you attempt to remove the Everyone group from a folder that inherits permissions.

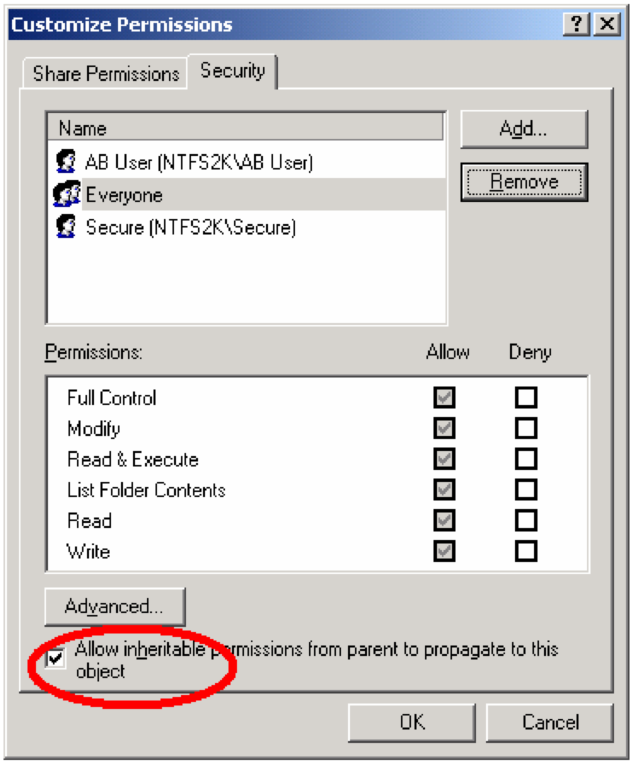


You cannot remove "Everyone" because this object is inheriting permissions from its parent. To remove "Everyone," you must prevent this object from inheriting permissions. Turn off the option for inheriting permissions, and then try removing "Everyone" again.

Figure 7.17: Error message that results from attempting to remove the Everyone group.

The big advantage of using the Computer Management snap-in to create and configure the shared folder is that the snap-in automatically clears the *Allow inheritable permissions* check box. However, if you are using Windows Explorer, you can work around the error message in Figure 7.17 using the following steps:

1. As Figure 7.18 shows, if you're using Windows Explorer to create and configure the share, you must clear the *Allow inheritable permissions* check box before you can configure the permissions. As the figure shows, the permissions check boxes will be grayed until you clear this check box.



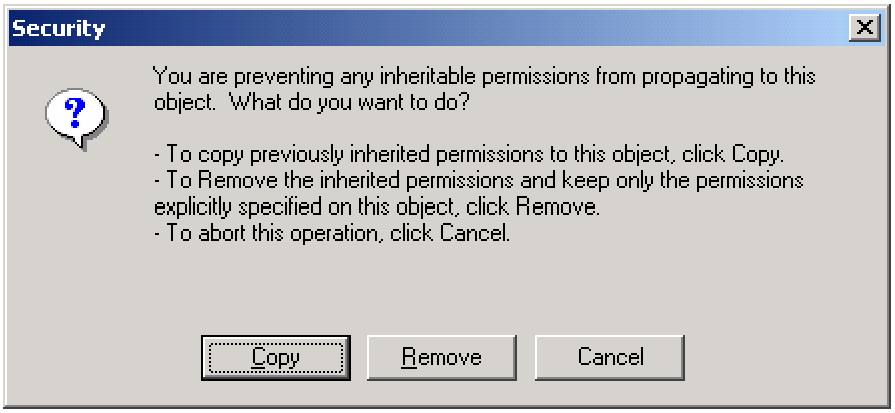
Name
- AB User (NTFS2K\AB User)
- Everyone
- Secure (NTFS2K\Secure)

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

Figure 7.18: Clear the Allow inheritable permissions check box to configure the folder's permissions.

2. After you clear this check box, you will be presented with the pop-up message that Figure 7.19 shows. Click Remove in this dialog box.

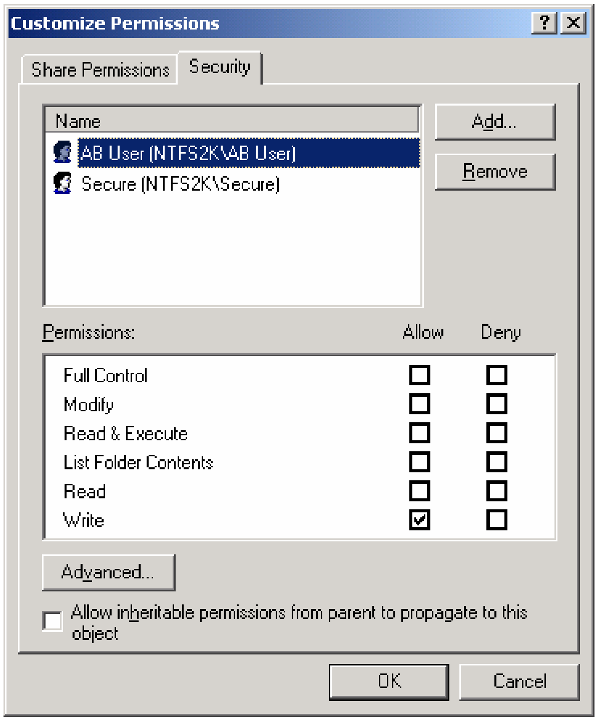


You are preventing any inheritable permissions from propagating to this object. What do you want to do?

- To copy previously inherited permissions to this object, click Copy.
- To Remove the inherited permissions and keep only the permissions explicitly specified on this object, click Remove.
- To abort this operation, click Cancel.

Figure 7.19: The pop-up message that results from clearing the Allow inheritable permissions check box.

3. In the Customize Permissions window, which Figure 7.20 shows, clear the Read check box under Allow, but leave the Write check box under Allow selected.



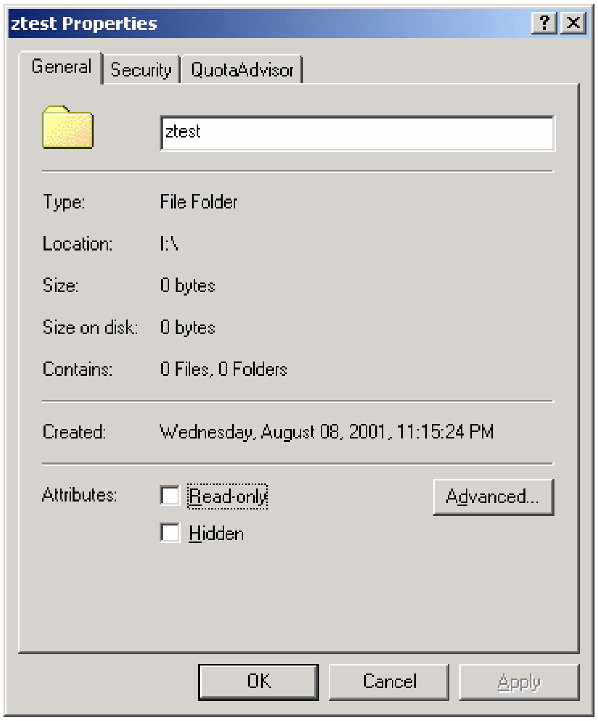
Name
AB User (NTFS2K\AB User)
Secure (NTFS2K\Secure)

Permissions:	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	□	□
List Folder Contents	□	□
Read	□	□
Write	☑	□

□ Allow inheritable permissions from parent to propagate to this object

Figure 7.20: Setting write-only permissions for the secure drop share.

As Figure 7.21 shows, AB User cannot even see the size of files and folders.



ztest

Type: File Folder

Location: I:\

Size: 0 bytes

Size on disk: 0 bytes

Contains: 0 Files, 0 Folders

Created: Wednesday, August 08, 2001, 11:15:24 PM

Attributes: □ Read-only

□ Hidden

Figure 7.21: AB User cannot see the size of files and folders.

Ongoing Process of Storage Management

From here, the process of storage management will consist of everything from designing and deploying the appropriate storage systems to developing the techniques to manage them. Traditionally, storage management starts with defining the types of information that will be stored, and developing the appropriate type of storage to house it. Next, information is classified and prioritized so that appropriate protection and disaster recovery procedures can be implemented. Once the storage is online and adequately protected (from both a security perspective as well as fault protection, such as RAID), the storage monitoring begins, ensuring availability and performance. Integrity of the information will need to be maintained as well (protecting the data from corruption as well as ensuring that the information is necessary for the business). Finally, future storage requirements will need to be anticipated and met; this process involves selecting the best technology and making sure that the technology is distributed and used wisely. Table 7.3 will help you keep track of the recurring tasks that comprise storage and information systems management.

Priority	**Task**	**Recurrence**	**Estimate of Time Needed**	**Details and Example**	**Resources**
1	Monitor server and storage availability	Real-time	Hours, unless automated	Verify servers are online and not reporting any failed hardware or predicted hardware failures (such as members of RAID disk sets), verify that services are running, and verify that disk storage is available to users and applications	
	SRM tools, WS2K3 Performance Monitor, application monitors, hardware reporting tools, and the system information in the Computer Management console				
2	Monitor information flow	Periodically, such as ping every hour	Hours, unless automated	Ensure that network transport is active and mail queues or file transfers are not queuing up	Application or transport-specific automation tools

Priority	Task	Recurrence	Estimate of Time Needed	Details and Example	Resources
3	Troubleshoot and support	Daily, on demand	2 to 4 hours	Respond to support requests on the end-user or server level	Help desk support system
4	Document change control	Daily, as needed (as changes occur)	30 minutes	Record changes to the servers, storage, and network environment	Auditing or surveying tools
5	Perform backups	Daily, weekly	4 to 8 hour window, hands-on is time minimal	Application data and system state backups	NT Backup and other backup software
6	Review security logs	Daily, as needed (as changes occur)	30 minutes	Review Windows event logs and application-specific logs	Event log filtering, and monitoring tools that read the event logs (for example, MOM)
7	Monitor storage utilization	At least weekly, automation makes this process more real-time	Hours, unless automated	Check for available free disk space, perform usage forecast (trend analysis), and run reports on duplicate, aged, and unwanted file types	SRM tools and WS2K3 Performance Monitor
8	Routine maintenance	Weekly	1 to 2 hours per system	Includes offline defragmentation, removing temporary files, and so on	Disk defragmenter or database-application specific utilities
9	Patch or update systems	Monthly or more often if there is a security issue	1 hour per system; schedule change control if updates involve downtime	Hotfixes and service packs for OSs, and firmware updates such as ROM flashes	Windows Update, security bulletins, and the QChain tool for applying WS2K3 hotfixes
10	Document environment and current project status	Daily or weekly, as needed (as changes occur)	30 minutes	Update the documentation of the network and storage systems and prepare reports for management	Visio, SMS, and other tracing tools; and project status emails and Microsoft Project Gantt charts

Priority	Task	Recurrence	Estimate of Time Needed	Details and Example	Resources
11	Monitor server and storage performance	At least weekly, automation makes this process more real-time	15 to 30 minutes	Measure the storage performance compared with baseline or last-known state—Is performance adequate?	WS2K3 Performance Monitor and hardware-specific tools such as SCSI or fibre-channel diagnostic utilities
12	Review directory	Weekly	15 to 30 minutes	Check for inactive user and computer accounts	Resources depend on the directory (for example, Active Directory Users and Computers for AD)
13	Validate backups	Monthly	2 to 6 hours	Perform an offline server recovery and ensure that backups and recovery procedures are valid	Backup software and standby recovery systems
14	Perform security audit	Annually or quarterly	8 hours	Perform intrusion-detection audits and attempts to breach security	Intrusion detection tools, security consultants, and the Microsoft security toolkit
15	Research new technologies	Annually, as needed	Varies	Keep up-to-date on improvements in technologies and update professional certifications	Web sites and email subscriptions such as InfoStor news and Storage UPDATE from the *Windows & .NET Server Magazine* network
16	Upgrade systems	Annually, as needed	Entire days	Ongoing upgrades to servers and storage systems	Keep track in configuration log, including needed changes
17	Pointless meetings	Too often	Eternity	Keep a sense of humor here, I'm only joking!	Dilbert books and cartoons

Table 7.3: Storage systems management recurring tasks.

Summary

The goal of this chapter is to aid you in developing a daily approach to SRM that automates repetitive tasks, for example monitoring disk usage by using the SRM software that we have discussed. This approach will free your time for other crucial tasks, such as maintaining your security defenses, which we explored. We finished the SRM deployment by setting up systems to monitor and maintain the SRM solution. We covered the technical aspects of what you need to monitor and what solutions are available. I gave you a complete list of systems management recurring tasks that you can use to make sure that you have all your operations in place, including SRM functions. Without a daily approach, important tasks might get squeezed out, as you only have so much time, and must continually fight to ensure that your priorities match those of the business.

In the next chapter, we will look at the future of storage and SRM, including both hardware technology and software changes. First, we'll look at the immediate future—at changes that are happening all around us—that you'd be wise to learn about and consider. Then I'll take a more predictive look into the future and attempt to divine what the predominant or surviving technologies and standards will be.

Much of the next chapter will focus on networked storage, as that is clearly where the most improvement and increases in adoption will occur. In the area of hardware, we'll look at changes in speeds and feeds as we get faster pipes and possibly even greater distances. One of the upcoming changes is in virtualization of devices and storage, which we touched upon earlier. In the next chapter, we will also look at what these changes mean from a storage management perspective. We will look at the server side of storage networks, changes in host bus adapters (HBAs), booting from the SAN, and multi-path I/O and what it means for performance and fault tolerance.

No discussion would be complete without covering disaster recovery, so we will look at distance mirroring, cloning, snapshots, and serverless backup. Some of these technologies exist today, albeit in their infancy, so we will look at where they will need to go to speed adoption.