Microsoft®

Administrator's Pocket Consultant

# Microsoft® WINDOWS SERVER 2003

William R. Stanek

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Cataloging-in-Publication Data pending.

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWE 8 7 6 5 4 3

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to *mspinput@microsoft.com*.

**Acquisitions Editor:** Juliana Aldous Atkinson
**Project Editor:** Julie Miller
**Technical Editor:** Toby Andrews

Body Part No. X08-04490

# Table of Contents

## Part I
## Microsoft Windows Server 2003 Administration Fundamentals

Part II

## Microsoft Windows Server 2003 Directory Service Administration

Part III
**Microsoft Windows Server 2003 Data Administration**

## 14 Data Sharing, Security, and Auditing 315

## Part IV
## Microsoft Windows Server 2003 Network Administration

# Tables

## Chapter 2

# Managing Servers Running Microsoft Windows Server 2003

Servers are the heart of any Microsoft Windows network. One of your primary responsibilities as an administrator is to manage these resources. Your key tool is the Computer Management console, which provides a single integrated interface for handling such core system administration tasks as

- Managing user sessions and connections to servers
- Managing file, directory, and share usage
- Setting administrative alerts
- Managing applications and network services
- Configuring hardware devices
- Viewing and configuring disk drives and removable storage devices

Although the Computer Management console is great for remote management of network resources, you also need a tool that gives you fine control over system environment settings and properties. This is where the System utility comes into the picture. You'll use this utility to

- Configure application performance, virtual memory, and registry settings
- Manage system and user environment variables
- Set system startup and recovery options
- Manage hardware and user profiles

## Managing Networked Systems

The Computer Management console is designed to handle core system administration tasks on local and remote systems. You'll spend a lot of time working with this tool, and you should get to know every nook and cranny. Access the Computer Management console with either of the following techniques:

- Choose Start, then Programs or All Programs as appropriate, then Administrative Tools, and finally Computer Management.
- Select Computer Management from the Administrative Tools folder.

As Figure 2-1 shows, the main window has a two-pane view that's similar to Windows Explorer. You use the console tree in the left pane for navigation and tool selection. Tools are divided into three broad categories:

- **System Tools** Provides access to general-purpose tools for managing systems and viewing system information
- **Storage** Displays information on removable and logical drives and provides access to drive management tools
- **Services And Applications** Lets you view and manage the properties of services and applications installed on the server

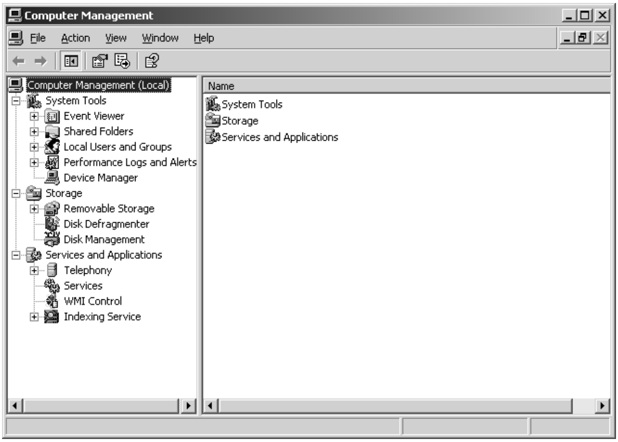


**Figure 2-1.** *Use the Computer Management console to manage network computers and resources.*

The tools available through the console tree provide the core functionality for the Computer Management console. When Computer Management is selected in the console tree, you can easily access three important tasks:

- Connect to other computers
- Send console messages
- Export information lists

The following sections examine these tasks, and then we'll take a detailed look at working with tools in the Computer Management console.

## Connecting to Other Computers

The Computer Management console is designed to be used with local and remote systems. You can select a computer to manage by completing the following steps:

1. Right-click the Computer Management entry in the console tree and then select Connect To Another Computer on the shortcut menu. This opens the Select Computer dialog box.

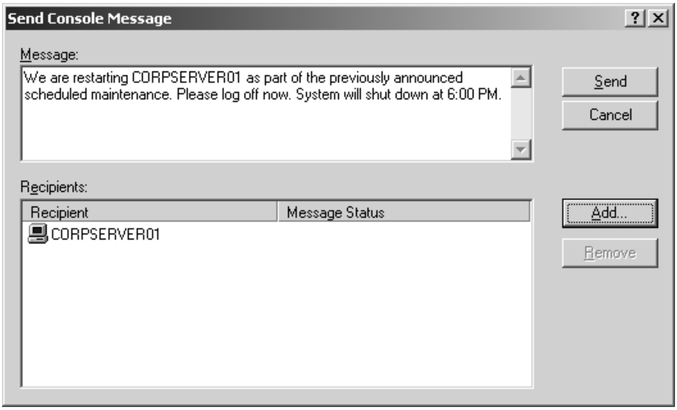
2. Choose Another Computer and then type the fully qualified name of the computer you want to work with, such as engsvr01.technology.microsoft.com, where *engsvr01* is the computer name and *technology.microsoft.com* is the domain name. Or click Browse to search for the computer you want to work with.
3. Click OK.

## Sending Console Messages

You can use the Computer Management console to send messages to users logged on to local or remote systems. These messages appear in a dialog box that the user must click to close.

You send messages to remote users by completing the following steps:

1. In the Computer Management console, right-click the Computer Management entry in the console tree. Then, on the shortcut menu, select All Tasks and then choose Send Console Message. This opens the dialog box shown in Figure 2-2.



Send Console Message

Message: We are restarting CORPSERVER01 as part of the previously announced scheduled maintenance. Please log off now. System will shut down at 6:00 PM.

Recipients:

| Recipient | Message Status |
|---|---|
| CORPSERVER01 | |

**Figure 2-2.** *Use the Send Console Message dialog box to send console messages to other systems.*

2. Type the text of the message in the Message area. In the Recipients area, you should see the name of the computer you're currently connected to.
3. If you want to send a message to users of this system, click Send. Otherwise, use the Add button to add recipients or the Remove button to delete a selected recipient. Then, when you're ready to send the message, click Send.

**Note** Only users logged on to the selected system will receive the message. Other users won't. Additionally, Windows NT, Windows 2000, Windows XP, and Windows Server 2003 systems must be running the Messenger service to send and receive console messages. Windows 95 and Windows 98 systems running the WinPopup utility can also send and receive console messages.

## Exporting Information Lists

The ability to export information lists is one of my favorite features of the Computer Management console, and if you maintain system information records or regularly work with Windows scripting it'll probably be one of yours, too. The Export List feature allows you to save textual information displayed in the right pane to a tab-delimited or comma-delimited text file. You could, for example, use this feature to save detailed information on all the services running on the system by completing the following steps:

1. In the Computer Management console, click the plus sign (+) next to the System Tools node. This expands the node to display its tools.
2. Right-click Event Viewer, and then from the shortcut menu select Export List. This opens the Export List dialog box.
3. Use the Save In selection list to choose the save location and then enter a name for the export file.
4. Use the Save As Type selection list to set the formatting of the export file. You can separate columns of information with tabs or commas and save as ASCII text or Unicode text. In most cases you'll want to use ASCII text.
5. Click Save to complete the export process.

You can use a similar procedure to export lists of other information displayed in the Computer Management console.

## Using Computer Management System Tools

The Computer Management system tools are designed to manage systems and view system information. The available system tools are

- **Event Viewer** View the event logs on the selected computer. Event logs are covered in "Event Logging and Viewing" in Chapter 3, "Monitoring Processes, Services, and Events."
- **Shared Folders** Manage the properties of shared folders, user sessions, and open files. Managing user sessions, open files, and network shares is covered in Chapter 13, "Managing Files and Folders."
- **Local Users And Groups** Manage local users and local user groups on the currently selected computer. Working with users and groups is covered in Part II, "Microsoft Windows Server 2003 Directory Service Administration," along with other types of accounts that you can manage in the Active Directory directory service.

**Note** Local users and local user groups aren't a part of Active Directory and are managed instead through the Local Users And Groups view. Domain controllers don't have entries in the Local Users And Groups view.

- **Performance Logs And Alerts** Monitor system performance and create logs based on performance parameters. You can also use this tool to notify or alert users of performance conditions. For more information on alerts and monitoring systems, see Chapter 3.

- **Device Manager** Use as a central location for checking the status of any device installed on a computer and for updating the associated device drivers. You can also use it to troubleshoot device problems. Managing devices is covered later in the chapter.

## Using Computer Management Storage Tools

The Computer Management storage tools display drive information and provide access to drive management tools. The available storage tools are

- **Removable Storage** Manages removable media devices and tape libraries. Tracks work queues and operator requests related to removable media devices.
- **Disk Defragmenter** Corrects drive fragmentation problems by locating and combining fragmented files.
- **Disk Management** Manages hard disks, disk partitions, volume sets, and redundant array of independent disks (RAID) arrays. Replaces the Disk Administrator utility in Windows NT 4.0.

Working with files, drives, and storage devices is the subject of Part III, "Microsoft Windows Server 2003 Data Administration."

## Working with Services and Applications

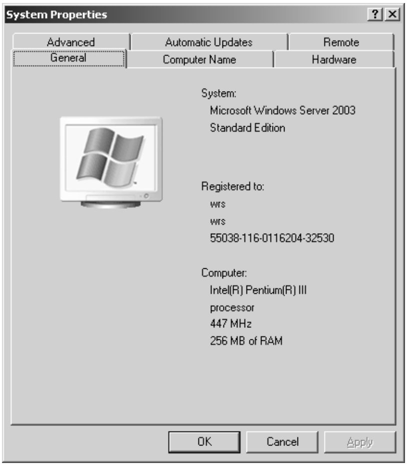
You use the Computer Management services and applications tools to manage services and applications installed on the server. Any application or service-related task that can be performed in a separate tool can be performed through the Services And Applications node as well. For example, if the currently selected system has Dynamic Host Configuration Protocol (DHCP) installed, you can manage DHCP through the Server Applications And Services node. You could also use the DHCP tool in the Administrative Tools folder. You can perform the same tasks either way.

This technology is possible because the DHCP tool is a Microsoft Management Console (MMC) snap-in. When you access the DHCP tool in the Administrative Tools folder, the snap-in is displayed in a separate console. When you access the DHCP tool through the Server Applications And Services node, the snap-in is displayed within the Computer Management console. Working with services and applications is discussed in Chapter 3 and elsewhere in this book.

# Managing System Environments, Profiles, and Properties

You use the System utility to manage system environments, profiles, and properties. To access the System utility, double-click System in the Control Panel. This displays the System Properties dialog box.

As shown in Figure 2-3, the System Properties dialog box is divided into six tabs. Each of these tabs is discussed in the sections that follow.



System:
Microsoft Windows Server 2003
Standard Edition

Registered to:
wrs
wrs
55038-116-0116204-32530

Computer:
Intel(R) Pentium(R) III
processor
447 MHz
256 MB of RAM

**Figure 2-3.** *Use the System utility to manage system environment variables, profiles, and properties.*

## The General Tab

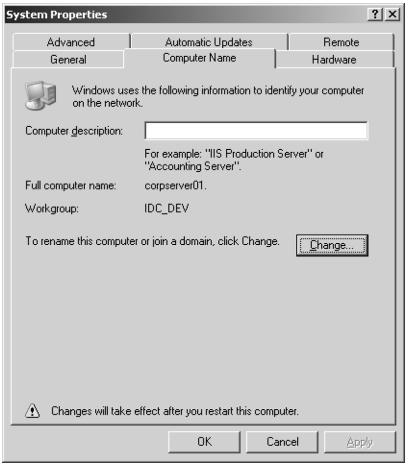
General system information is available for any server running Windows Server 2003 through the System utility's General tab, which is shown in Figure 2-3. To access the General tab, start the System utility by double-clicking the System icon in the Control Panel.

The information provided in the General tab includes

- Operating system version and service pack
- Registered owner
- Windows serial number
- Computer type
- Amount of RAM installed on the computer
- Processor type
- Total system RAM

## The Computer Name Tab

You can display and modify the computer's network identification with the System utility's Computer Name tab, shown in Figure 2-4. As the figure shows, the tab displays the full computer name of the system and the domain membership. The full computer name is essentially the Domain Name System (DNS) name of the computer, which also identifies the computer's place within the Active Directory hierarchy.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name: corpserver01.

Workgroup: IDC_DEV

To rename this computer or join a domain, click Change.

Changes will take effect after you restart this computer.

**Figure 2-4.** *Use the Computer Name tab to display and configure system identification. Notice that you can't change the identification or access information for domain controllers.*

To access the Network Identification tab, start the System utility by double-clicking the System icon in the Control Panel; then click the Computer Name tab. You can now click Change to change the system name and domain associated with the computer.

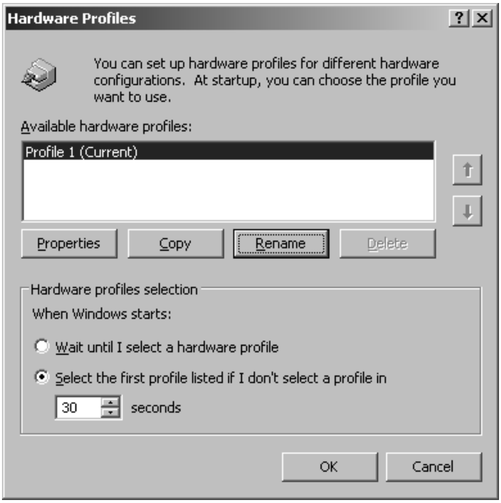
## The Hardware Tab

Servers running Windows Server 2003 can use multiple hardware profiles. Hardware profiles are most useful for mobile servers, such as those configured on laptops. Using hardware profiles, you can configure one profile for when the computer is connected to the network (*docked*) and one profile for when the computer is mobile (*undocked*).

### Configuring the Way Hardware Profiles Are Used

To configure hardware profiles, click the System utility's Hardware tab and then click the Hardware Profiles button. This opens the dialog box shown in Figure 2-5. As with systems with multiple operating systems, Windows Server 2003 allows you to configure the way hardware profiles are used as follows:

- Set a default profile by changing the profile's position in the Available Hardware Profiles list. The top profile is the default profile.
- Determine how long the system displays the startup hardware profile menu by setting a value using the field Select The First Profile Listed If I Don't Select A Profile In. The default value is 30 seconds.
- Have the system wait indefinitely for user input by selecting Wait Until I Select A Hardware Profile.



You can set up hardware profiles for different hardware configurations. At startup, you can choose the profile you want to use.

Available hardware profiles:

Profile 1 (Current)

Hardware profiles selection

When Windows starts:

○ Wait until I select a hardware profile

● Select the first profile listed if I don't select a profile in

30 seconds

**Figure 2-5.** *You can configure multiple hardware profiles for any Windows Server 2003 system.*

## Configuring for Docked and Undocked Profiles

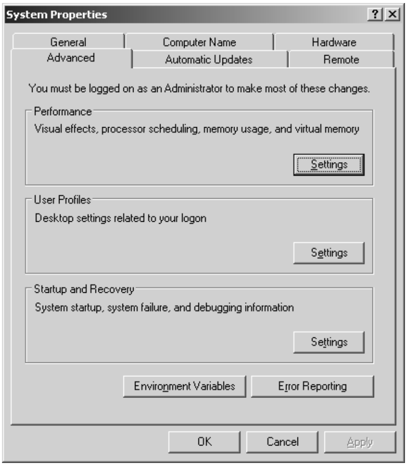
To configure a computer for docked and undocked profiles, complete the following steps:

1. In the Available Hardware Profiles list, select the default profile, and then click Copy.
2. In the Copy Profile dialog box, type a name for the Docked profile in the To field.
3. Select the new profile, and then click the Properties button.
4. Select the This Is A Portable Computer check box, and then choose The Computer Is Docked.
5. Select Always Include This Profile As An Option When Windows Starts, and then click OK.
6. Select the default profile in the Available Hardware Profiles list, and then click Copy.
7. In the Copy Profile dialog box, type a name for the Undocked profile in the To field.
8. Select the new profile, and then click the Properties button.
9. Select the This Is A Portable Computer check box, and then choose The Computer Is Undocked.
10. Select Always Include This Profile As An Option When Windows Starts, and then click OK.
11. Now set the default hardware profile as appropriate for the computer's current state as either docked or undocked.
12. You're done. Click OK.

When the system is booted, the hardware profiles are displayed, and you can select the appropriate profile.

## The Advanced Tab

The System utility's Advanced tab, shown in Figure 2-6, controls many of the key features of the Windows operating system, including application performance, virtual memory usage, user profile, environment variables, and startup and recovery. To access the Advanced tab, start the System utility by double-clicking the System icon in the Control Panel; then click the Advanced tab.



You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your logon

System startup, system failure, and debugging information

**Figure 2-6.** *The Advanced tab lets you configure advanced options, including performance options, environment variables, and startup and recovery.*

### Setting Windows Performance

Many graphics enhancements have been added to the Windows Server 2003 interface. These enhancements include many visual effects for menus, toolbars, windows, and the taskbar. To ensure that the server performs at its best level, these options are turned off by default in an initial installation. This reduces the amount of work the server must do when administrators log on locally to perform tasks, and you shouldn't change this default setting in most cases. However, if you need to modify these options, you can do so by following these steps:

1. Click the Advanced tab in the System utility, and then click the Settings button in the Performance panel to display the Performance Options dialog box.
2. The Visual Effects tab should be selected by default. You have the following options for controlling visual effects:
   - **Let Windows Choose What's Best For My Computer** Allows the operating system to choose the performance options based on the hardware configuration. On a server, this typically means that Windows selects only the Use Visual Styles On Windows And Buttons option and that all other options are cleared.

- **Adjust For Best Appearance** When you optimize Windows for best appearance, you enable all visual effects for all graphical interfaces. Menus and the taskbar use transitions and shadows. Screen fonts have smooth edges. List boxes have smooth scrolling. Folders use Web views and more. On a server, this setting unnecessarily uses a lot of memory and system resources, and you should rarely use it.
- **Adjust For Best Performance** When you optimize Windows for best performance, you turn off the resource-intensive visual effects, such as slide transitions and smooth edges for fonts, while maintaining a basic set of visual effects. In some cases this completely turns off all visual effects.
- **Custom** You can customize the visual effects as well. To do this, select or clear the visual effects options in the Performance Options dialog box. If you clear all options, Windows doesn't use visual effects.

3. When you're finished changing visual effects, click OK and then click OK again.

## Setting Application Performance

Application performance is related to processor scheduling and memory caching options that you set for the Windows Server 2003 system. Processor Scheduling determines the responsiveness of the current active application (as opposed to background applications that might be running on the system). Memory Caching determines whether physical memory is optimized for applications or the system cache.

You control application performance by completing the following steps:

1. Access the Advanced tab in the System utility, and then display the Performance Options dialog box by clicking the Settings button in the Performance panel. Select the Advanced tab to modify the performace settings.
2. The Processor Scheduling panel has two options:
   - **Programs** To give the active application the best response time and the greatest share of available resources, select Applications. Generally, you'll want to use this option for Application, Web, and Streaming Media servers.
   - **Background Services** To give background applications a better response time than the active application, select Background Services. Generally, you'll want to use this option for Active Directory, File, Print, and Network and Communications servers.
3. The Memory Usage panel has two options:
   - **Programs** Choose this option to optimize physical memory usage for applications. Generally, you'll want to use this option for Application, Web, and Streaming Media servers.
   - **System Cache** Choose this option to optimize physical memory usage for the system cache. Generally, you'll want to use this option for Active Directory, File, Print, and Network and Communications servers.
4. Click OK.

## Configuring Virtual Memory

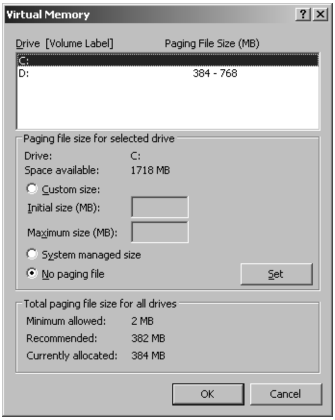
Virtual memory allows you to use disk space to extend the amount of available RAM on a system. This feature of Intel 386 and later processors writes RAM to disks using a process called *paging*. With paging, a set amount of RAM, such as 32 MB, is written to the disk as a paging file, where it can be accessed from the disk when needed.

An initial paging file is created automatically for the drive containing the operating system. By default, other drives don't have paging files, and you must create these paging files manually if you want them. When you create a paging file, you set an initial size and a maximum size. Paging files are written to the volume as a file called Pagefile.sys.

**Best Practices** Microsoft recommends that you create a paging file for each physical volume on the system. On most systems, multiple paging files can improve the performance of virtual memory. Thus, instead of a single large paging file, it's better to have several small ones. Keep in mind that removable drives don't need paging files.

You can configure virtual memory by completing the following steps:

1. Start the System utility, and then click the Advanced tab.
2. Click Setting in the Performance panel to display the Performance Options dialog box, and then select the Advanced tab. Then click Change to display the Virtual Memory dialog box shown in Figure 2-7.



Virtual Memory

| Drive [Volume Label] | Paging File Size (MB) |
|---|---|
| C: | |
| D: | 384 - 768 |

Paging file size for selected drive

Drive: C:

Space available: 1718 MB

○ Custom size:

Initial size (MB):

Maximum size (MB):

○ System managed size

● No paging file

Total paging file size for all drives

Minimum allowed: 2 MB

Recommended: 382 MB

Currently allocated: 384 MB

**Figure 2-7.** *Virtual memory extends the amount of RAM on a system.*

This dialog box has three key areas:

- ***Drive* [*Volume Label*]** Shows how virtual memory is currently configured on the system. Each volume is listed with its associated paging file (if any). The paging file range shows the initial and maximum size values set for the paging file.

- **Paging File Size For Selected Drive** Provides information on the currently selected drive and allows you to set its paging file size. Space Available tells you how much space is available on the drive.
- **Total Paging File Size For All Drives** Provides a recommended size for virtual RAM on the system and tells you the amount currently allocated. If this is the first time you're configuring virtual RAM, you'll note that the recommended amount has already been given to the system drive (in most instances).

**Best Practices** Although Windows Server 2003 can expand paging files incrementally as needed, this can result in fragmented files, which slow system performance. For optimal system performance, set the initial size and maximum size to the same value. This ensures that the paging file is consistent and can be written to a single contiguous file (if possible, given the amount of space on the volume). In most cases I recommend setting the total paging file size so that it's twice the physical RAM size on the system. For instance, on a computer with 512 MB of RAM, you would ensure that the Total Paging File Size For All Drives setting is at least 1024 MB. However, on servers with 2 GB or more of RAM, it's best to follow the hardware manufacturer's guidelines for paging file sizes.

3. In the Drive list box, select the volume you want to work with.
4. Use the Paging File Size For Selected Drive area to configure the paging file for the drive. Select Custom Size. Then enter an initial size and a maximum size and click Set to save the changes.
5. Repeat Steps 3 and 4 for each volume you want to configure.

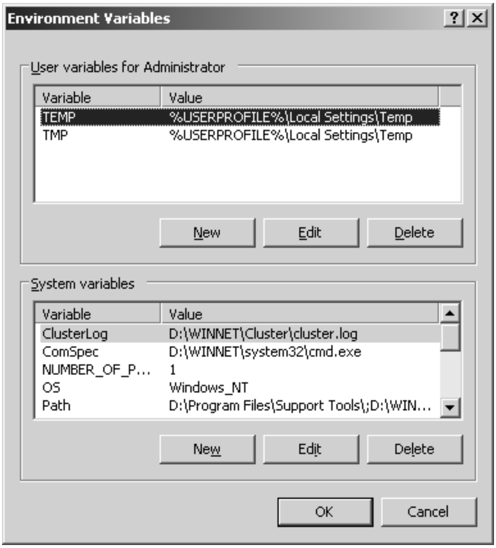
**Note** The paging file is also used for debugging purposes when a STOP error occurs on the system. If the paging file on the system drive is smaller than the minimum amount required to write the debugging information to the paging file, this feature will be disabled. If you want to use debugging, the minimum size should be set to the same figure as the amount of RAM on the system. For example, a system with 256 MB of RAM would need a paging file of 256 MB on the system drive.

6. On the system volume, the initial size must be as large as the current physical RAM. If it isn't, Windows won't be able to write STOP information to the system drive when fatal errors occur. Click Set to save the changes.
7. Repeat Steps 3 and 4 for each volume you want to configure.
8. Click OK, and, if prompted to overwrite an existing Pagefile.sys file, click Yes.
9. Close the System utility.

**Note** If you updated the settings for the paging file that is currently in use, you'll see a prompt explaining that you need to restart the server for the changes to take effect. Click OK. When you close the System utility, you'll see a prompt telling you that you need to restart the system for the changes to take effect. On a server, you should schedule this reboot outside normal business hours.

## Configuring System and User Environment Variables

You configure system and user environment variables by means of the Environment Variables dialog box, shown in Figure 2-8. To access this dialog box, start the System utility, click the Advanced tab, and then choose Environment Variables.



| Variable | Value |
|---|---|
| TEMP | %USERPROFILE%\Local Settings\Temp |
| TMP | %USERPROFILE%\Local Settings\Temp |

| Variable | Value |
|---|---|
| ClusterLog | D:\WINNET\Cluster\cluster.log |
| ComSpec | D:\WINNET\system32\cmd.exe |
| NUMBER_OF_P... | 1 |
| OS | Windows_NT |
| Path | D:\Program Files\Support Tools\;D:\WIN... |

**Figure 2-8.** *The Environment Variables dialog box lets you configure system and user environment variables.*

## Creating an Environment Variable

You can create environment variables by completing the following steps:

1. Click the New button under User Variables or System Variables, whichever is appropriate for the type of environment variable you want to create. This opens the New User Variable dialog box or the New System Variable dialog box, respectively.
2. In the Variable Name field, type the variable name. Then in the Variable Value field type the variable value.
3. Choose OK.

### Editing an Environment Variable

You can edit an existing environment variable by completing the following steps:

1. Select the variable in the User Variables or System Variables list box.
2. Click the Edit button under User Variables or System Variables, whichever is appropriate for the type of environment variable you're modifying. This opens the Edit User Variable dialog box or the Edit System Variable dialog box, respectively.
3. Type a new value in the Variable Value field.
4. Choose OK.

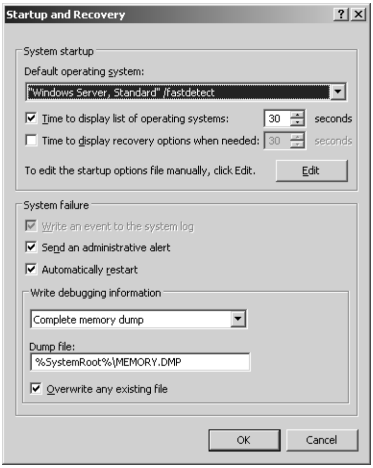
### Deleting an Environment Variable

You can delete an environment variable by selecting the variable and then clicking the Delete button.

**Note** When you create or modify system environment variables, the changes take effect when you restart the computer. When you create or modify user environment variables, the changes take effect the next time the user logs on to the system.

## Configuring System Startup and Recovery

You configure system startup and recovery properties by means of the Startup And Recovery dialog box, shown in Figure 2-9. To access this dialog box, start the System utility, click the Advanced tab, and then click Settings on the Startup And Recovery panel.



Startup and Recovery

System startup

Default operating system: "Windows Server, Standard" /fastdetect

☑ Time to display list of operating systems: 30 seconds

☐ Time to display recovery options when needed: 30 seconds

To edit the startup options file manually, click Edit.

System failure

☑ Write an event to the system log

☑ Send an administrative alert

☑ Automatically restart

Write debugging information: Complete memory dump

Dump file: %SystemRoot%\MEMORY.DMP

☑ Overwrite any existing file

**Figure 2-9.** *The Startup And Recovery dialog box lets you configure system startup and recovery procedures.*

## Setting Startup Options

The System Startup frame of the Startup And Recovery dialog box controls system startup. To set the default operating system, select one of the operating systems listed in the Default Operating System field. These options are obtained from the operating system section of the system's Boot.ini file.

At startup, Windows Server 2003 displays the startup configuration menu for 30 seconds by default. You can

- Boot immediately to the default operating system by clearing the Time To Display List Of Operating Systems check box.
- Display the available options for a specific amount of time by selecting the Time To Display List Of Operating Systems check box and then setting a time delay in seconds.

Generally, on most systems you'll want to use a value of 3–5 seconds. This is long enough to be able to make a selection, yet short enough to expedite the system startup process.

When the system is in a recovery mode and booting, a list of recovery options might be displayed. As with the standard startup options, you can configure recovery startup options in one of two ways. You can set the computer to boot immediately using the default recovery option by clearing the Time To Display Recovery Options When Needed check box, or you can display the available options for a specific amount of time by selecting Time To Display Recovery Options When Needed and then setting a time delay in seconds.

## Setting Recovery Options

The System Failure and Write Debugging Information areas of the Startup And Recovery dialog box control system recovery. Recovery options allow administrators to control precisely what happens when the system encounters a fatal system error (also known as a STOP error). The available options for the System Failure area are

- **Write An Event To The System Log** Logs the error in the system log, which allows administrators to review the error later using the Event Viewer
- **Send An Administrative Alert** Sends an alert to the recipients specified in the Alert dialog box
- **Automatically Restart** Check this option to have the system attempt to reboot when a fatal system error occurs

**Note** Configuring automatic restarts isn't always a good thing. Sometimes you might want the system to halt rather than reboot, which should ensure that the system gets proper attention. Otherwise, you can only know that the system rebooted when you view the system logs or if you happen to be in front of the system's monitor when it reboots.

The Write Debugging Information selection menu allows you to choose the type of debugging information that you want to write to a dump file. You can in turn use the dump file to diagnose system failures. The options are:

- **None** Use None if you don't want to write debugging information.
- **Small Memory Dump** Use this option to dump the physical memory segment in which the error occurred. This dump is 64 KB in size.
- **Kernel Memory Dump** Use this option to dump the physical memory area being used by the Windows kernel. The dump file size depends on the size of the Windows kernel.
- **Complete Memory Dump** Use this option to dump all physical memory being used at the time of the failure. The maximum dump file size is the same as the total physical memory size.

If you elect to write a dump file, you must also set a location for the dump file. The default dump locations are %SystemRoot%\Minidump for small memory dumps and %SystemRoot%\Memory.dmp for all other memory dumps. You'll usually want to select Overwrite Any Existing File as well. This option ensures that any existing dump files are overwritten if a new STOP error occurs.

**Note** You can create the dump file only if the system is properly configured. The system drive must have a sufficiently large memory-paging file (as set for virtual memory with the Advanced tab), and the drive where the dump file is written must have free space as well. For example, my server has 256 MB of RAM and requires a paging file on the system drive of the same size—256 MB. Since the same drive is used for the dump file, the drive must have at least 512 MB of free space to create a complete dump of debugging information correctly (that's 256 MB for the paging file and 256 MB for the dump file).

## Enabling and Disabling Error Reporting

Windows Server 2003 features built-in system and program error reporting. Error reporting sends information about errors to Microsoft or to a corporate file share that administrators can monitor. Error reporting is enabled by default for all Windows Server 2003 installations, and you can configure it to monitor these specific areas:

- **Windows Operating System** Reports critical operating system errors that cause a blue screen crash. The error report contains all the information that is displayed on the blue screen.
- **Unplanned Machine Shutdowns** Reports when the server is shut down and the shutdown reason is listed as unplanned. Selecting this option helps you keep track of unplanned reasons for server shutdowns, which is essential to maintaining good uptime and service records.
- **Programs** Reports illegal program operations and internal program errors that cause a program to stop working. With program errors, you can specify which programs should be monitored for errors and which shouldn't. If you

elect to report program errors, you can enable Force Queue Mode For Program Errors. In Queue mode, the last 10 errors are displayed the next time an administrator logs on and the administrator is able to choose which errors are reported. Without selecting this option, only the last error that occurs is reported, which might be misleading.

How an error is reported depends on where the error originated. When a component or program error occurs, a dialog box appears asking if you want to report the problem. If you choose to report the problem, the error report is sent over the Internet to Microsoft and a Thank You dialog box is displayed with additional information that might be helpful in resolving the problem. When an operating system error occurs, the system doesn't generate the error report until the next time you successfully boot and log on to the system.

You can enable and configure error reporting by completing the following steps:

1. Start the System utility. Click the Advanced tab and then click the Error Reporting button.
2. Select Enable Error Reporting and then select areas to monitor.

**Tip** By default, all program errors are reported, regardless of who the manufacturer is. If you chose to report program errors, you can change the default configuration. Choose Programs in the Error Reporting dialog box, and then select All Programs In This List. You can now select programs to add to the reporting list and you can disable reporting for Programs From Microsoft and Windows Components. You can also add programs to the Do Not Report Errors list.

3. Click OK.

You can disable error reporting by completing these steps:

1. Start the System utility. Click the Advanced tab, and then click the Error Reporting button.
2. Select Disable Error Reporting, and then click OK.

Another way to configure Error Reporting is to do so through Group Policy. Because Group Policy is discussed in detail in Chapter 4, "Automating Administrative Tasks, Policies, and Procedures," and in other chapters, I won't go into depth on how Group Policy works. I will tell you, however, which policies you'll want to look at to help better manage Error Reporting for the enterprise. These policies are located in Computer Configuration\Administrative Templates\System\Error Reporting and in Computer Configuration\Administrative Templates\System\Error Reporting\Advanced Error Reporting Settings.

**Tip** Error reporting can be distracting, but the information helps ensure that Microsoft resolves problems. To remove potential distraction, yet still help improve Windows for the future, you might want to disable Display Error Notification and enable Report Errors. When you do this, errors are automatically reported without notifying users that an error occurred.

The two most useful error reporting policies are:

- **Display Error Notification** Determines whether users are notified when errors occur. If not configured, users can specify error notification preferences using the System utility. If disabled, users aren't notified when an error occurs (but this doesn't prevent error reporting). If enabled, users are notified when an error occurs and given the opportunity to report the error.
- **Report Errors** Determines whether errors are reported and provides the opportunity to precisely control error reporting. If not configured, users can specify error reporting preferences using the System utility. If disabled, users won't be able to report errors but might still be notified when errors occur. If enabled, errors might be reported to Microsoft over the Internet or to a corporate file share that administrators can monitor. You can also specify whether More Information links are available, whether associated files and machine data is collected, and whether application errors are queued.

**Real World** Storing error reports on a file share can be helpful in resolving problems. Users might not tell you they're having problems. They might assume that a crashing program or other problems that they see are normal behavior. To be proactive in your support, you might want to store error reports on a corporate file share. If you want to do this, create a network share and then specify the share using the Universal Naming Convention (UNC) notation, such as \\Gamma\ErrorReports, where *Gamma* is the server name and *ErrorReports* is the network share.

**Tip** If you display errors and report them, you might want to customize the error reporting text with your company name. To do this, type your company name in the Replace Instances Of The Word "Microsoft" With field of the Report Errors Properties dialog box. Now your company name appears in text instead of Microsoft.

## The Automatic Updates Tab

The Automatic Update tab of the System utility controls the Automatic Updates configuration on the server. This feature is discussed in the section entitled "Understanding and Using Automatic Updates" in Chapter 5, "Working with Support Services and Remote Desktop."

### The Remote Tab

The Remote tab of the System utility controls Remote Assistance invitations and Remote Desktop connections. These options are discussed in Chapter 5 in the section entitled “Managing Remote Access to Servers.”

## Managing Hardware Devices and Drivers

Windows Server 2003 provides four key tools for managing hardware devices and drivers. These tools are

- Device Manager
- Add Hardware Wizard
- Hardware Update Wizard
- Hardware Troubleshooter

You’ll use these tools whenever you install, uninstall, or troubleshoot hardware devices and drivers. Before you work with device drivers, you should know the basics of signed and unsigned device drivers as well as the system settings that might prevent the use of unsigned drivers.

### Working with Signed and Unsigned Device Drivers

Microsoft recommends that you use signed device drivers whenever possible. Signed device drivers have a digital signature that authenticates them as having passed rigorous testing by the Windows Hardware Quality Labs. The digital signature also means the device driver hasn’t been tampered with.

Now, there are situations when you might have to use an unsigned device driver. For example, you might find that a device installed on a server doesn’t have a signed device driver. Your first response should be to check the manufacturer’s Web site to see if a signed driver is available. A signed driver might be available but not distributed with the device or on the Windows Server 2003 distribution disks. However, if one isn’t available, you might find that you have to use an unsigned driver. You have several options:

- Install an unsigned driver—a driver that worked with Windows 2000 might work in this instance. However, the system might become unstable. The system might crash, lose data, or even fail to restart.
- Stop using the device or use a different device with supported drivers. Cost might be a factor in your decision, but it shouldn’t be the only factor you consider. An unstable system costs time and money as well.

By default, Windows Server 2003 warns you if you try to install an unsigned device driver. If you don’t want to see this prompt, you can change the configuration so that this warning isn’t displayed. You can also specify that unsigned drivers should never be installed. One way to configure device driver settings is to use the System utility in the Control Panel.

1. Start the System utility. Click the Hardware tab and then click the Driver Signing button.
2. Choose the action you want Windows to take when someone tries to install an unsigned device driver. The options are:
    - **Ignore** Install the software anyway and don't ask for my approval.
    - **Warn** Prompt me each time to choose an action.
    - **Block** Never install unsigned driver software.
3. If the settings are only for the current user, clear Make This Action The System Default. Otherwise, select this check box to make this the default for all users.
4. Click OK twice.

If you want to assign device driver settings for the enterprise, you can do this through Group Policy. In this case Group Policy specifies the least secure setting that is allowed and, if Group Policy is set to Block, unsigned device drivers can't be installed without overriding Group Policy.

Code Signing For Device Drivers policy controls device driver signing settings. This policy is located in User Configuration\Administrative Templates\System. If enabled, you can specify the action to take: Ignore, Warn, or Block.

**Note** If you're trying to install a device and find that you can't install an unsigned driver, you should first check the System utility settings for driver signing. If you find that the settings are set to block and you can't change the setting, Code Signing For Device Drivers has been enabled and set to Block in Group Policy. You will need to override Group Policy in order to install the unsigned device driver.

## Viewing and Managing Hardware Devices

You can view a detailed list of all the hardware devices installed on a system by completing the following steps:

1. Choose Start, Programs or All Programs as appropriate, then Administrative Tools, and then Computer Management.
2. In the Computer Management console, click the plus sign (+) next to the System Tools node. This expands the node to display its tools.
3. Select Device Manager. You should now see a complete list of devices installed on the system. By default, this list is organized by device type.
4. Click the plus sign (+) next to a device type to see a list of the specific instances of that device type.
5. If you right-click the device entry, you can manage the device using the shortcut menu. Which options are available depends on the type of device, but they include
    - **Disable** Disables the device but doesn't uninstall it
    - **Enable** Enables a device if it's disabled

- **Properties** Displays the Properties dialog box for the device
- **Uninstall** Uninstalls the device and its drivers
- **Update Driver** Updates the driver file

**Tip** The device list shows warning symbols if there are problems with a device. A yellow warning symbol with an exclamation point indicates a problem with a device. A red X indicates a device that's improperly installed or has been disabled by the user or administrator for some reason.

You can use the options on the View menu in the Computer Management console to change the defaults for what types of devices are displayed and how the devices are listed. The options are

- **Devices By Type** Displays devices by the type of device installed, such as Disk Drive or Printer. The connection name is listed below the type. This is the default view.
- **Devices By Connection** Displays devices by connection type, such as System Board or Logical Disk Manager.
- **Resources By Type** Displays the status of allocated resources by type of device using the resource. Resource types are direct memory access (DMA) channels, input/output (I/O) ports, interrupt request (IRQ), and memory addresses.
- **Resources By Connection** Displays the status of all allocated resources by connection type rather than device type.
- **Show Hidden Devices** Displays non–Plug and Play devices as well as devices that have been physically removed from the computer but haven't had their drivers uninstalled.

## Configuring Device Drivers

Device drivers are required for devices, such as sound cards and display adapters, to work properly. Windows Server 2003 provides comprehensive management tools for maintaining and updating device drivers. These tools allow you to track driver information, install and update driver versions, roll back to a previously installed driver, and uninstall device drivers.

### Tracking Driver Information

Each driver being used on a system has a driver file associated with it. You can view the location of the driver file and related details by completing the following steps:

1. Start Computer Management. In the Computer Management console, click the plus sign (+) next to the System Tools node. This expands the node to display its tools.
2. Select Device Manager. You should now see a complete list of devices installed on the system. By default, this list is organized by device type.
3. Right-click the connection for the device you want to manage and then choose Properties from the shortcut menu. This opens the Properties dialog box for the device. Choose the Driver tab.

4. Display the Driver File Details dialog box by clicking Driver Details. The information displayed includes
   - **Driver Files** Displays a list of file locations where the driver exists within %SystemRoot%
   - **Provider** The creator of the driver
   - **File Version** The version of the file

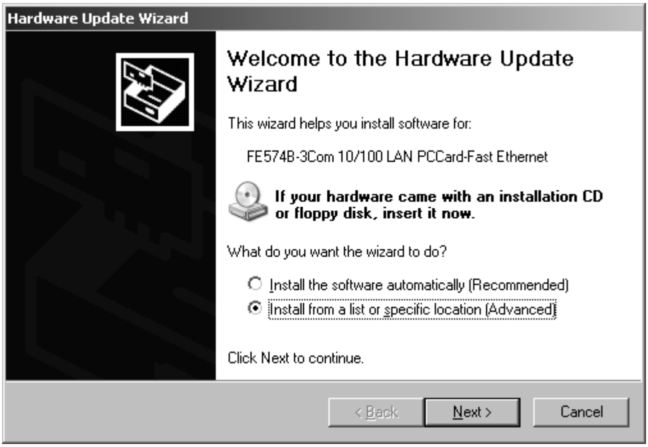
## Installing and Updating Drivers

To keep devices operating smoothly, it's essential that you keep the device drivers current. You can install and update device drivers by completing the following steps:

1. Start Computer Management. In the Computer Management console, click the plus sign (+) next to the System Tools node. This expands the node to display its tools.
2. Select Device Manager in the Computer Management console. You should now see a complete list of devices installed on the system. By default, this list is organized by device type.
3. Right-click the connection for the device you want to manage, and then choose Update Driver from the shortcut menu. This starts the Hardware Update Wizard.

**Best Practices** Updated drivers can add functionality to a device, improve performance, and resolve device problems. However, you should rarely install the latest drivers on a deployment server without first testing the drivers in a test environment. Test first, then install.

4. As shown in Figure 2-10, you can specify whether you want to install the drivers automatically or install manually by selecting the driver from a list or specific location.



Hardware Update Wizard

Welcome to the Hardware Update Wizard

This wizard helps you install software for:

FE574B-3Com 10/100 LAN PCCard-Fast Ethernet

**If your hardware came with an installation CD or floppy disk, insert it now.**

What do you want the wizard to do?

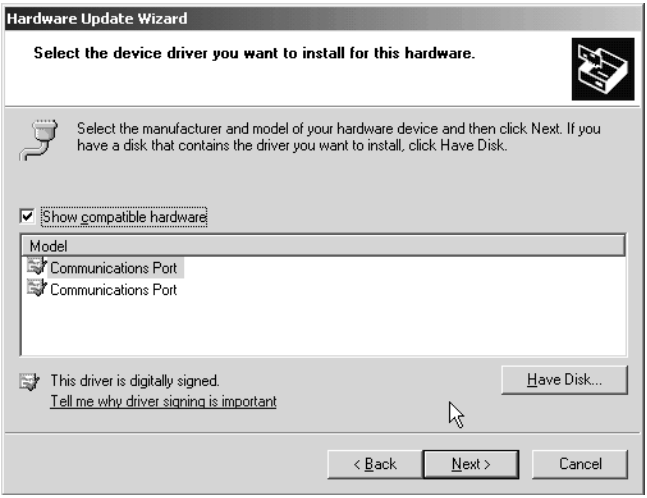
○ Install the software automatically (Recommended)

● Install from a list or specific location (Advanced)

Click Next to continue.

**Figure 2-10.** *Specify whether to search for the necessary drivers or select the drivers from a list of known drivers.*

5. If you elect to automatically install the driver, Windows looks for a more recent version of the device driver and installs the driver if found. If a more recent version of the driver isn't found, Windows keeps the current driver. In either case, click Finish to complete the process and then skip the remaining steps.
6. If you choose to install the driver manually, you'll have the opportunity to
    - **Search For The Best Driver In These Locations** If you search for drivers, the wizard checks the driver database on the system for drivers and any of the optional locations you specify, such as a floppy disk or CD-ROM. Any matching drivers found are displayed, and you can select a driver.
    - **Don't Search. I Will Choose The Driver To Install** If you decide to install drivers yourself, the next wizard window shows a list of compatible hardware and a recommended list of drivers for this hardware, as seen in Figure 2-11. If a correct driver is listed, all you need to do is to select it. If a correct driver isn't listed, clear the Show Compatible Hardware check box. You can now view a list of manufacturers to find the manufacturer of the device. Once you find the manufacturer, select the appropriate device driver in the Models pane.



**Hardware Update Wizard**

**Select the device driver you want to install for this hardware.**

Select the manufacturer and model of your hardware device and then click Next. If you have a disk that contains the driver you want to install, click Have Disk.

☑ Show compatible hardware

| Model |
|---|
| Communications Port |
| Communications Port |

This driver is digitally signed.
Tell me why driver signing is important

**Figure 2-11.** *Select the device driver by manufacturer and type.*

## Rolling Back Drivers

Sometimes you'll find that a device driver that you've installed causes device failure or other critical problems on a system. Don't worry, you can recover the system to the previously installed device driver. To do this, follow these steps:

1. Start Computer Management. In the Computer Management console, click the plus sign (+) next to the System Tools node. This expands the node to display its tools.
2. Select Device Manager in the Computer Management console. You should now see a complete list of devices installed on the system. By default, this list is organized by device type.
3. Right-click the connection for the device you want to manage and then choose Properties from the shortcut menu. This opens the Properties dialog box for the device.
4. Choose the Driver tab and then click Roll Back Driver. When prompted to confirm the action, click Yes.
5. Click OK.

**Note** If the driver file hasn't been updated, a backup driver file won't be available. Instead of being able to roll back the driver, you'll see a prompt telling you that no driver files have been backed up for this device. If you're having problems with the device, click Yes to start the Troubleshooter. Otherwise, click No to quit the operation.

## Removing Device Drivers for Removed Devices

Usually when you remove a device from a system, Windows Server 2003 detects this fact and removes the drivers for that device automatically. Sometimes, however, when you remove a device, Windows Server 2003 doesn't detect the change and you must remove the drivers manually. You can remove device drivers manually by completing the following steps:

1. Start Computer Management. In the Computer Management console, click the plus sign (+) next to the System Tools node. This expands the node to display its tools.
2. Select Device Manager in the Computer Management console.
3. Right-click the connection for the device you want to remove and then select Uninstall from the shortcut menu.
4. When prompted to confirm the action, click OK.

## Uninstalling Device Drivers

Uninstalling a device driver uninstalls the related device. Sometimes when a device isn't working properly you can completely uninstall the device, restart the system, and then reinstall the device driver to restore normal operations. You can uninstall and then reinstall a device by completing the following steps:

1. Start Computer Management. In the Computer Management console, click the plus sign (+) next to the System Tools node. This expands the node to display its tools.
2. Select Device Manager in the Computer Management console. You should now see a complete list of devices installed on the system. By default, this list is organized by device type.
3. Right-click the connection for the device you want to manage and then choose Uninstall from the shortcut menu.
4. When prompted to confirm the action, click OK.
5. Reboot the system. Windows should detect the presence of the device and then automatically reinstall the necessary device driver. If the device isn't automatically reinstalled, reinstall it manually as discussed in the section of this chapter entitled "Adding New Hardware."

**Note** To prevent a device from being reinstalled automatically, disable the device instead of uninstalling it. You disable a device by right-clicking it in Device Manager and then selecting Disable.

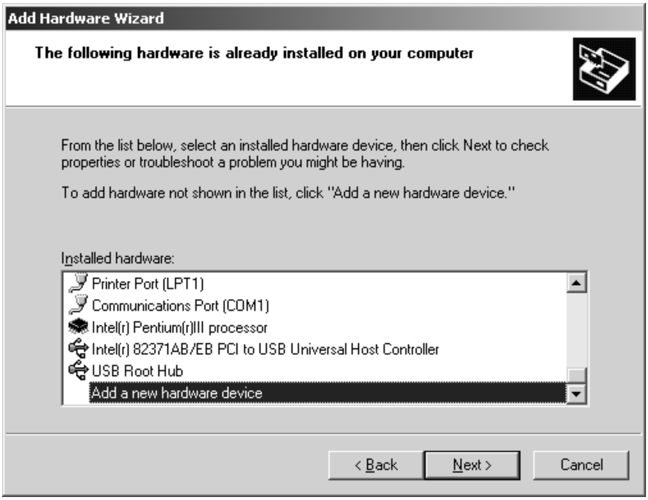
## Managing Hardware

Windows Plug and Play technology does a good job of detecting and automatically configuring new hardware. However, if the hardware doesn't support Plug and Play or isn't automatically detected, you'll need to enter information about the new hardware into the Windows Server 2003 system. You do this by installing the hardware device and its related drivers on the system using the Add New Hardware Wizard. You can also use this wizard to troubleshoot problems with existing hardware.

### Adding New Hardware

You can install new hardware using the Add Hardware Wizard by completing the following steps:

1. Access the Control Panel and then double-click Add Hardware. This starts the Add Hardware Wizard. Click Next.
2. At this point, you have two options:
   - If you've already connected the new hardware, select Yes, I Have Already Connected the Hardware and click Next to continue. The Add Hardware Wizard screen shown in Figure 2-12 should be displayed. Go on to Step 3.
   - If you haven't connected the hardware, click No, I Have Not Added the Hardware Yet and then click Next. The only option you have now is to click Finish. You'll need to connect the hardware (which might require shutting down the computer) and then restart the Add Hardware Wizard. Skip the remaining steps.



Add Hardware Wizard

The following hardware is already installed on your computer

From the list below, select an installed hardware device, then click Next to check properties or troubleshoot a problem you might be having.

To add hardware not shown in the list, click "Add a new hardware device."

Installed hardware:

- Printer Port (LPT1)
- Communications Port (COM1)
- Intel(r) Pentium(r)III processor
- Intel(r) 82371AB/EB PCI to USB Universal Host Controller
- USB Root Hub
- Add a new hardware device

**Figure 2-12.** *Use the Add Hardware Wizard to install, uninstall, or troubleshoot hardware devices.*

3. To add new hardware, select Add A New Hardware Device from the Installed Hardware list box and then click Next. This option is located at the very bottom of the Installed Hardware list. In the Find New Hardware dialog box determine whether the wizard should search for new hardware or whether you want to select the hardware from a list.
   - If you choose the search option, the wizard searches for and automatically detects new hardware. The process takes a few minutes to go through all the device types and options. When the search is completed, any new devices found are displayed, and you can select a device.
   - If you choose the manual option, or if no new devices are found in the automatic search, you'll have to select the hardware type yourself. Select the type of hardware, such as Modem or Network Adapter, and then click Next. Scroll through the list of manufacturers to find the device's manufacturer, and then choose the appropriate device in the Models pane.
4. Once you complete the selection and installation process, click Next and then click Finish. The new hardware should now be available.

## Enabling and Disabling Hardware

When a device isn't working properly, sometimes you'll want to uninstall or disable it. Uninstalling a device removes the driver association for the device so that it temporarily appears that the device has been removed from the system. The next time you restart the system, Windows Server 2003 might try to reinstall the device. Typically, Windows Server 2003 reinstalls Plug and Play devices automatically, but not non–Plug and Play devices.

Disabling a device turns it off and prevents Windows Server 2003 from using it. Because a disabled device doesn't use system resources, you can be sure that it isn't causing a conflict on the system. You can uninstall or disable a device by completing the following steps:

1. Start Computer Management. In the Computer Management console, click the plus sign (+) next to the System Tools node. This expands the node to display its tools.
2. Select Device Manager in the Computer Management console. You should now see a complete list of devices installed on the system. By default, this list is organized by device type.
3. Right-click the connection for the device you want to manage and then select one of the following options:
    - **Enable** To enable the device
    - **Uninstall** To uninstall the device
    - **Disable** To disable the device
4. If prompted to confirm the action, click Yes or OK as appropriate.

## Troubleshooting Hardware

You can use the Add Hardware Wizard to troubleshoot hardware problems as well. The basic steps are as follows:

1. Access the Control Panel and then double-click Add Hardware. This starts the Add Hardware Wizard. Click Next.
2. At this point, you have two options:
    - If you've already connected the hardware that you want to examine, select Yes, I Have Already Connected the Hardware and click Next to display the Installed Hardware list box. Go on to Step 3.
    - If you haven't connected the hardware, click No, I Have Not Added the Hardware Yet and then click Next. The only option you have now is to click Finish. You'll need to connect the hardware (which might require shutting down the computer) and then restart the Add Hardware Wizard. Skip the remaining steps.

3. From the Devices list, select the hardware device that you want to troubleshoot, and then click Next. The final wizard dialog box provides a device status. When you click Finish, the wizard does one of two things:
    - If an error code is shown with the device status, the wizard accesses the error code in the online help documentation—if it's available and installed. The help documentation should include a proposed technique to resolve the issue.
    - The wizard starts the Hardware Troubleshooter, which attempts to solve the hardware problem using your responses to the questions it asks. Follow the advice of the Hardware Troubleshooter to resolve the hardware problem.

You can also access the Hardware Troubleshooter directly. To do that, complete the following steps:

1. In the Computer Management console, access Device Manager.
2. Right-click the connection for the device you want to troubleshoot and then select Properties on the shortcut menu.
3. In the General tab, click Troubleshoot.

# Managing Dynamic-Link Libraries

As an administrator, you might be asked to install or uninstall dynamic-link libraries (DLLs), particularly if you work with IT (information technology) development teams. The utility you use to work with DLLs is Regsvr32. This utility is run at the command line.

Once you start a command window, you install or register a DLL by typing **regsvr32** ***name*****.dll**, such as:

```
regsvr32 mylibs.dll
```

If necessary, you can uninstall or unregister a DLL by typing **regsvr32 /u** ***name*****.dll**, such as:

```
regsvr32 /u mylibs.dll
```

**Note** Windows File Protection prevents replacement of protected system files. You'll be able to replace only DLLs installed by the Windows Server 2003 operating system as part of a hot fix, service pack update, Windows update, or Windows upgrade. Windows File Protection is an important part of the Windows Server 2003 security architecture.

## Chapter 3

# Monitoring Processes, Services, and Events

As an administrator, it's your job to keep an eye on the network systems. The status of system resources and usage can change dramatically over time. Services might stop running. File systems might run out of space. Applications might throw exceptions, which in turn can cause system problems. Unauthorized users might try to break into the system. The techniques discussed in this chapter will help you find and resolve these and other system problems.

## Managing Applications, Processes, and Performance

Any time you start an application or type a command on the command line, Microsoft Windows Server 2003 starts one or more processes to handle the related program. Generally, processes that you start in this manner are called *interactive processes*. That is, you start the processes *interactively* with the keyboard or mouse. If the application or program is active and selected, the related interactive process has control over the keyboard and mouse until you switch control by terminating the program or selecting a different one. When a process has control, it's said to be running *in the foreground*.

Processes can also run *in the background*. With processes started by users, this means that programs that aren't currently active can continue to operate—only they generally aren't given the same priority as the active process. You can also configure background processes to run independently of the user logon session; the operating system usually starts such processes. An example of this type of background process is a batch file started with an AT command. The AT command tells the system to run the file at a specified time, and (if permissions are configured correctly) the AT command can do so regardless of whether a user is logged on to the system.

### Task Manager

The key tool you'll use to manage system processes and applications is Task Manager. You can access Task Manager using any of the following techniques:

- Press Ctrl+Shift+Esc
- Press Ctrl+Alt+Del and then click the Task Manager button

- Type **taskmgr** into the Run utility or a command prompt
- Right-click the taskbar and select Task Manager from the shortcut menu

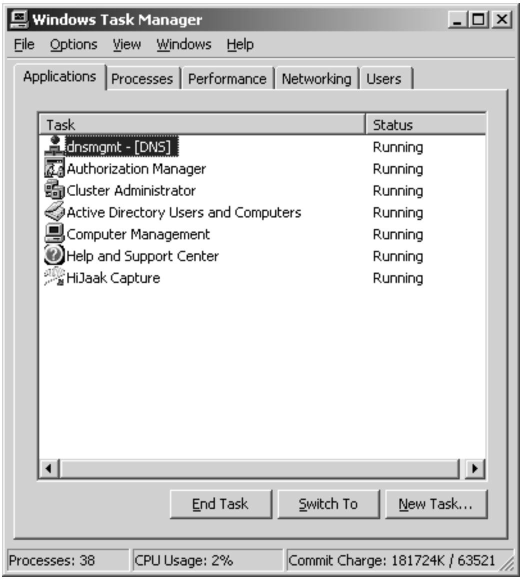
Techniques you'll use to work with Task Manager are covered in the following sections.

## Administering Applications

Task Manager's Applications tab is shown in Figure 3-1. This tab shows the status of the programs that are currently running on the system. You can use the buttons on the bottom of this tab as follows:

- Stop an application by selecting the application and then clicking End Task.
- Switch to an application and make it active by selecting the application and then clicking Switch To.
- Start a new program by selecting New Task, and then enter a command to run the application. New Task functions like the Start menu's Run utility.

**Tip** The Status column tells you if the application is running normally or if the application has gone off into the ozone. A status of Not Responding is an indicator that an application might be frozen, and you might want to end its related task. However, some applications might not respond to the operating system during certain process-intensive tasks. Because of this, you should be certain the application is really frozen before you end its related task.



| Task | Status |
|---|---|
| dnsmgmt - [DNS] | Running |
| Authorization Manager | Running |
| Cluster Administrator | Running |
| Active Directory Users and Computers | Running |
| Computer Management | Running |
| Help and Support Center | Running |
| HiJaak Capture | Running |

Processes: 38 | CPU Usage: 2% | Commit Charge: 181724K / 63521

**Figure 3-1.** *The Applications tab of the Windows Task Manager shows the status of programs currently running on the system.*

### Right-Clicking a Listing

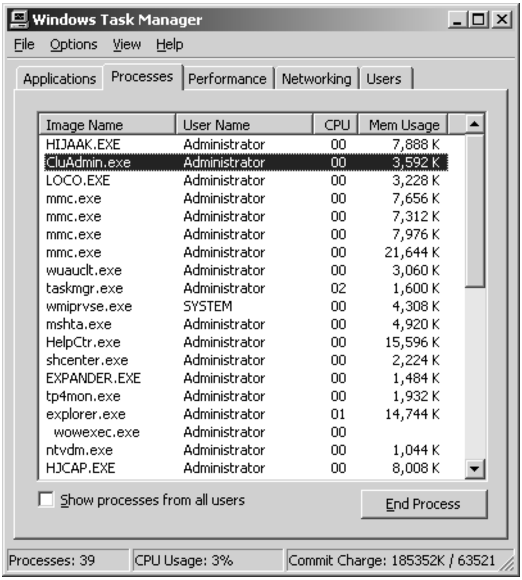
Right-clicking an application's listing in the Windows Task Manager displays a shortcut menu that allows you to

- Switch to the application and make it active
- Bring the application to the front of the display
- Minimize and maximize the application
- Tile or cascade the application
- End the application
- Go to the related process in the Processes tab

**Note** The Go To Process is very helpful when you're trying to find the primary process for a particular application. Selecting this option highlights the related process in the Processes tab.

## Administering Processes

The Task Manager Processes tab is shown in Figure 3-2. This tab provides detailed information about the processes that are running. By default, the Processes tab shows only processes run by the operating system, local services, network services, and the interactive user. The interactive user is the user account logged on to the local console. To see processes run by remote users, such as those connecting using a remote desktop connection, you'll need to select Show Processes From All Users.



| Image Name | User Name | CPU | Mem Usage |
|---|---|---|---|
| HIJAAK.EXE | Administrator | 00 | 7,888 K |
| CluAdmin.exe | Administrator | 00 | 3,592 K |
| LOCO.EXE | Administrator | 00 | 3,228 K |
| mmc.exe | Administrator | 00 | 7,656 K |
| mmc.exe | Administrator | 00 | 7,312 K |
| mmc.exe | Administrator | 00 | 7,976 K |
| mmc.exe | Administrator | 00 | 21,644 K |
| wuauclt.exe | Administrator | 00 | 3,060 K |
| taskmgr.exe | Administrator | 02 | 1,600 K |
| wmiprvse.exe | SYSTEM | 00 | 4,308 K |
| mshta.exe | Administrator | 00 | 4,920 K |
| HelpCtr.exe | Administrator | 00 | 15,596 K |
| shcenter.exe | Administrator | 00 | 2,224 K |
| EXPANDER.EXE | Administrator | 00 | 1,484 K |
| tp4mon.exe | Administrator | 00 | 1,932 K |
| explorer.exe | Administrator | 01 | 14,744 K |
| wowexec.exe | Administrator | 00 | |
| ntvdm.exe | Administrator | 00 | 1,044 K |
| HJCAP.EXE | Administrator | 00 | 8,008 K |

Processes: 39 | CPU Usage: 3% | Commit Charge: 185352K / 63521

**Figure 3-2.** *The Processes tab provides detailed information on running processes.*

The fields of the Processes tab provide lots of information about running processes. You can use this information to determine which processes are hogging system resources, such as CPU time and memory. The fields displayed by default are:

- **Image Name** The name of the process or executable running the process
- **User Name** The name of the user or system service running the process
- **CPU** The percentage of CPU utilization for the process
- **Mem Usage** The amount of memory the process is currently using

If you click View and choose Select Columns, you'll see a dialog box that will let you add columns to the Processes view. When you're trying to troubleshoot system problems using process information, you might want to add these columns to the view:

- **Base Priority** Priority determines how much of the system resources are allocated to a process. To set the priority of a process, right-click the process, choose Set Priority, and then select the new priority. Priorities are Low, Below Normal, Normal, Above Normal, High, and Real-Time. Most processes have a normal priority by default. The highest priority is given to real-time processes.
- **CPU Time** The total amount of CPU cycle time used by the process since it was started. To quickly see the processes that are using the most CPU time, display this column and then click the column header to sort process entries by CPU Time.
- **Handle Count** The total number of file handles maintained by the process. Use the handle count to gauge how dependent the process is on the file system. Some processes, such as those used by Microsoft Internet Information Services (IIS), have thousands of open file handles. Each file handle requires system memory to maintain.
- **I/O Reads, I/O Writes** The total number of disk input/output (I/O) reads or writes since the process was started. Together, the number of I/O reads and writes tell you how much disk I/O activity there is. If the number of I/O reads and writes is growing disproportional to actual activity on the server, the process might not be caching files or file caching might not be properly configured. Ideally, file caching will reduce the need for I/O read and writes.
- **Page Faults** A page fault occurs when a process requests a page in memory and the system can't find it at the requested location. If the requested page is elsewhere in memory, the fault is called a *soft page fault*. If the requested page must be retrieved from disk, the fault is called a *hard page fault*. Most processors can handle large numbers of soft faults. Hard faults, however, can cause significant delays.
- **Paged Pool, Non-paged Pool** The *paged pool* is an area of system memory for objects that can be written to disk when they aren't used. The *non-paged pool* is an area of system memory for objects that can't be written to disk. You

should note processes that require a high amount of nonpaged pool memory. If there isn't enough free memory on the server, these processes might be the reason for a high level of page faults.

- **Peak Memory Usage** The highest amount of memory used by the process. The change or delta between current memory usage and peak memory usage is important to note as well. Applications, such as Microsoft SQL Server, that have a high delta between base memory usage and peak memory usage might need to be allocated more memory on startup so that they perform better.
- **Thread Count** The current number of threads that the process is using. Most server applications are multithreaded. Multithreading allows concurrent execution of process requests. Some applications can dynamically control the number of concurrently executing threads to improve application performance. Too many threads, however, can actually reduce performance, as the operating system has to switch thread contexts too frequently.

If you examine processes running in Task Manager, you'll note a process called System Idle Process. You can't set the priority of this process. Unlike other processes that track resource usage, System Idle Process tracks the amount of system resources that aren't used. Thus, a 99 in the CPU column for the System Idle Process means 99 percent of the system resources currently aren't being used.

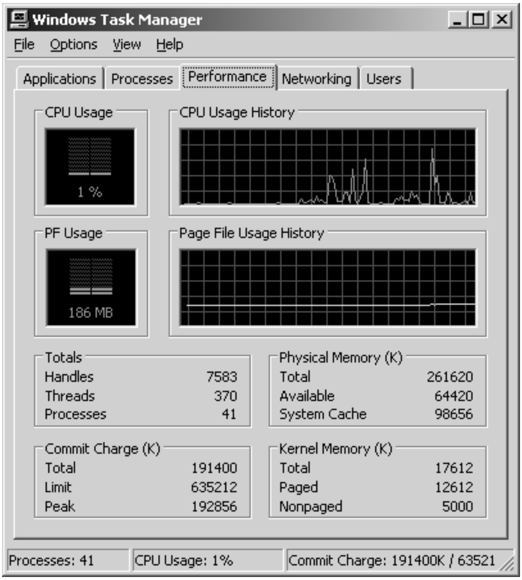
As you examine processes, keep in mind that a single application might start multiple processes. Generally, these processes are dependent on a central process, and from this main process a process tree containing dependent processes is formed. You can find the main process for an application by right-clicking the application in the Applications tab and selecting Go To Process. When you terminate processes, you'll usually want to target the main application process or the application itself rather than dependent processes. This ensures that the application is stopped cleanly.

To stop the main application process and dependent processes, you have several choices. You can:

- Select the application on the Applications tab, and then click End Task
- Right-click the main application process on the Processes tab, and then select End Process
- Select the main or a dependent process on the Processes tab, and then select End Process Tree

## Viewing and Managing System Performance

The Task Manager Performance tab provides an overview of CPU and memory usage. As shown in Figure 3-3, the tab displays graphs as well as statistics. This information gives you a quick check on system resource usage. For more detailed information, use Performance Monitor, as explained later in this chapter.



CPU Usage: 1 %

PF Usage: 186 MB

Totals
Handles 7583
Threads 370
Processes 41

Physical Memory (K)
Total 261620
Available 64420
System Cache 98656

Commit Charge (K)
Total 191400
Limit 635212
Peak 192856

Kernel Memory (K)
Total 17612
Paged 12612
Nonpaged 5000

Processes: 41
CPU Usage: 1%
Commit Charge: 191400K / 63521

**Figure 3-3.** *The Performance tab provides a quick check on system resource usage.*

## Graphs on the Performance Tab

The graphs on the Performance tab provide the following information:

- **CPU Usage** The percentage of processor resources being used currently.
- **CPU Usage History** A history graph of CPU usage plotted over time. The update speed determines how often the graph is updated.
- **PF Usage** The amount of the paging file (or virtual memory) being used by the system currently.
- **Page File Usage History** A history graph of paging file usage plotted over time.

**Tip** To view a close-up of the CPU graphs, double-click within the Performance tab. Double-clicking again returns you to normal viewing mode. If CPU usage is consistently high, even under average usage conditions, you might want to perform more detailed performance monitoring to determine the cause of the problem. Memory is often a source of performance problems, and you should rule it out before upgrading or adding CPUs. For more details, see the section of this chapter entitled “Tuning System Performance.”

## Customizing and Updating the Graph Display

To customize or update the graph display, use the following options on the View menu:

- **Update Speed** Allows you to change the speed of graph updating as well as to pause the graph. Updates occur once every four seconds for Low, once every two seconds for Normal, and twice per second for High.
- **CPU History** On multiprocessor systems, allows you to specify how CPU graphs are displayed. You can, for example, display one CPU in each graph or multiple CPUs in each graph.
- **Show Kernel Times** Allows you to display the amount of CPU time used by the operating system kernel. Usage by the kernel is shown in red plotting (as opposed to green plotting, which is used otherwise).

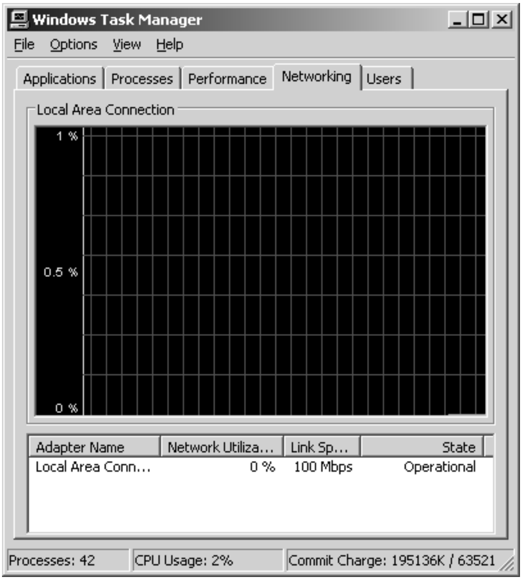
Beneath the graphs you'll find several lists of statistics. These statistics provide the following information:

- **Commit Charge** Provides information on the total memory used by the operating system. *Total* lists all physical and virtual memory currently in use. *Limit* lists the total physical and virtual memory available. *Peak* lists the maximum memory used by the system since bootup. If the difference between the total memory used and the peak memory used is consistently large, you might want to add physical memory to the system to improve performance. If the peak memory usage is within 10 percent of the Limit value, you might want to add physical memory and/or increase the amount of virtual memory.
- **Kernel Memory** Provides information on the memory used by the operating system kernel. Critical portions of kernel memory must operate in RAM and can't be paged to virtual memory. This type of kernel memory is listed as *Nonpaged*. The rest of kernel memory can be paged to virtual memory and is listed as *Paged*. The total amount of memory used by the kernel is listed under *Total*.
- **Physical Memory** Provides information on the total RAM on the system. *Total* shows the amount of physical RAM. *Available* shows the RAM not currently being used and available for use. *System Cache* shows the amount of memory used for system caching. If the server has very little physical memory available you might need to add memory to the system. In general, you want the available memory to be no less than 5 percent of the total physical memory on the server.
- **Totals** Provides information on CPU usage. *Handles* shows the number of I/O handles in use. *Threads* shows the number of threads in use. *Processes* shows the number of processes in use. I/O throughput and disk performance have more of an impact on a system than a consistently high number of I/O handles has.

## Viewing and Managing Networking Performance

The Task Manager Networking tab provides an overview of the network adapters being used by a system. You can use the information provided to quickly determine the percent utilization, link speed, and operational status usage of each network adapter configured on a system.

If a system has one network adapter, the summary graph shown in Figure 3-4 details the network traffic on this adapter over time. If a system has multiple network adapters, the graph displays a composite index of all network connections, which represents all network traffic. By default, the graph displays only the network traffic total byte count. You can change this by clicking View, choosing Network History, and then enabling Bytes Sent, Bytes Received, or both. Bytes Sent are shown in red, Bytes Received in yellow, Bytes Total in green.



| Adapter Name | Network Utiliza... | Link Sp... | State |
|---|---|---|---|
| Local Area Conn... | 0 % | 100 Mbps | Operational |

Processes: 42 | CPU Usage: 2% | Commit Charge: 195136K / 63521

**Figure 3-4.** *Networking performance allows you to easily track network activity on the server.*

The fields of the Networking tab provide lots of information about network traffic to and from the server. You can use this information to determine how much external traffic a server is experiencing at any time. The fields displayed by default are:

- **Adapter Name** Name of the network adapter in the Network Connections folder.
- **Network Utilization** Percentage of network usage based on the initial connection speed for the interface. For example, an adapter with an initial link speed of 100 megabits per second (Mbps) and current traffic of 10 Mbps would have a 10 percent utilization.

- **Link Speed** Connection speed of the interface as determined by the initial connection speed.
- **State** Operational status of network adapters.

**Real World** Any time you see usage consistently approaching or over 50 percent of total capacity, you'll want to start monitoring the server more closely and might also want to consider adding additional network adapters. Plan any upgrade carefully; there's a lot more planning required than you might think. Consider not only the implications for that server, but also for the network as a whole. You might also have connectivity issues if you exceed the allotted bandwidth of your service provider—and it can often take several months to obtain additional bandwidth for external connections.

If you click View and choose Select Columns, you'll see a dialog box that will let you add columns to the Processes view. When you're trying to troubleshoot networking problems, you might want to add these columns to the view:

- **Bytes Sent Throughput** Percentage of current connection bandwidth used by traffic sent from the system
- **Bytes Received Throughput** Percentage of current connection bandwidth used by traffic received by the system
- **Bytes Throughput** Percentage of current connection bandwidth used for all traffic on the network adapter
- **Bytes Sent** Cumulative total bytes sent on the connection to date
- **Bytes Received** Cumulative total bytes received on the connection to date
- **Bytes Total** Cumulative total bytes on the connection to date

## Viewing and Managing Remote User Sessions

Remote users can connect to systems using Terminal Services or Remote Desktop. Terminal Services allow remote terminal connections to systems. Remote Desktop allows you to remotely administer systems as if you were sitting at the keyboard.

Remote Desktop connections are automatically enabled on Windows Server 2003 installations. One way to view and manage remote desktop connections is to use Task Manager. To do this, start Task Manager, and then select the Users tab. The Users tab shows interactive user sessions for both local and remote users.

Each user connection is listed with the user account name, session ID, status, originating client computer, and session type. A user logged on to the local system is listed with Console as the session type. Other users have a session type that indicates the connection type and protocol, such as RDP-TCP for a connection using the Remote Desktop Protocol with TCP as the transport protocol. If you right-click user sessions, you have the following options:

- **Connect** Connects the user session if it's inactive.
- **Disconnect** Disconnects the user session, halting all user-started applications without saving application data.

- **Log Off** Logs the user off, using the normal logoff process. Application data and system state information are saved as during a normal log off.
- **Remote Control** Sets the hot keys used to end remote control sessions. The default hot keys are Ctrl+*.
- **Send Message** Sends a console message to users logged on to remote systems.

# Managing System Services

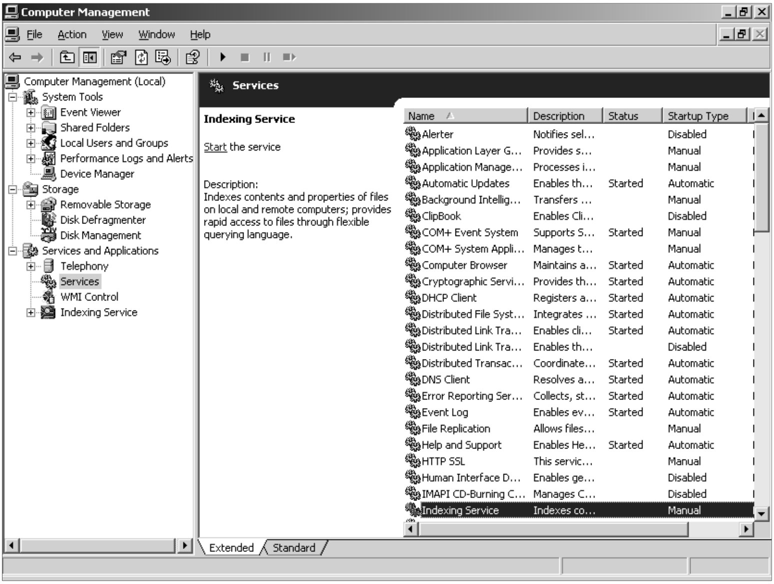
Services provide key functions to workstations and servers. To manage system services, you'll use the Services entry in the Computer Management console. You can start Computer Management and access the Services entry by completing the following steps:

1. Choose Start, then choose Programs or All Programs as appropriate, then Administrative Tools, and finally Computer Management. Or select Computer Management in the Administrative Tools folder.
2. Right-click the Computer Management entry in the console tree and select Connect To Another Computer on the shortcut menu. You can now choose the system whose services you want to manage.
3. Expand the Services And Applications node by clicking the plus sign (+) next to it, and then choose Services.

**Note** Windows Server 2003 provides several other ways to access services. For example, you can also use the Services entry in the Component Services utility.

Figure 3-5 shows the Services view in the Computer Management console. The key fields of this dialog box are used as follows:

- **Name** The name of the service. Only services installed on the system are listed here. Double-click an entry to configure its startup options. If a service you need isn't listed, you can install it by using the Network Connection Properties dialog box or the Windows Optional Networking Components Wizard. See Chapter 16, "Managing TCP/IP Networking," for details.
- **Description** A short description of the service and its purpose.
- **Status** Whether the status of the service is started, paused, or stopped. (Stopped is indicated by a blank entry.)
- **Startup Type** The startup setting for the service. Automatic services are started at bootup. Users or other services start manual services. Disabled services are turned off and can't be started while they remain disabled.
- **Log On As** The account the service logs on as. The default in most cases is the local system account.



**Indexing Service**

Start the service

Description:
Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.

| Name | Description | Status | Startup Type |
|---|---|---|---|
| Alerter | Notifies sel... | | Disabled |
| Application Layer G... | Provides s... | | Manual |
| Application Manage... | Processes i... | | Manual |
| Automatic Updates | Enables th... | Started | Automatic |
| Background Intellig... | Transfers ... | | Manual |
| ClipBook | Enables Cli... | | Disabled |
| COM+ Event System | Supports S... | Started | Manual |
| COM+ System Appli... | Manages t... | | Manual |
| Computer Browser | Maintains a... | Started | Automatic |
| Cryptographic Servi... | Provides th... | Started | Automatic |
| DHCP Client | Registers a... | Started | Automatic |
| Distributed File Syst... | Integrates ... | Started | Automatic |
| Distributed Link Tra... | Enables cli... | Started | Automatic |
| Distributed Link Tra... | Enables th... | | Disabled |
| Distributed Transac... | Coordinate... | Started | Automatic |
| DNS Client | Resolves a... | Started | Automatic |
| Error Reporting Ser... | Collects, st... | Started | Automatic |
| Event Log | Enables ev... | Started | Automatic |
| File Replication | Allows files... | | Manual |
| Help and Support | Enables He... | Started | Automatic |
| HTTP SSL | This servic... | | Manual |
| Human Interface D... | Enables ge... | | Disabled |
| IMAPI CD-Burning C... | Manages C... | | Disabled |
| Indexing Service | Indexes co... | | Manual |

**Figure 3-5.** *Use the Services view to manage services on workstations and servers.*

Services has two views: extended and standard. To change the view, click the tabs at the bottom of the Services area. In extended view, quick links are provided for managing services. Click Start to start a stopped service. Click Restart to stop and then start a service—essentially resetting that service. If you select a service in extended view, a service description is shown, which details the service's purpose.

**Note** Both the operating system and a user can disable Services. Generally, Windows Server 2003 disables services if there's a possible conflict with another service.

## Starting, Stopping, and Pausing Services

As an administrator, you'll often have to start, stop, or pause Windows Server 2003 services. To start, stop, or pause a service, complete the following steps:

1. Start the Computer Management console.
2. Right-click the Computer Management entry in the console tree and select Connect To Another Computer on the shortcut menu. You can now choose the system whose services you want to manage.
3. Expand the Services And Applications node by clicking the plus sign (+) next to it, and then choose Services.

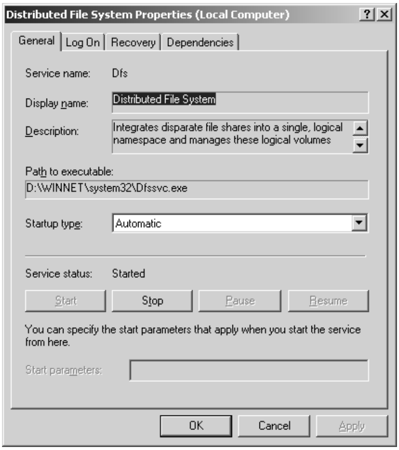
4. Right-click the service you want to manipulate, and then select Start, Stop, or Pause as appropriate. You can also choose Restart to have Windows stop and then start the service after a brief pause. Additionally, if you pause a service, you can use the Resume option to resume normal operation.

**Note** When services that are set to start automatically fail, the status is listed as blank and you'll usually receive notification in a pop-up dialog box. Service failures can also be logged to the system's event logs. In Windows Server 2003, you can configure actions to handle service failure automatically. For example, you could have Windows Server 2003 attempt to restart the service for you. For details, see the section of this chapter entitled "Configuring Service Recovery."

## Configuring Service Startup

You can set Windows Server 2003 services to start manually or automatically. You can also turn them off permanently by disabling them. You configure service startup by completing the following steps:

1. In the Computer Management console, connect to the computer whose services you want to manage.
2. Expand the Services And Applications node by clicking the plus sign (+) next to it, and then choose Services.
3. Right-click the service you want to configure, and then choose Properties.
4. In the General tab, use the Startup Type drop-down list box to choose a startup option, as shown in Figure 3-6. Select Automatic to start services at bootup. Select Manual to allow the services to be started manually. Select Disabled to turn off the service.
5. Click OK.



Service name: Dfs

Display name: Distributed File System

Description: Integrates disparate file shares into a single, logical namespace and manages these logical volumes

Path to executable: D:\WINNET\system32\Dfssvc.exe

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

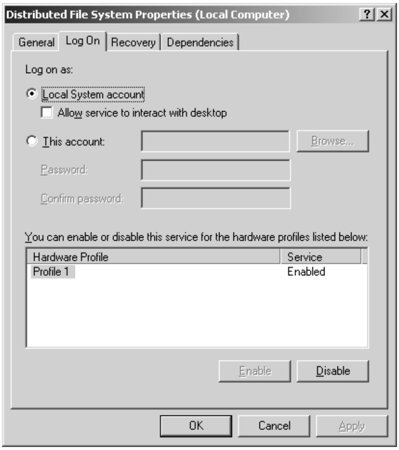
**Figure 3-6.** *Use the General tab's Startup Type drop-down list box to configure service startup options.*

**Real World** When a server has multiple hardware profiles, you can enable or disable services for a particular profile. Before you disable services permanently, you might want to create a separate hardware profile for testing the server with these services disabled. In this way you can use the original profile to quickly resume operations using the original service status. The profile doesn't save other service configuration options, however. To enable or disable a service by profile, use the Logon tab of the Service Properties dialog box. Select the profile that you want to work with under Hardware Profile, and then click Enable or Disable as appropriate.

## Configuring Service Logon

You can configure Windows Server 2003 services to log on as a system account or as a specific user. To do either of these, complete the following steps:

1. In the Computer Management console, connect to the computer whose services you want to manage.
2. Expand the Services And Applications node by clicking the plus sign (+) next to it, and then choose Services.
3. Right-click the service you want to configure, and then choose Properties.
4. Select the Log On tab, as shown in Figure 3-7.
5. Select Local System Account if the service should log on using the system account (which is the default for most services). If the service provides a user interface that can be manipulated, select Allow Service To Interact With Desktop to allow users to control the service's interface.
6. Select This Account if the service should log on using a specific user account. Be sure to type an account name and password in the fields provided. Use the Browse button to search for a user account, if necessary.
7. Click OK.



Distributed File System Properties (Local Computer)

Log on as:

● Local System account

☐ Allow service to interact with desktop

○ This account:

Password:

Confirm password:

You can enable or disable this service for the hardware profiles listed below:

| Hardware Profile | Service |
|---|---|
| Profile 1 | Enabled |

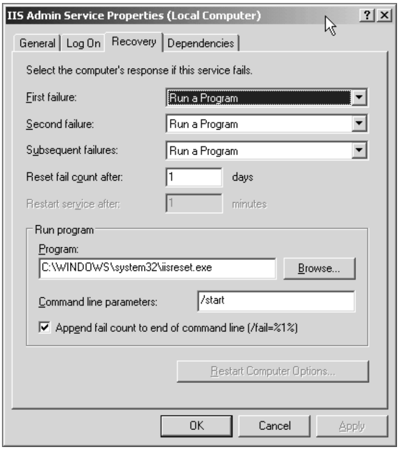
**Figure 3-7.** *Use the Log On tab to configure the service logon account.*

**Security Alert** As an administrator, you should keep track of any accounts that are used with services. These accounts can be the source of huge security problems if they're not configured properly. Service accounts should have the strictest security settings and as few permissions as possible while allowing the service to perform necessary functions. Typically, accounts used with services don't need many of the permissions you would assign to a normal user account. For example, most service accounts don't need the right to log on locally. Every administrator should know what service accounts are used (so they can better track use of these accounts), and the accounts should be treated as if they were administrator accounts. This means: secure passwords, careful monitoring of account usage, careful application of account permissions and privileges, and so on.

## Configuring Service Recovery

You can configure Windows Server 2003 services to take specific actions when a service fails. For example, you could attempt to restart the service or run an application. To configure recovery options for a service, complete the following steps:

1. In the Computer Management console, connect to the computer whose services you want to manage.
2. Expand the Services And Applications node by clicking the plus sign (+) next to it, and then choose Services.
3. Right-click the service you want to configure, and then choose Properties.
4. Select the Recovery tab, as shown in Figure 3-8.


IIS Admin Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Browse...
Restart Computer Options...
OK
Cancel
Apply

Select the computer's response if this service fails.

First failure: Run a Program

Second failure: Run a Program

Subsequent failures: Run a Program

Reset fail count after: 1 days

Restart service after: 1 minutes

Run program

Program: C:\WINDOWS\system32\iisreset.exe

Command line parameters: /start

☑ Append fail count to end of command line (/fail=%1%)

**Figure 3-8.** *Use the Recovery tab to specify actions that should be taken in case of service failure.*

**Note** Windows Server 2003 automatically configures recovery for some critical system services during installation. In Figure 3-8, you see that the IIS Admin service is set to run a program called Iisreset.exe if the service fails. This program is an application that corrects service problems and safely manages dependent IIS services while working to restart the service. Iisreset.exe requires the command line parameter/start as well.

5. You can now configure recovery options for the first, second, and subsequent recovery attempts. The available options are
    - **Take No Action** The operating system won't attempt recovery for this failure but might still attempt recovery of previous or subsequent failures.
    - **Restart the Service** Stops and then starts the service after a brief pause.
    - **Run a Program** Allows you to run a program or a script in case of failure. The script can be a batch program or a Windows script. If you select this option, set the full file path to the program you want to run and then set any necessary command line parameters to pass in to the program when it starts.
    - **Restart the Computer** Shuts down and then restarts the computer. Before you choose this option, double-check Startup and Recovery options as well as Hardware Profile options as discussed in the sections entitled "Configuring System Startup and Recovery" and "Configuring the Way Hardware Profiles Are Used," respectively, in Chapter 2, "Managing Servers Running Microsoft Windows Server 2003." You want the system to select defaults quickly and automatically.

**Best Practices** When you configure recovery options for critical services, you might want to try to restart the service on the first and second attempts and then reboot the server on the third attempt.

6. Configure other options based on your previously selected recovery options. If you elected to run a program as a recovery option, you'll need to set options in the Run Program panel. If you elected to restart the service, you'll need to specify the restart delay. After stopping the service, Windows Server 2003 waits for the specified delay before trying to start the service. In most cases a delay of 1–2 minutes should be sufficient.
7. Click OK.

## Disabling Unnecessary Services

As an administrator, it's your job to ensure server and network security, and unnecessary services are a potential source of security problems. For example, in many organizations that I've reviewed for security problems, I've found servers running Worldwide Web Publishing Service, Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP) Publishing Service when these services weren't needed.

Unfortunately, these services can make it possible for anonymous users to access servers and can also open the server to attack if not properly configured.

If you find services that aren't needed, you have several options. In the case of IIS Admin services, Domain Name System (DNS), and other services that are installed as separate Windows components, you could use the Add/Remove Programs utility in the Control Panel to remove the unnecessary component and its related services. Or you could simply disable the services that aren't being used. Typically, you'll want to start by disabling services rather than uninstalling components. This way, if you disable a service and another administrator or a user says they can't perform task X anymore, you can restore the related service, if necessary.

To disable a service, follow these steps:

1. In Computer Management, right-click the service you want to disable, and then choose Properties.
2. In the General tab, select Disabled as the option for the Startup Type drop-down list box.

Disabling a service doesn't stop a running service. It only prevents it from being started the next time the computer is booted, meaning the security risk still exists. To address this, click Stop in the Properties dialog box on the General tab, and then click OK.

# Event Logging and Viewing

Event logs provide historical information that can help you track down system and security problems. The Event Log service controls whether events are tracked on Windows Server 2003 systems. When this service is started, you can track user actions and system resource usage events with the following event logs:

- **Application Log** Records events logged by applications, such as the failure of Microsoft SQL Server to access a database. Default location is: %SystemRoot%\system32\config\AppEvent.Evt.
- **Directory Service** Records events logged by Active Directory directory service and its related services. Default location is: %SystemRoot%\system32\config\NTDS.Evt.
- **DNS Server** Records DNS queries, responses, and other DNS activities. Default location is: %SystemRoot%\system32\config\DNSEvent.Evt.
- **File Replication Service** Records file replication activities on the system. Default location is: %SystemRoot%\system32\config\NtFrs.Evt.
- **Security Log** Records events you've set for auditing with local or global group policies. Default location is: %SystemRoot%\system32\config\SecEvent.Evt.

**Note** Any user who needs access to the security log must be granted the user right to Manage Auditing and the Security Log. By default, members of the administrators group have this user right. To learn how to assign user rights, see "Configuring User Rights Policies" in Chapter 9, "Creating User and Group Accounts."

- **System Log** Records events logged by the operating system or its components, such as the failure of a service to start at bootup. Default location is: %SystemRoot%\system32\config\SysEvent.Evt.

**Security Alert** As administrators, we tend to monitor the application and system logs the most—but don't forget about the security log. The security log is one of the most important logs, and you should monitor it closely. If the security log on a server doesn't contain events, the likeliest reason is that local auditing hasn't been configured or that domain-wide auditing is configured, in which case you should monitor the security logs on domain controllers rather than member servers. Note also that any user who needs access to the security log must be granted the user right to Manage Auditing and the Security Log. By default, members of the Administrators group have this user right. To learn how to assign user rights, see the section entitled "Configuring User Rights Policies" in Chapter 9, "Creating User and Group Accounts."

# Accessing and Using the Event Logs

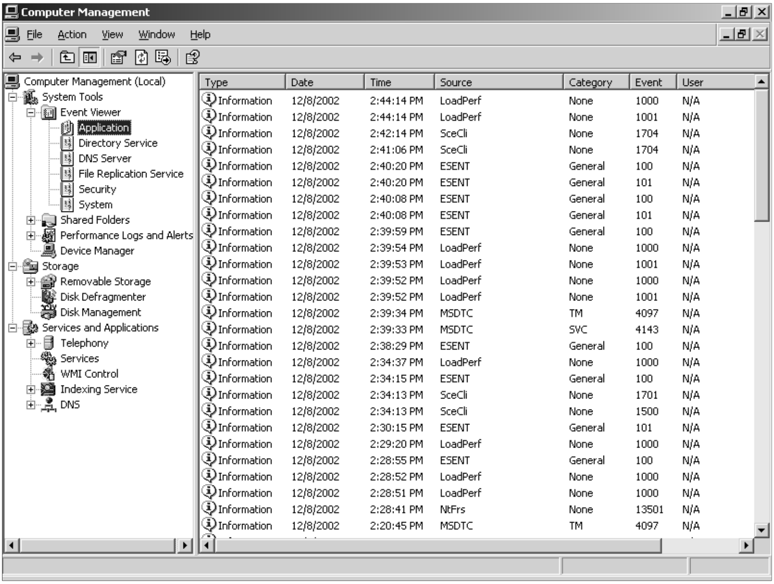
You access the event logs by completing the following steps:

1. In the Computer Management console, connect to the computer whose event logs you want to view or manage.
2. Expand the System Tools node by clicking the plus sign (+) next to it, and then double-click Event Viewer. You should now see a list of logs, as shown in Figure 3-9.
3. Select the log you want to view.

Entries in the main panel of Event Viewer provide a quick overview of when, where, and how an event occurred. To obtain detailed information on an event, double-click its entry. The event type precedes the date and time of the event. Event types include

- **Information** An informational event, which is generally related to a successful action.
- **Success Audit** An event related to the successful execution of an action.
- **Failure Audit** An event related to the failed execution of an action.
- **Warning** A warning. Details for warnings are often useful in preventing future system problems.
- **Error** An error, such as the failure of a service to start.

**Note** Warnings and errors are the two types of events that you'll want to examine closely. Whenever these types of events occur and you're unsure of the cause, double-click the entry to view the detailed event description.



| Type | Date | Time | Source | Category | Event | User |
|---|---|---|---|---|---|---|
| Information | 12/8/2002 | 2:44:14 PM | LoadPerf | None | 1000 | N/A |
| Information | 12/8/2002 | 2:44:14 PM | LoadPerf | None | 1001 | N/A |
| Information | 12/8/2002 | 2:42:14 PM | SceCli | None | 1704 | N/A |
| Information | 12/8/2002 | 2:41:06 PM | SceCli | None | 1704 | N/A |
| Information | 12/8/2002 | 2:40:20 PM | ESENT | General | 100 | N/A |
| Information | 12/8/2002 | 2:40:20 PM | ESENT | General | 101 | N/A |
| Information | 12/8/2002 | 2:40:08 PM | ESENT | General | 100 | N/A |
| Information | 12/8/2002 | 2:40:08 PM | ESENT | General | 101 | N/A |
| Information | 12/8/2002 | 2:39:59 PM | ESENT | General | 100 | N/A |
| Information | 12/8/2002 | 2:39:54 PM | LoadPerf | None | 1000 | N/A |
| Information | 12/8/2002 | 2:39:53 PM | LoadPerf | None | 1001 | N/A |
| Information | 12/8/2002 | 2:39:52 PM | LoadPerf | None | 1000 | N/A |
| Information | 12/8/2002 | 2:39:52 PM | LoadPerf | None | 1001 | N/A |
| Information | 12/8/2002 | 2:39:34 PM | MSDTC | TM | 4097 | N/A |
| Information | 12/8/2002 | 2:39:33 PM | MSDTC | SVC | 4143 | N/A |
| Information | 12/8/2002 | 2:38:29 PM | ESENT | General | 100 | N/A |
| Information | 12/8/2002 | 2:34:37 PM | LoadPerf | None | 1000 | N/A |
| Information | 12/8/2002 | 2:34:15 PM | ESENT | General | 100 | N/A |
| Information | 12/8/2002 | 2:34:13 PM | SceCli | None | 1701 | N/A |
| Information | 12/8/2002 | 2:34:13 PM | SceCli | None | 1500 | N/A |
| Information | 12/8/2002 | 2:30:15 PM | ESENT | General | 101 | N/A |
| Information | 12/8/2002 | 2:29:20 PM | LoadPerf | None | 1000 | N/A |
| Information | 12/8/2002 | 2:28:55 PM | ESENT | General | 100 | N/A |
| Information | 12/8/2002 | 2:28:52 PM | LoadPerf | None | 1000 | N/A |
| Information | 12/8/2002 | 2:28:51 PM | LoadPerf | None | 1000 | N/A |
| Information | 12/8/2002 | 2:28:41 PM | NtFrs | None | 13501 | N/A |
| Information | 12/8/2002 | 2:20:45 PM | MSDTC | TM | 4097 | N/A |

**Figure 3-9.** *Event Viewer displays events for the selected log.*

In addition to type, date, and time, the summary and detailed event entries provide the following information:

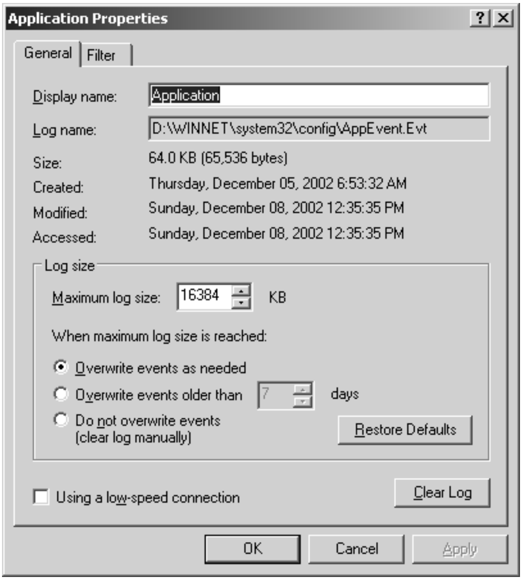
- **Source** The application, service, or component that logged the event
- **Category** The category of the event, which is sometimes used to further describe the related action
- **Event** An identifier for the specific event
- **User** The user account that was logged on when the event occurred
- **Computer** The name of the computer where the event occurred
- **Description** In the detailed entries, a text description of the event
- **Data** In the detailed entries, any data or error code output by the event

## Setting Event Log Options

Log options allow you to control the size of the event logs as well as how logging is handled. By default, event logs are set with a maximum file size of 512 KB. Then, when a log reaches this limit, events are overwritten to prevent the log from exceeding the maximum file size.

To set the log options, complete the following steps:

1. In the Computer Management console, double-click the Event Viewer entry. You should now see a list of event logs.
2. Right-click the event log whose properties you want to set and select Properties from the shortcut menu. This opens the dialog box shown in Figure 3-10.



Display name: Application

Log name: D:\WINNET\system32\config\AppEvent.Evt

Size: 64.0 KB (65,536 bytes)

Created: Thursday, December 05, 2002 6:53:32 AM

Modified: Sunday, December 08, 2002 12:35:35 PM

Accessed: Sunday, December 08, 2002 12:35:35 PM

Log size

Maximum log size: 16384 KB

When maximum log size is reached:

● Overwrite events as needed

○ Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

☐ Using a low-speed connection

**Figure 3-10.** *You should configure log settings according to the level of auditing on the system.*

3. Type a maximum size in the Maximum Log Size field. Make sure that the drive containing the operating system has enough free space for the maximum log size you select. Log files are stored in the %SystemRoot%\system32\config directory by default.

**Note** Throughout this book you'll see references to %SystemRoot%. This is an environment variable that Windows Server 2003 uses to designate the base directory for the Windows Server 2003 operating system, such as C:\WINDOWS. For more information on environment variables, see the section entitled "Configuring the User's Environment Settings" in Chapter 10, "Managing Existing User and Group Accounts."

4. Select an event log-wrapping mode. The options available are
   - **Overwrite Events As Needed** Events in the log are overwritten when the maximum file size is reached. Generally, this is the best option on a low priority system.
   - **Overwrite Events Older Than . . . Days** When the maximum file size is reached, events in the log are overwritten only if they are older than the setting you select. If the maximum size is reached and the events can't be overwritten, the system generates error messages telling you the event log is full.

- **Do Not Overwrite Events (Clear Log Manually)** When the maximum file size is reached, the system generates error messages telling you the event log is full.

5. Click OK when you're finished.

**Note** On critical systems where security and event logging is very important, you might want to use Overwrite Events Older Than . . . Days or Do Not Overwrite Events (Clear Log Manually). When you use these methods, you should archive and clear the log file periodically to prevent the system from generating error messages.

## Clearing Event Logs

When an event log is full, you need to clear it. To do that, complete the following steps:

1. In the Computer Management console, double-click the Event Viewer entry. You should now see a list of event logs.
2. Right-click the event log whose properties you want to set and select Clear All Events from the shortcut menu.
3. Choose Yes to save the log before clearing it. Choose No to continue without saving the log file.
4. When prompted to confirm that you want to clear the log, click Yes.

## Archiving Event Logs

On key systems such as domain controllers and application servers, you'll want to keep several months' worth of logs. However, it usually isn't practical to set the maximum log size to accommodate this. Instead, you should periodically archive the event logs.

### Archive Log Formats

Logs can be archived in three formats:

- Event log format for access in Event Viewer
- Tab-delimited text format, for access in text editors or word processors or import into spreadsheets and databases
- Comma-delimited text format, for import into spreadsheets or databases

When you export log files to a comma-delimited file, a comma separates each field in the event entry. The event entries look like this:

```
12/11/02,9:43:24 PM,DNS,Information,None,2,N/A,ZETA,The DNS server has
started.

12/11/02,9:40:04 PM,DNS,Error,None,4015,N/A,ZETA,The DNS server has
encountered a critical error from the Directory Service (DS). The data is
the error code.
```

The format for the entries is as follows:

```
Date,Time,Source,Type,Category,Event,User,Computer,Description
```

## Creating Log Archives

To create a log archive, complete the following steps:

1. In the Computer Management console, double-click the Event Viewer entry. You should now see a list of event logs.
2. Right-click the event log you want to archive and select Save Log File As from the shortcut menu.
3. In the Save As dialog box, select a directory and a log file name.
4. In the Save As Type dialog box, Event Log (*.evt) will be the default file type. Select a log format as appropriate and then choose Save.

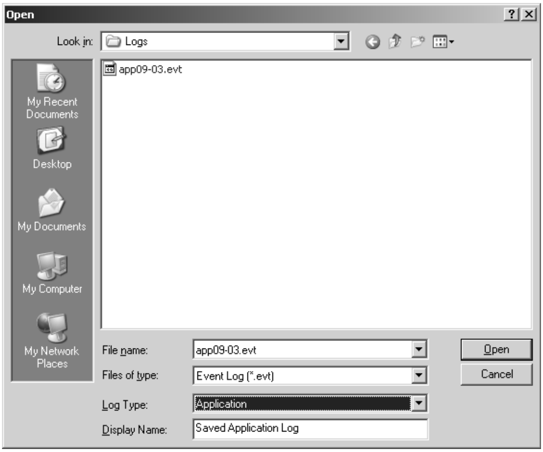
**Note** If you plan to archive logs regularly, you might want to create an archive directory. This way you can easily locate the log archives. You should also name the log file so that you can easily determine the log file type and the period of the archive. For example, if you're archiving the system log file for January 2003, you might want to use the file name System Log January 2003.

**Tip** The best format to use for archiving is the .evt format. Use this format if you plan to review old logs in the Event Viewer. However, if you plan to review logs in other applications, you might need to save the logs in a tab-delimited or comma-delimited format. With the tab-delimited or comma-delimited format, it's sometimes necessary to edit the log file in a text editor in order for the log to be properly interpreted. If you have saved the log in the .evt format, you can always save another copy as tab-delimited or comma-delimited format at a later date by doing another Save As after opening the archive in the Event Viewer.

## Viewing Log Archives

You can view log archives in text format in any text editor or word processor. You should view log archives in the event log format in Event Viewer. You can view log archives in Event Viewer by completing the following steps:

1. In the Computer Management console, right-click the Event Viewer entry. On the shortcut menu, select Open Log File. You should now see the Open dialog box shown in Figure 3-11.
2. Use the Open dialog box to select a directory and a log file name. If the log isn't saved in Event Viewer format, select All Files under the Files Of Type selection menu.
3. Use Log Type to specify the type of log as Application, Directory Service, and so on.
4. Click Open. The archived log is displayed as a separate view in Event Viewer. Select this view to display the saved events in the log.



File name: app09-03.evt

Files of type: Event Log (*.evt)

Log Type: Application

Display Name: Saved Application Log

**Figure 3-11.** *Use the Open dialog box to open the saved event log in a new view.*

# Monitoring Server Performance and Activity

Monitoring a server isn't something you should do haphazardly. You need to have a clear plan—a set of goals that you hope to achieve. Let's take a look at the reasons you might want to monitor a server and at the tools you can use to do this.

## Why Monitor Your Server?

Troubleshooting server performance problems is a key reason for monitoring. For example, users might be having problems connecting to the server and you might want to monitor the server to troubleshoot these problems. Here, your goal would be to track down the problem using the available monitoring resources and then to resolve it.

Another common reason for wanting to monitor a server is to improve server performance. You do this by improving disk I/O, reducing CPU usage, and cutting down on the network traffic load on the server. Unfortunately, often there are tradeoffs to be made when it comes to resource usage. For example, as the number of users accessing a server grows, you might not be able to reduce the network traffic load, but you might be able to improve server performance through load balancing or by distributing key data files on separate drives.

## Getting Ready to Monitor

Before you start monitoring a server, you might want to establish baseline performance metrics for your server. To do this, you measure server performance at various times and under different load conditions. You can then compare the baseline performance with subsequent performance to determine how the server is performing. Performance metrics that are well above the baseline measurements might indicate areas where the server needs to be optimized or reconfigured.

After you establish the baseline metrics, you should formulate a monitoring plan. A comprehensive monitoring plan includes the following steps:

1. Determining which server events should be monitored, to help you accomplish your goal
2. Setting filters to reduce the amount of information collected
3. Configuring monitors and alerts to watch the events
4. Logging the event data so that it can be analyzed
5. Analyzing the event data in Performance Monitor

These procedures are examined later in this chapter. Although you should develop a monitoring plan in most cases, there are times when you might not want to go through all these steps to monitor your server. For example, you might want to monitor and analyze activity as it happens rather than logging and analyzing the data later.

## Using Performance Monitor

Performance Monitor graphically displays statistics for the set of performance parameters you've selected for display. These performance parameters are referred to as *counters*. You can also update the available counters when you install services and add-ons on the server. For example, when you configure DNS on a server, Performance Monitor is updated with a set of objects and counters for tracking DNS performance. Performance Monitor creates a graph depicting the various counters you're tracking.

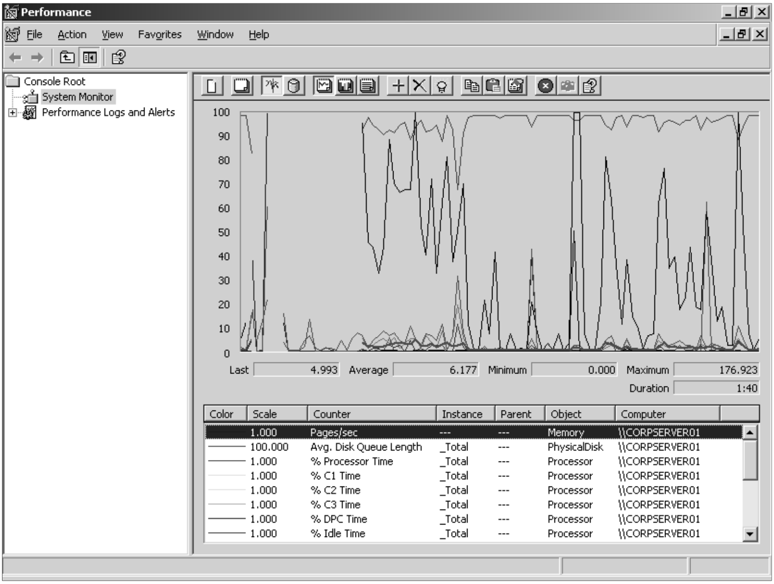
The update interval for this graph is completely configurable but by default is set to one second. As you'll see when you work with Performance Monitor, the tracking information is most valuable when you record the information in a log file and when you configure alerts to send messages when certain events occur or when certain thresholds are reached, such as when the CPU processor time reaches 99 percent. The sections that follow examine key techniques you'll use to work with performance monitor.

## Choosing Counters to Monitor

The Performance Monitor only displays information for counters you're tracking. Dozens of counters are available—and as you add services, you'll find there are even more. These counters are organized into groupings called *performance objects*. For example, all CPU-related counters are associated with the Processor object.

To select which counters you want to monitor, complete the following steps:

1. Select the Performance option on the Administrative Tools menu. This displays the Performance console.
2. Select the System Monitor entry in the left pane, as shown in Figure 3-12.



Last 4.993 Average 6.177 Minimum 0.000 Maximum 176.923
Duration 1:40

| Color | Scale | Counter | Instance | Parent | Object | Computer |
|---|---|---|---|---|---|---|
| | 1.000 | Pages/sec | --- | --- | Memory | \\CORPSERVER01 |
| | 100.000 | Avg. Disk Queue Length | _Total | --- | PhysicalDisk | \\CORPSERVER01 |
| | 1.000 | % Processor Time | _Total | --- | Processor | \\CORPSERVER01 |
| | 1.000 | % C1 Time | _Total | --- | Processor | \\CORPSERVER01 |
| | 1.000 | % C2 Time | _Total | --- | Processor | \\CORPSERVER01 |
| | 1.000 | % C3 Time | _Total | --- | Processor | \\CORPSERVER01 |
| | 1.000 | % DPC Time | _Total | --- | Processor | \\CORPSERVER01 |
| | 1.000 | % Idle Time | _Total | --- | Processor | \\CORPSERVER01 |

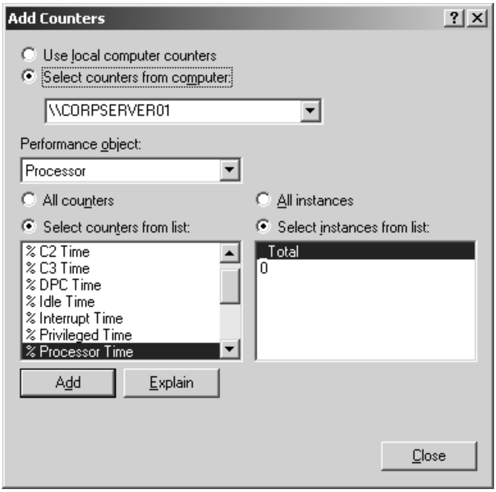
**Figure 3-12.** *Counters are listed in the lower portion of the Performance Monitor window.*

3. Performance Monitor has several viewing modes. Make sure you're in View Current Activity and View Graph display mode by clicking the View Current Activity and View Graph buttons on the Performance Monitor toolbar.
4. To add counters, click the Add button on the Performance Monitor toolbar or press Ctl+l. This displays the Add Counters dialog box shown in Figure 3-13. The key fields are
    - **Use Local Computer Counters** Configure performance options for the local computer.
    - **Select Counters From Computer** Enter the Universal Naming Convention (UNC) name of the server you want to work with, such as \\ZETA. Or use the selection list to select the server from a list of computers you have access to over the network.
    - **Performance Object** Select the type of object you want to work with, such as Processor.

**Tip** The easiest way to learn what you can track is to explore the objects and counters available in the Add Counters dialog box. Select an object in the Performance Object field, click the Explain button, and then scroll through the list of counters for this object.

- **All Counters** Select all counters for the current object.

- **Select Counters From List** Select one or more counters for the current object. For example, you could select % Processor Time and % User Time.
- **All Instances** Select all counter instances for monitoring.
- **Select Instances From List** Select one or more counter instances to monitor.


Add Counters

○ Use local computer counters

● Select counters from computer: \\CORPSERVER01

Performance object: Processor

○ All counters

● Select counters from list:
% C2 Time
% C3 Time
% DPC Time
% Idle Time
% Interrupt Time
% Privileged Time
% Processor Time

○ All instances

● Select instances from list:
_Total
0

**Figure 3-13.** *Select counters you want to monitor.*

**Best Practices** Don't try to chart too many counters or counter instances at once. You'll make the display difficult to read and you'll use system resources—namely CPU time and memory—that might affect server responsiveness.

5. When you've selected all the necessary options, click Add to add the counters to the chart. Then repeat this process, as necessary, to add other performance parameters.
6. Click Done when you're finished adding counters.
7. You can delete counters later by clicking their entry in the lower portion of the Performance window and then clicking Delete.

## Using Performance Logs

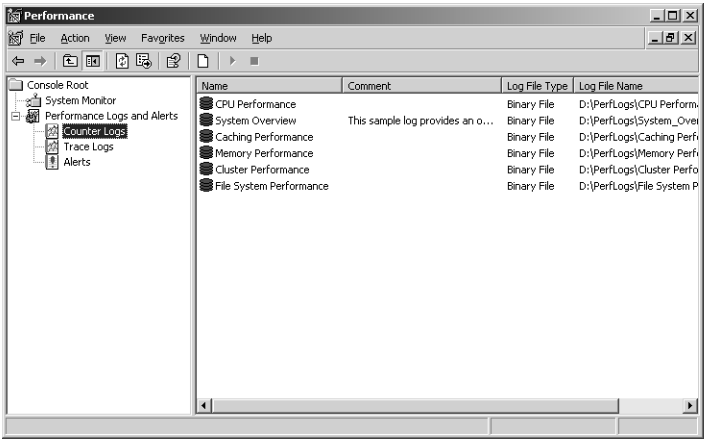
You can use performance logs to track the performance of a server, and you can replay them later. As you set out to work with logs, keep in mind that parameters that you track in log files are recorded separately from parameters that you chart in the Performance window. You can configure log files to update counter data automatically or manually. With automatic logging, a snapshot of key parameters is recorded at specific time intervals, such as every 10 seconds. With manual logging, you determine when snapshots are made. Two types of performance logs are available:

- **Counter logs** Record performance data on the selected counters when a predetermined update interval has elapsed
- **Trace logs** Record performance data whenever their related events occur

## Creating and Managing Performance Logging

To create and manage performance logging, complete the following steps:

1. Access the Performance console by selecting the Performance option on the Administrative Tools menu.
2. Expand the Performance Logs And Alerts node by clicking the plus sign (+) next to it. If you want to configure a counter log, select Counter Logs. Otherwise, select Trace Logs.
3. As shown in Figure 3-14, you should see a list of current logs (if any) in the right pane. A green log symbol next to the log name indicates logging is active. A red log symbol indicates logging is stopped.



| Name | Comment | Log File Type | Log File Name |
|---|---|---|---|
| CPU Performance | | Binary File | D:\PerfLogs\CPU Perform |
| System Overview | This sample log provides an o... | Binary File | D:\PerfLogs\System_Over |
| Caching Performance | | Binary File | D:\PerfLogs\Caching Perf |
| Memory Performance | | Binary File | D:\PerfLogs\Memory Perf |
| Cluster Performance | | Binary File | D:\PerfLogs\Cluster Perfo |
| File System Performance | | Binary File | D:\PerfLogs\File System P |

**Figure 3-14.** *Current performance logs are listed with summary information.*

4. You can create a new log by right-clicking in the right pane and selecting New Log Settings from the shortcut menu. A New Log Settings box appears, asking you to give a name to the new log settings. Type a descriptive name here before continuing.
5. To manage an existing log, right-click its entry in the right pane, and then select one of the following options:
   - **Delete** To delete the log
   - **Properties** To display the log properties dialog box
   - **Start** To activate logging
   - **Stop** To halt logging

- **Save Settings As** Saves the log configuration as a Web page that can be viewed in a browser, such as Internet Explorer, and imported into a new counter log using New Log Settings From

**Real World** The Hypertext Markup Language (HTML) page created using Save Settings As has an embedded Performance monitor that you can use to view the performance data you've configured. If you save the settings to a folder published under IIS, you'll be able to easily remotely view performance data. All you need to do is type the appropriate Uniform Resource Locator (URL) in the Web browser's Address field.

## Creating Counter Logs

Counter logs record performance data on the selected counters at a specific sample interval. For example, you could sample performance data for the CPU every 15 minutes. To create a counter log, complete the following steps:

1. Right-click Counter Logs in the left pane of the Performance console, and then choose New Log Settings.
2. In the New Log Settings dialog box, type a name for the log, such as **System Performance Monitor** or **Processor Status Monitor**. Then click OK.
3. To add all counters for specific performance objects, click Add Objects, and then use the Add Object dialog box to select the objects you want to add. All counters for these objects will be logged.
4. To add specific counters for objects, click Add Counters, and then use the Select Counters dialog box to select the counters you want to add.
5. In the Sample Data Every ... field, type in a sample interval and select a time unit in seconds, minutes, hours, or days. The sample interval specifies when new data is collected. For example, if you sample every 15 minutes, the log is updated every 15 minutes.

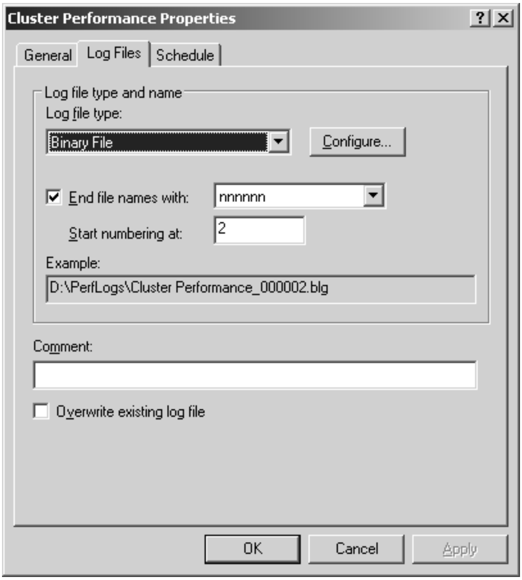
**Best Practices** Log files can grow in size very quickly. If you plan to log data for an extended period, be sure to place the log file on a drive with lots of free space. Remember, the more frequently you update the log file, the higher the drive space and CPU resource usage on the system.

6. In the Run As field, type the name of the account under which the counter log will run, and then click Set Password. After you type the password for the account and then confirm the password, click OK to close the Set Password dialog box. To run the log under the default system account, type **<Default>**.
7. Click the Log Files tab as shown in Figure 3-15. By default, counter logs are saved as sequentially numbered binary files in the %SystemDrive%\PerfLogs directory. If desired, change the log file defaults using the following options:
   - **Log File Type** Changes the default log type. Text File (Comma Delimited) creates a log file with comma-separated entries. Text File (Tab Delimited) creates a log file with tab-separated entries. Binary File creates a binary file that Performance Monitor can read. Binary Circular

File creates a binary file that overwrites old data with new data when the file reaches a specified size limit. SQL Database writes the performance data to a SQL Database.

- **End File Names With** Sets an automatic suffix for each new file created when you run the counter log. Logs can have a numeric suffix or a suffix in a specific date format.
- **Start Numbering At** Sets the first serial number for a log that uses an automatic numeric suffix.
- **Comment** Sets an optional description of the log, which is displayed in the Comment column.

**Tip** If you plan to use Performance Monitor to analyze or view the log, use one of the binary file formats.



Log file type: Binary File

☑ End file names with: nnnnnn

Start numbering at: 2

Example: D:\PerfLogs\Cluster Performance_000002.blg

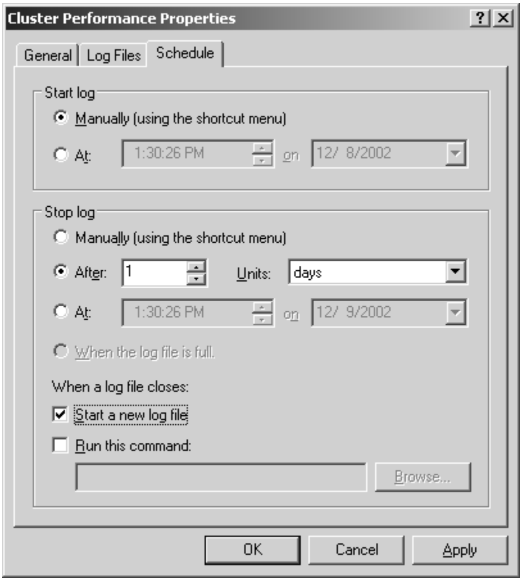
Comment:

☐ Overwrite existing log file

**Figure 3-15.** *Configure the log file format and usage.*

8. After you set the log file type, click Configure to configure the log file location. If you selected SQL Database as the file type, use the Configure SQL Logs dialog box to select a previously configured system data source name (DSN). The DSN is used to establish a connection to a SQL-compliant database. If you selected another file type, you'll be able to set the log file name and folder location. With either selection, you have the option of limiting the log file size to a specific value.
9. Click the Schedule tab, shown in Figure 3-16, and then specify when logging should start and stop.

10. You can configure the logging to start manually or automatically at a specific date. Select the appropriate option and then specify a start date if necessary.



Cluster Performance Properties

General | Log Files | Schedule

Start log

● Manually (using the shortcut menu)

○ At: 1:30:26 PM on 12/ 8/2002

Stop log

○ Manually (using the shortcut menu)

● After: 1 Units: days

○ At: 1:30:26 PM on 12/ 9/2002

○ When the log file is full.

When a log file closes:

☑ Start a new log file

☐ Run this command:

**Figure 3-16.** *Specify when logging starts and stops.*

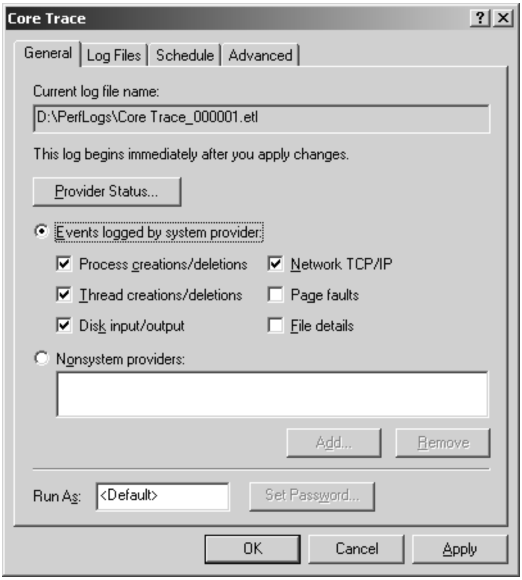
11. You can configure the log file to stop manually after a specified period of time, such as seven days, at a specific date and time, or when the log file is full (if you've set a specific file size limit). When a log file closes, you can start a new log file or run a command automatically as well.
12. Click OK when you've finished setting the logging schedule. The log is then created, and you can manage it as explained in the "Creating and Managing Performance Logging" section earlier in this chapter.

## Creating Trace Logs

Trace logs record performance data whenever events related to their source providers occur. A source provider is an application or operating system service that has traceable events.

To create a trace log, complete the following steps:

1. Right-click Trace Logs in the left pane of the Performance console, and then choose New Log Settings.
2. In the New Log Settings dialog box, type a name for the log, such as Logon Trace or Disk I/O Trace. Then click OK. This opens the dialog box shown in Figure 3-17.



Current log file name: D:\PerfLogs\Core Trace_000001.etl

This log begins immediately after you apply changes.

● Events logged by system provider:

☑ Process creations/deletions ☑ Network TCP/IP

☑ Thread creations/deletions ☐ Page faults

☑ Disk input/output ☐ File details

○ Nonsystem providers:

Run As: <Default>

**Figure 3-17.** *Use the General tab to select the provider to use in the trace.*

3. If you want to trace operating system events, select the Events Logged By System Provider option button. As shown in Figure 3-17, you can now select system events to trace.

**Caution** Collecting page faults and file details events puts a heavy load on the server and causes the log file to grow rapidly. Because of this, you should collect page faults and file details only for a limited amount of time.

4. If you want to trace another provider, select the Nonsystem Providers option button and then click Add. This displays the Add Nonsystem Providers dialog box, which you'll use to select the provider to trace.
5. In the Run As field, type the name of the account under which the counter log will run, and then click Set Password. After you type the password for the account and then confirm the password, click OK to close the Set Password dialog box. To run the log under the default system account, type **<Default>**.
6. When you're finished selecting providers and events to trace, select the Log Files tab. You can now configure the trace file as explained in Steps 7 and 8 of the section of this chapter entitled "Creating Counter Logs." The only change is that the log file types are different. With trace logs, you have two log types:
   - **Sequential Trace File** Writes events to the trace log sequentially up to the maximum file size (if any)
   - **Circular Trace File** Overwrites old data with new data when the file reaches a specified size limit

7. Choose the Schedule tab, and then specify when tracing starts and stops.
8. You can configure the logging to start manually or automatically at a specific date. Select the appropriate option, and then specify a start date, if necessary.
9. You can configure the log file to stop manually, after a specified period of time (such as seven days), at a specific date and time, or when the log file is full (if you've set a specific file size limit). When a log file closes, you can start a new log file or run a command automatically as well.
10. When you've finished setting the logging schedule, click OK. The log is then created and you can manage it as explained in the section of this chapter entitled "Creating and Managing Performance Logging."

## Viewing and Replaying Performance Logs

When you're troubleshooting problems, you'll often want to log performance data over an extended period of time and then replay the data to analyze the results. To do this, complete the following steps:

1. Configure automatic logging as described in the "Using Performance Logs" section of this chapter.
2. In Performance Monitor, select the System Monitor entry on the left pane and then right-click the System Monitor details pane. Finally, select Properties from the shortcut menu. This displays the System Monitor Properties dialog box.
3. Click the Source tab. Under Data Source, click Log Files and then click Add to open the Select Log File dialog box. You can now select the log file you want to analyze.
4. Specify the time window that you want to analyze. Click Time Range, and then drag the Total Range bar to specify the appropriate starting and ending times. Drag the left edge to the right to move up the start time. Drag the right edge to the left to move down the end time.
5. Select the Data tab. You can now select counters to view. Click the Add button. This displays the Add Counter dialog box, which you can use to select the counters that you want to analyze.

**Note** Only counters that you selected for logging are available. If you don't see a counter that you want to work with, you'll need to modify the log properties, restart the logging process, and then check the logs at a later date.

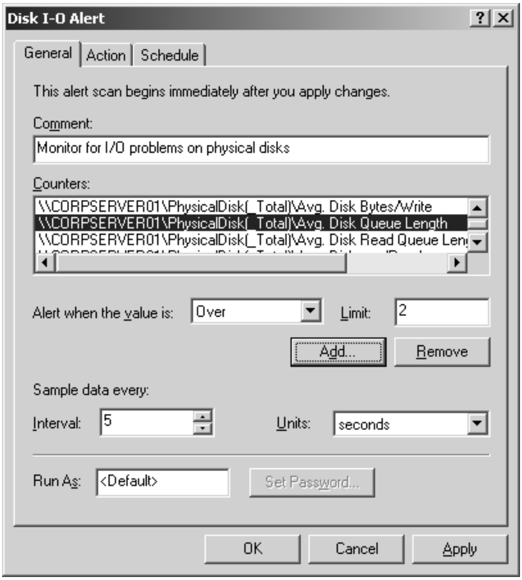
6. Click OK. Then in System Monitor, use the View Graph, View Histogram, and View Report buttons on the toolbar to display information based on the counters selected.

## Configuring Alerts for Performance Counters

You can configure alerts to notify you when certain events occur or when certain performance thresholds are reached. You can send these alerts as network messages and as events that are logged in the application event log. You can also configure alerts to start applications and performance logs.

To add alerts in Performance Monitor, complete the following steps:

1. Right-click Alerts in the left pane of the Performance console, and then choose New Alert Settings.
2. In the New Alert Settings dialog box, type a name for the alert, such as **Processor Alert** or **Disk I/O Alert**. Then click OK. This opens the dialog box shown in Figure 3-18.



This alert scan begins immediately after you apply changes.

Comment: Monitor for I/O problems on physical disks

Counters:
\\CORPSERVER01\PhysicalDisk(_Total)\Avg. Disk Bytes/Write
\\CORPSERVER01\PhysicalDisk(_Total)\Avg. Disk Queue Length
\\CORPSERVER01\PhysicalDisk(_Total)\Avg. Disk Read Queue Len

Alert when the value is: Over
Limit: 2

Sample data every:
Interval: 5
Units: seconds

Run As: <Default>

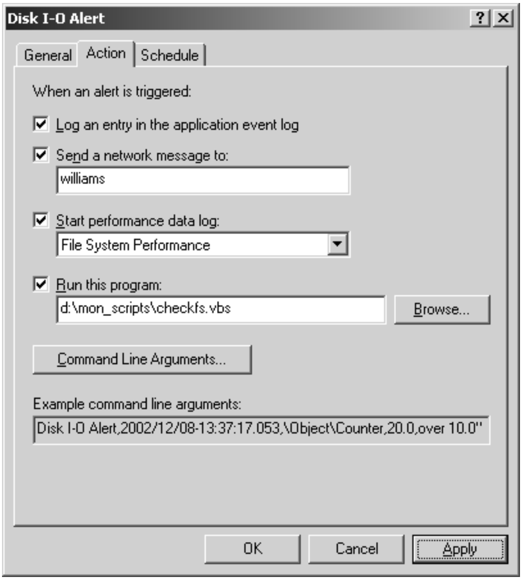
**Figure 3-18.** *Use the Disk I-O Alert dialog box to configure counters that trigger alerts.*

3. In the General tab, type an optional description of the alert. Then click Add to display the Add Counters dialog box. This dialog box is identical to the Add Counters dialog box shown previously in Figure 3-13.
4. Use the Add Counters dialog box to add counters that trigger the alert. Click Close when you're finished.
5. In the Counters panel, select the first counter and then use the Alert When Value Is ... field to set the occasion when an alert for this counter is triggered. Alerts can be triggered when the counter is over or under a specific value. Select Over or Under, and then set the trigger value. The unit of measurement is whatever makes sense for the currently selected counter(s). For example, to alert if processor time is over 95 percent, you would select Over and then type **95**. Repeat this process to configure other counters you've selected.

6. In the Sample Data Every ... field, type in a sample interval and select a time unit in seconds, minutes, hours, or days. The sample interval specifies when new data is collected. For example, if you sample every 10 minutes, the log is updated every 10 minutes.

**Caution** Don't sample too frequently. You'll use system resources and might cause the server to seem unresponsive to user requests.

7. In the Run As field, type the name of the account under which the counter log will run, and then click Set Password. After you type the password for the account and then confirm the password, click OK to close the Set Password dialog box. To run alert logging under the default system account, type **<Default>**.
8. Select the Action tab, shown in Figure 3-19. You can now specify any of the following actions to happen when an alert is triggered:
   - **Log An Entry In The Application Event Log** Creates log entries for alerts
   - **Send A Network Message To** Sends a network message to the computer specified
   - **Start Performance Data Log** Sets a counter log to start when an alert occurs
   - **Run This Program** Sets the complete file path of a program or batch file script to run when the alert occurs



When an alert is triggered:

☑ Log an entry in the application event log

☑ Send a network message to: williams

☑ Start performance data log: File System Performance

☑ Run this program: d:\mon_scripts\checkfs.vbs

Example command line arguments: Disk I-O Alert,2002/12/08-13:37:17.053,\Object\Counter,20.0,over 10.0"

**Figure 3-19.** *Set actions that are executed when the alert occurs.*

**Note** Alerts can be configured to run executable programs with the .exe extension and batch files with the .bat or .cmd extension when an alert is triggered. Be sure to type the full path to the program or batch file you want to run. The Run This Program text field will accept only valid file paths. If you enter an invalid file path, you'll see a warning specifying this when you click OK or try to access another tab. To pass arguments to an executable or batch file application, use the options of the Command Line Arguments panel. Normally, arguments are passed as individual strings. However, if you select Single Argument String, the arguments are passed in a comma-separated list within a single string. The Example Command Line Arguments list at the bottom of the tab shows how the arguments would be passed.

9. Choose the Schedule tab, and then specify when alerting starts and stops. For example, you could configure the alerts to start on a Friday evening and stop on Monday morning. Then each time an alert occurs during this period, the specified action(s) are executed.
10. You can configure alerts to start manually or automatically at a specific date. Select the appropriate option, and then specify a start date, if necessary.
11. You can configure alerts to stop manually or automatically after a specified period of time, such as seven days, or at a specific date and time.
12. When you've finished setting the alert schedule, click OK. The alert is then created, and you can manage it in much the same way that you manage counter and trace logs.

**Real World** Figure 3-19 shows the Run This Program field with the path to a Windows script with the .vbs extension as the action to take. If the .vbs script exists in the location specified, this will be accepted as a valid entry. However, when the alert is triggered, the Windows script won't run and an error will be entered in the Application event log. To run a Windows script as an action, you must follow the steps outlined in the section of this chapter entitled "Running Scripts as Actions."

## Running Scripts as Actions

Performance Logs And Alerts is the service responsible for handling alerts. To run batch scripts or any programs that launch command prompts or perform other actions that require access to the desktop, you'll need to configure the service so that it can interact with the desktop. To do this, complete the following steps:

1. Click Start, choose Settings, click Control Panel, double-click Administrative Tools, and then click Services.
2. Right-click Performance Logs And Alerts, and then click Properties.
3. In the Log On tab, select the Local System Account and Allow Service To Interact With Desktop check boxes.
4. In the General tab, click Start, and then click OK.

This allows the Performance Logs And Alerts service to execute batch (.bat, .cmd) and script (.js, .vbs, .wsf) files interactively. However, you can't enter the name of a Windows script directly in the Run This Program field. Instead, you must enter the path to the Windows Script engine that you want to run when the action is triggered, such as C:\WINDOWS\system32\Cscript.exe, and then set Command Line Arguments that point to the script you want to execute. To do this, follow these steps:

1. Set up the alert. For the alert action, select Run This Program. Click Browse. Use the Select File To Run dialog box to find the full path to the Windows Script engine you want to use, such as C:\WINDOWS\system32\Cscript.exe. Click Open.
2. In the Action tab of the alert Properties dialog box, click Command Line Arguments. In the Command Line Arguments dialog box, select Single Argument String and Text Message. Clear all other arguments.
3. In the Text Message field, type the full path to the script, such as c:\scripts\Test.vbs.
4. Click OK twice.
5. Select the Schedule tab, and then specify when alerting starts and stops. For example, you could configure the alerts to start on a Friday evening and stop on Monday morning. Then each time an alert occurs during this period, the specified action(s) are executed.
6. You can configure alerts to start manually or automatically at a specific date. Select the appropriate option, and then specify a start date, if necessary.
7. You can configure alerts to stop manually, after a specified period of time, such as seven days, or at a specific date and time.
8. When you've finished setting the alert schedule, click OK. The alert is then created, and you can manage it in much the same way that you manage counter and trace logs.

# Tuning System Performance

Now that you know how to monitor your system, let's look at how you can tune the operating system and hardware performance. The areas I'll examine are the following:

- Memory usage and caching
- Processor utilization
- Disk I/O
- Network bandwidth and connectivity

## Monitoring and Tuning Memory Usage

Memory is often the source of performance problems, and you should always rule out memory problems before examining other areas of the system. Systems use both physical and virtual memory. To rule out memory problems with a system, you should configure application performance, memory usage, and data throughput settings, and then monitor the server's memory usage to check for problems.

## Setting Application Performance and Memory Usage

Application performance and memory usage settings determine how system resources are allocated. In most cases, you want to give the operating system and background applications the lion's share of resources. This is especially true for Active Directory, file, print, and network and communications servers. On the other hand, for application, database and streaming media servers, you'll want to give the programs the server is running the most resources.

To check these settings, follow these steps:

1. Start the System utility from the Control Panel.
2. Access the Advanced tab in the System utility, and then display the Performance Options dialog box by clicking Settings on the Performance panel. Choose the Advanced tab.
3. The Processor Scheduling panel controls allocation of CPU time. To give more CPU time to the operating system and background services, select Background Services. Otherwise, select Programs.
4. The Memory Usage panel controls allocation of memory. To give more memory to the operating system and background services, select System Cache. Otherwise, select Programs.
5. Click OK.

## Setting Data Throughput

Data throughput settings control how well a server responds to user requests, file handles, and client connections. You can optimize data throughput settings in one of four ways:

- **Minimize Memory Used** Optimizes the server to serve a small number of users. This means very little system memory is reserved for user requests, file handles, and client connections. This allows the server to reserve memory for other purposes but doesn't necessarily reduce the size of the system cache or reserved memory. (You'll experience poor responsiveness and performance if there are a lot of user requests, file handles, and client connections.)
- **Balance** Optimizes the server for mixed usage environments where the server has multiple roles that include file and printer sharing as well as other tasks. This results in average responsiveness to requests, file handles, and client connections.
- **Maximize Data Throughput For File Sharing** Optimizes the server to handle file and print services. This means the server will dedicate as many resources as possible to handling user requests, file handles, and client connections, which improves responsiveness and can also improve performance for user, file, and client actions.
- **Maximize Data Throughput For Network Applications** Optimizes the server memory for distributed applications that manage their own memory cache, such as SQL Server and IIS. This reduces the size of the system cache and allows more memory to be allocated to applications.

To configure data throughput, complete the following steps:

1. Access Network Connections in Control Panel.
2. Right-click Local Area Connection, and then select Properties. This displays the Properties dialog box. Servers with multiple network interface cards will have multiple network connections shown in Network Connections. You should optimize each of these connections appropriately.
3. Select File And Printer Sharing For Microsoft Networks, and then click Properties.
4. On the Server Optimization tab, select the appropriate optimization setting. Click OK.
5. You'll need to reboot the server for these changes to take effect.

## Checking Memory, Caching, and Virtual Memory Usage

Now that you've optimized the system, you can determine how the system is using memory and check for problems. Table 3-1 provides an overview of counters that you'll want to track to uncover memory, caching, and virtual memory (paging) bottlenecks. The table is organized by issue category.

**Table 3-1. Uncovering Memory-Related Bottlenecks**

| Issue | Counters to Track | Details |
|---|---|---|
| Physical and virtual memory usage | Memory\Available Kbytes<br>Memory\Committed Bytes | Memory\Available Kbytes is the amount of physical memory available to processes running on the server. Memory\Committed Bytes is the amount of committed virtual memory. If the server has very little available memory, you might need to add memory to the system. In general, you want the available memory to be no less than 5 percent of the total physical memory on the server. If the server has a high ratio of committed bytes to total physical memory on the system, you might need to add memory as well. In general, you want the committed bytes value to be no more than 75 percent of the total physical memory. |
| Memory page faults | Memory\Page Faults/sec<br>Memory\Pages Input/sec<br>Memory\Page Reads/sec | A page fault occurs when a process requests a page in memory and the system can't find it at the requested location. If the requested page is elsewhere in memory, the fault is called a *soft page fault*. If the requested page must be retrieved from disk, the fault is called a *hard page fault*. Most processors can handle large numbers of soft faults. Hard faults, however, can cause significant delays. Page Faults/sec is the overall rate at which the processor handles all types of page faults. Pages Input/sec is the total number of pages read from disk to resolve hard page faults. Page Reads/sec is the total disk reads needed to resolve hard page faults. Pages Input/sec will be greater than or equal to Page Reads/sec and can give you a good idea of your hard page fault rate. If there are a high number of hard page faults, you may need to increase the amount of memory or reduce the cache size on the server. |

*(continued)*

**Table 3-1. Uncovering Memory-Related Bottlenecks** *(continued)*

| Issue | Counters to Track | Details |
|---|---|---|
| Memory paging | Memory\Pool Paged Bytes, Memory\Pool Nonpaged Bytes | These counters track the number of bytes in the page and nonpaged pool. The paged pool is an area of system memory for objects that can be written to disk when they aren't used. The nonpaged pool is an area of system memory for objects that can't be written to disk. If the size of the page pool is large relative to the total amount of physical memory on the system, you might need to add memory to the system. If the size of the nonpaged pool is large relative to the total amount of virtual memory allocated to the server, you might want to increase the virtual memory size. |

## Monitoring and Tuning Processor Usage

The CPU does the actual processing of information on your server. As you examine a server's performance, you should focus on the CPU after memory bottlenecks have been eliminated. If the server's processors are the performance bottleneck, adding memory, drives, or network connections won't overcome the problem. Instead, you might need to upgrade the processors to faster clock speeds or add processors to increase the server's upper capacity. You could also move processor-intensive applications, such as SQL Server, to another server.

Before you make a decision to upgrade CPUs or add CPUs, you should rule out problems with memory and caching. If signs still point to a processor problem, you should monitor the performance counters discussed in Table 3-2. Be sure to monitor these counters for each CPU installed on the server.

**Table 3-2. Uncovering Processor-Related Bottlenecks**

| Issue | Counters to Track | Details |
|---|---|---|
| Thread queuing | System\Processor Queue Length | This counter displays the number of threads waiting to be executed. These threads are queued in an area shared by all processors on the system. If this counter has a sustained value of two or more threads, you'll need to upgrade or add processors. |
| CPU usage | Processor\ %Processor Time | This counter displays the percentage of time the selected CPU is executing a nonidle thread. You should track this counter separately for all processor instances on the server. If the % Processor Time values are high while the network interface and disk I/O throughput rates are relatively low, you'll need to upgrade or add processors. |

## Monitoring and Tuning Disk I/O

With today's high-speed disks, the disk throughput rate is rarely the cause of a bottleneck. That said, however, accessing memory is much faster than accessing disks. So, if the server has to do a lot of disk reads and writes, the server's overall performance can be degraded. To reduce the amount of disk I/O, you want the server to manage memory very efficiently and page to disk only when necessary. You monitor and tune memory usage as discussed previously in the "Monitoring and Tuning Memory Usage" section of this chapter.

Beyond the memory tuning discussion, you can monitor some counters to gauge disk I/O activity. Specifically, you should monitor the counters discussed in Table 3-3.

**Table 3-3. Uncovering Drive-Related Bottlenecks**

| Issue | Counters to Track | Details |
|---|---|---|
| Overall drive performance | PhysicalDisk\% Disk Time in conjunction with Processor\% Processor Time and Network Interface Connection\Bytes Total/sec | If the % Disk Time value is high and the processor and network connection values aren't high, the system's hard disk drives might be creating a bottleneck. Be sure to monitor % Disk Time for all hard disk drives on the server. |
| Disk I/O | PhysicalDisk\Disk Writes /sec, Physical Disk\ Disk Reads/sec, Physical Disk\Avg. Disk Write Queue Length, Physical Disk\Avg. Disk Read Queue Length, Physical Disk\Current Disk Queue Length | The number of writes and reads per second tell you how much disk I/O activity there is. The write and read queue lengths tell you how many write or read requests are waiting to be processed. In general, you want there to be very few waiting requests. Keep in mind that the request delays are proportional to the length of the queues minus the number of drives in a redundant array of independent disks (RAID) set. |

## Monitoring and Tuning Network Bandwidth and Connectivity

No other factor weighs more in the way a user perceives your server's performance than the network that connects your server to the user's computer. The delay, or latency, between when a request is made and the time it's received can make all the difference. If there's a high degree of latency, it doesn't matter if you have the fastest server on the planet. The user experiences a delay and perceives that your servers are slow.

Generally speaking, the latency the user experiences is beyond your control. It's a function of the type of connection the user has and the route the request takes to your server. The total capacity of your server to handle requests and the amount of bandwidth available to your servers are factors under your control, however. Network bandwidth availability is a function of your organization's network infrastructure. Network capacity is a function of the network cards and interfaces configured on the servers.

The capacity of your network card can be a limiting factor in some instances. Most servers use 10/100 network cards, which can be configured in many ways. Someone might have configured a card for 10 Mbps or the card might be configured for half duplex instead of full duplex. If you suspect a capacity problem with a network card, you should always check the configuration.

To determine the throughput and current activity on a server's network cards, you can check the following counters:

- Network\Bytes Received/sec
- Network\Bytes Sent/sec
- Network\Bytes Total/sec
- Network Current Bandwidth

If the total bytes per second value is more than 50 percent of the total capacity under average load conditions, your server might have problems under peak load conditions. You might want to ensure that operations that take a lot of network bandwidth, such as network backups, are performed on a separate interface card. Keep in mind that you should compare these values in conjunction with PhysicalDisk\% Disk Time and Processor\% Processor Time. If the disk time and processor time values are low but the network values are very high, there might be a capacity problem. Solve the problem by optimizing the network card settings or by adding an additional network card. Remember, planning is everything—it isn't always as simply as inserting a card and plugging it into the network.