

Optimizing Windows

**In this chapter,
you will learn:**

- About Windows utilities and tools you can use to solve problems with Windows
- How to optimize Windows to improve performance


In the last chapter, you learned about the tools and strategies to maintain Windows and its hardware resources and about the importance of keeping good backups of data and system files. This chapter takes you one step further as a PC support technician so that you can get the best performance out of Windows. We begin the chapter learning about the Windows tools you'll need to optimize Windows. As a support technician, because you might be called on to edit the Windows registry, you'll also learn about the registry and how to safely edit it manually. Then we turn our attention to the steps you can follow to cause a sluggish Windows system to perform at its best. As you read, you might consider following the steps in the chapter first using a Windows Vista system and then going through the chapter again using a Windows XP system.

WINDOWS UTILITIES AND TOOLS TO SUPPORT THE OS

A+
220-701
3.2

Windows offers some powerful tools to help you understand what is happening behind the scenes with processes that are launched during and after startup, with events that might indicate a problem with software, hardware, or security, and with performance. By knowing how and when to use these tools, you can quickly zero in on a Windows problem or a performance block. In this part of the chapter, you will learn how to use the tools and then later in the chapter, you will see how these tools can help you when following the step-by-step strategy to optimize Windows.

Tools covered in this part of the chapter include Task Manager, System Configuration Utility (commonly called MSconfig), Services console, Computer Management console, Microsoft Management Console (MMC), Event Viewer, Reliability and Performance Monitor, and the Registry Editor. So, let's get started.

 **A+ Exam Tip** The A+ 220-701 Essentials exam expects you to know how to use Task Manager, MSconfig, the Services console, Computer Management console, MMC, Event Viewer, and Performance Monitor (also called the System Monitor).

TASK MANAGER

Task Manager (Taskmgr.exe) lets you view the applications and processes running on your computer as well as information about process and memory performance, network activity, and user activity. There are several ways you can access Task Manager:

- ▲ Press **Ctrl+Alt+Delete**. Depending on your system, Task Manager appears or the Windows Security screen appears. If the security screen appears, click **Start Task Manager**.
- ▲ Right-click a blank area on the taskbar, and then select **Task Manager** on the shortcut menu.
- ▲ Press **Ctrl+Shift+Esc**.
- ▲ Enter **taskmgr.exe** in the Vista Start Search box or the XP Run dialog box and press **Enter**.

Windows Vista Task Manager has six tabs: Applications, Processes, Services, Performance, Networking, and Users (see Figure 14-1). Windows XP Task Manager does not have the Services tab (see Figure 14-2). The Windows XP Users tab shows only when a system is set for Fast User Switching and lets you monitor other users logged onto the system.

Let's see how each tab of the Task Manager window works.

APPLICATIONS TAB

On the Applications tab shown in Figure 14-1, each application loaded can have one of two states: Running or Not Responding. If an application is listed as Not Responding, you can end it by selecting it and clicking the **End Task** button at the bottom of the window. The application will attempt a normal shutdown; if data has not been saved, you are given the opportunity to save it.

PROCESSES TAB

The Processes tab of Task Manager lists system services and other processes associated with applications, together with how much CPU time and memory the process uses. This

A+
220-701
3.2

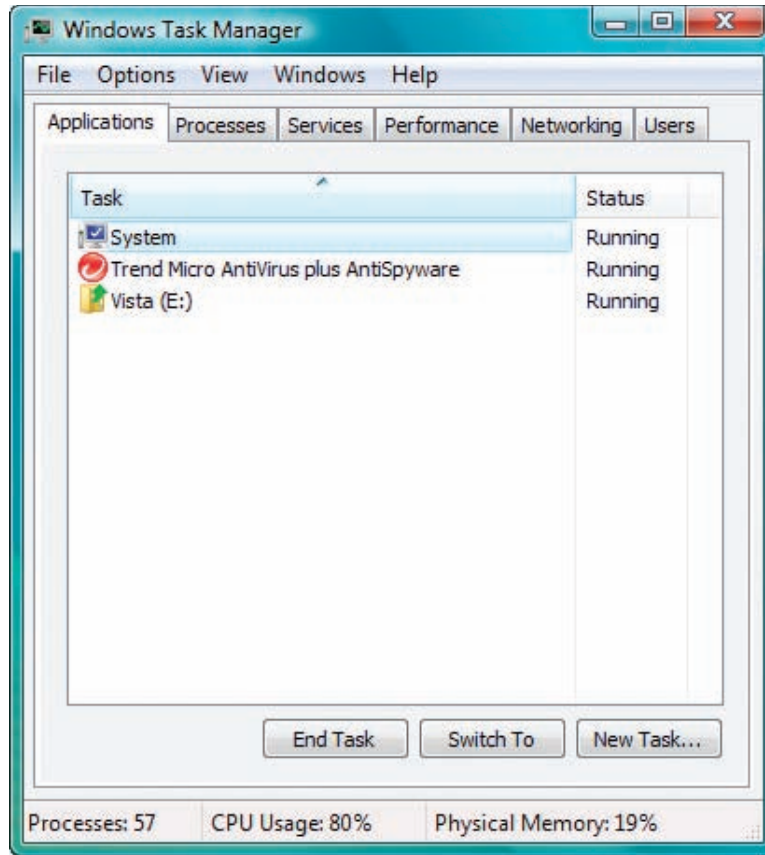


Figure 14-1 The Applications tab in Task Manager shows the status of active applications
Courtesy: Course Technology/Cengage Learning

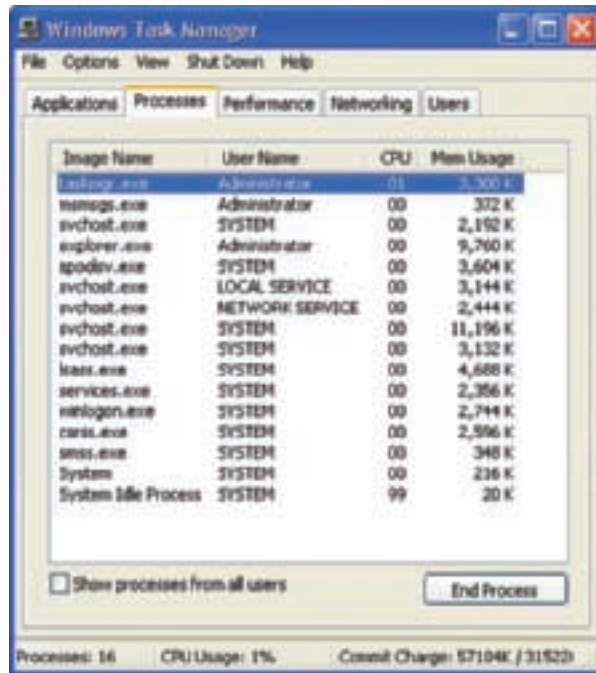


Figure 14-2 This Processes tab of Windows XP Task Manager shows Windows processes before any applications are installed
Courtesy: Course Technology/Cengage Learning

A+
220-701
3.2

information can help you determine which applications are slowing down your system. The Processes tab for Windows Vista Task Manager (see Figure 14-3) shows the processes running under the current user. This screen shot was taken immediately after a Vista installation before any applications were installed. To see all processes running, click **Show processes from all users** and respond to the UAC box (see Figure 14-4). Task Manager now shows processes running under the current user, System, Local Service, and Network Service accounts. Services running under these last three accounts cannot display a dialog box on-screen or interact with the user. To do that, the service must be running under a user account. Also, a service running under the System account has more core privileges than does a service running under another account. Figure 14-2 shows the list of processes for a Windows XP system immediately after the installation was completed with no applications installed.

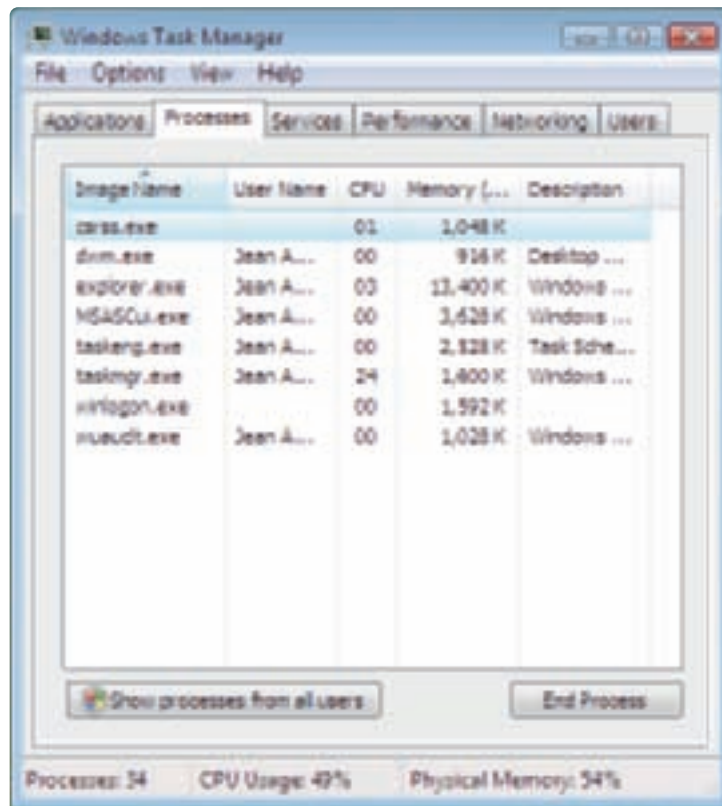


Figure 14-3 Processes running under the current user for a new Vista installation
Courtesy: Course Technology/Cengage Learning

When you have a sluggish Windows system, close all open applications and open Task Manager. Check the **Applications** tab to make sure no applications are running. Then click the **Processes** tab. Compare the list in Figure 14-2 (for Windows XP) or Figure 14-3 (for Windows Vista) with the list of processes running on the sluggish system. Any extra processes you see might be caused by unwanted applications running in the background or malicious software running. If you see a process running that you are not familiar with, search the Microsoft Web site (support.microsoft.com) to verify the process is legitimate. If you don't find it there, do a general Google search on the process. If you find that the process is not legitimate, stop the process and immediately run antivirus software. Chapter 20 gives more information about ridding your system of malicious software and about the processes you see listed in the Task Manager window.

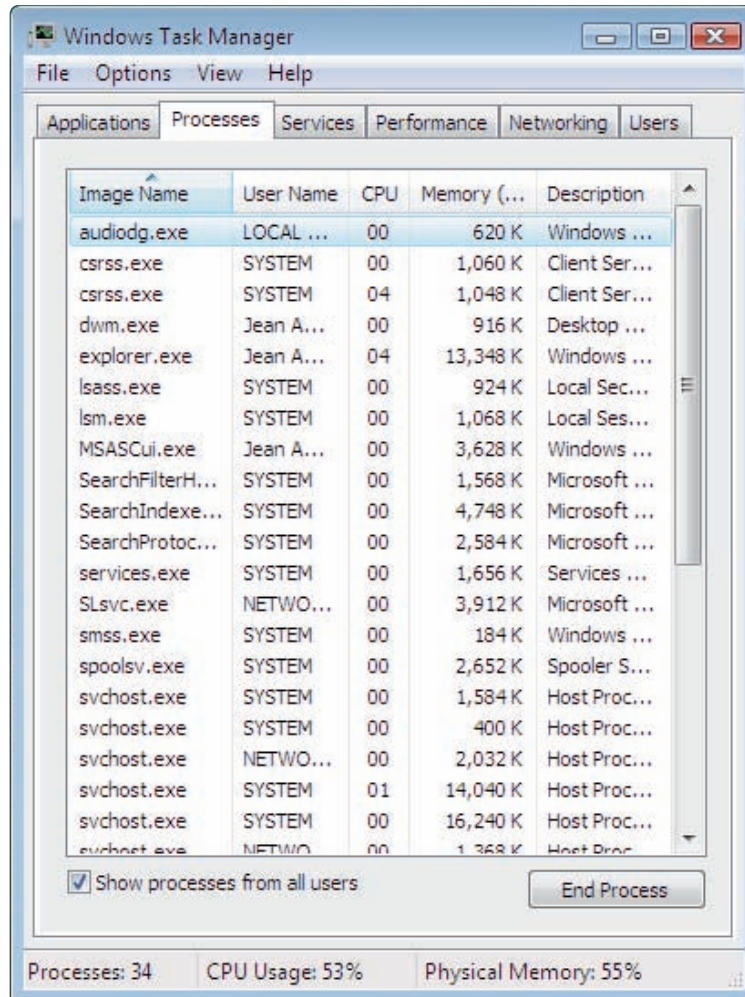


Figure 14-4 Vista processes for all users
Courtesy: Course Technology/Cengage Learning



Caution

A word of caution is important here: Many Web sites will tell you a legitimate process is malicious so that you will download and use their software to get rid of the process. However, their software is likely to be adware or spyware that you don't want. Make sure you can trust a site before you download from it or take its advice.

To stop a process using Task Manager, select the process and click **End Process**. The process is ended abruptly. If the process belongs to an application, you will lose any unsaved information in the application. Therefore, if an application is hung, try using the Applications tab to end the task before turning to the Processes tab to end its underlying process.

When an application is listed on the Applications tab, you can right-click it and select **Go To Process** on the shortcut menu (see Figure 14-5). Task Manager will take you to the Processes tab and the running process for this application.

If you want to end the process and all related processes, right-click the process and select **End Process Tree** from the shortcut menu. Be careful to not end critical Windows processes; ending these might crash your system.

Each application running on your computer is assigned a priority level, which determines its position in the queue for CPU resources. You can use Task Manager to change the priority level for an application that is already loaded. If an application performs slowly, increase

A+
220-701
3.2

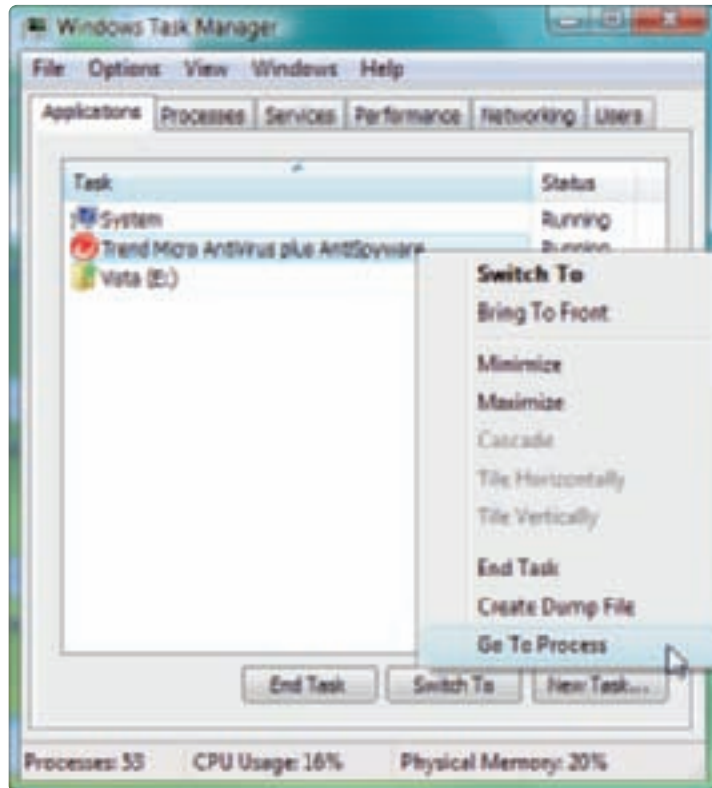


Figure 14-5 Find the running process for this running application
Courtesy: Course Technology/Cengage Learning

its priority. You should only do this with very important applications, because giving an application higher priority than certain background system processes can sometimes interfere with the operating system.

Notes If your desktop locks up, you can use Task Manager to refresh it. To do so, press **Ctrl+Alt+Del** and then click **Task Manager**. Click the **Processes** tab. Select **Explorer.exe** (the process that provides the desktop) and then click **End Process**. Click **End process** in the warning box. Then click the **Applications** tab. Click **New Task**. Enter **Explorer.exe** in the Create New Task dialog box and click **OK**. Your desktop will be refreshed and any running programs will still be open.

To use Task Manager to change the priority level of an open application, do the following:

1. In Task Manager, click the **Applications** tab. Right-click the application and select **Go To Process** from the shortcut menu. The **Processes** tab is selected and the process that runs the application is selected.
2. Right-click the selected process. From the shortcut menu that appears, set the new priority to **AboveNormal** (see Figure 14-6). If that doesn't give satisfactory performance, then try **High**.

Notes Remember: any changes you make to an application's priority level affect only the current session.

SERVICES TAB

The third Vista tab, the Services tab, is shown in Figure 14-7. This tab lists the services currently installed along with the status of each service. Recall that a service is a program that runs in the background and is called on by other programs to perform a background task.

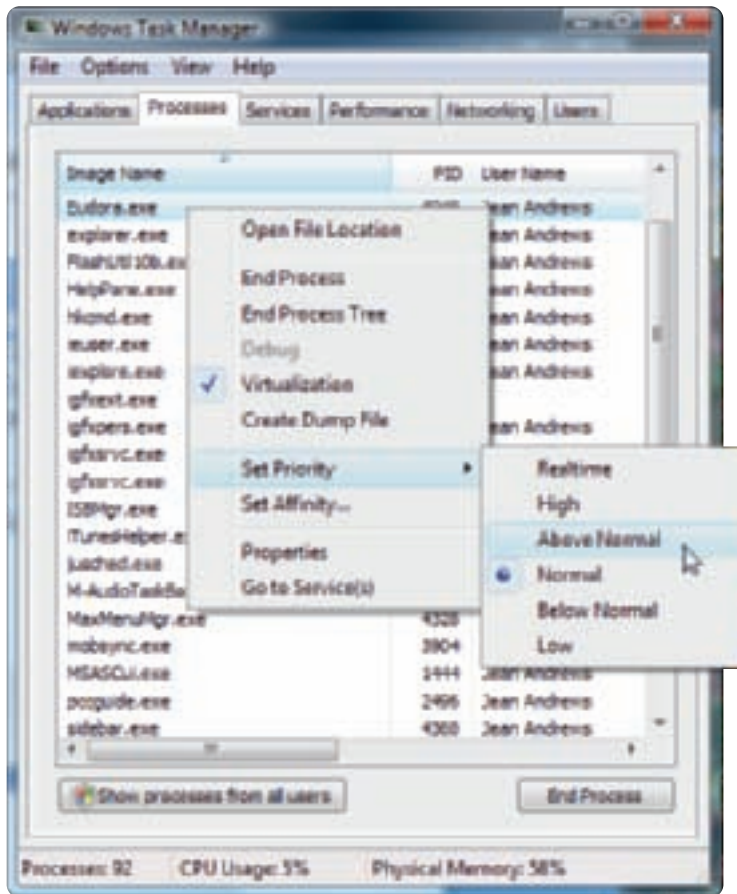


Figure 14-6 Change the priority level of a running application
Courtesy: Course Technology/Cengage Learning

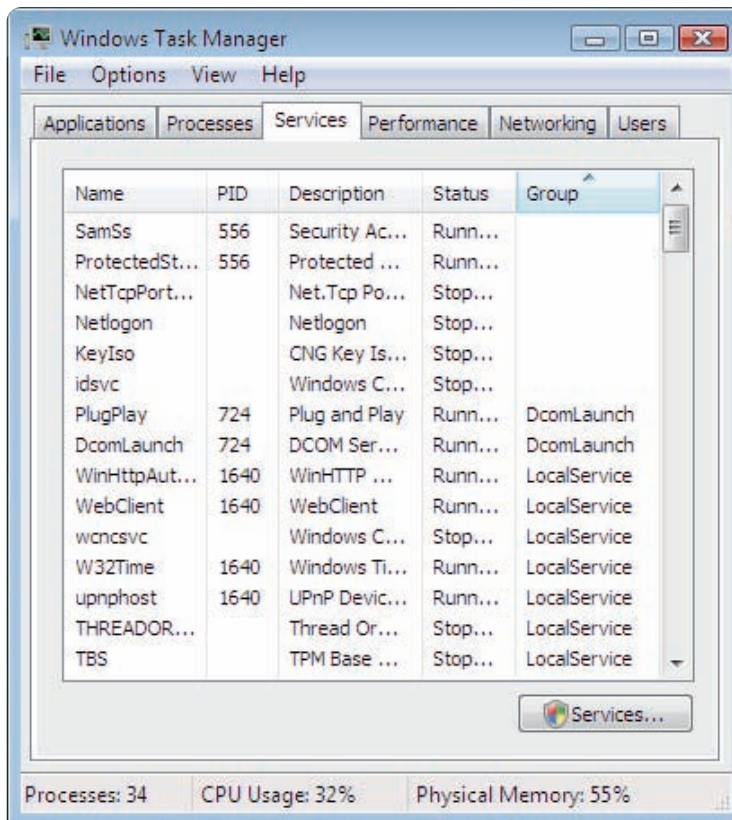


Figure 14-7 This Services tab of Windows Vista Task Manager gives the current status of all installed services
Courtesy: Course Technology/Cengage Learning

A+
220-701
3.2

Running services are sometimes listed in the notification area of the taskbar. To manage a service, click the Services button at the bottom of the window to go to the Services console. How to use this console is discussed later in the chapter.

PERFORMANCE TAB

The fourth Vista tab, the Performance tab, is shown in Figure 14-8. It provides details about how a program uses system resources. You can use these views to identify which applications and processes use the most CPU time.

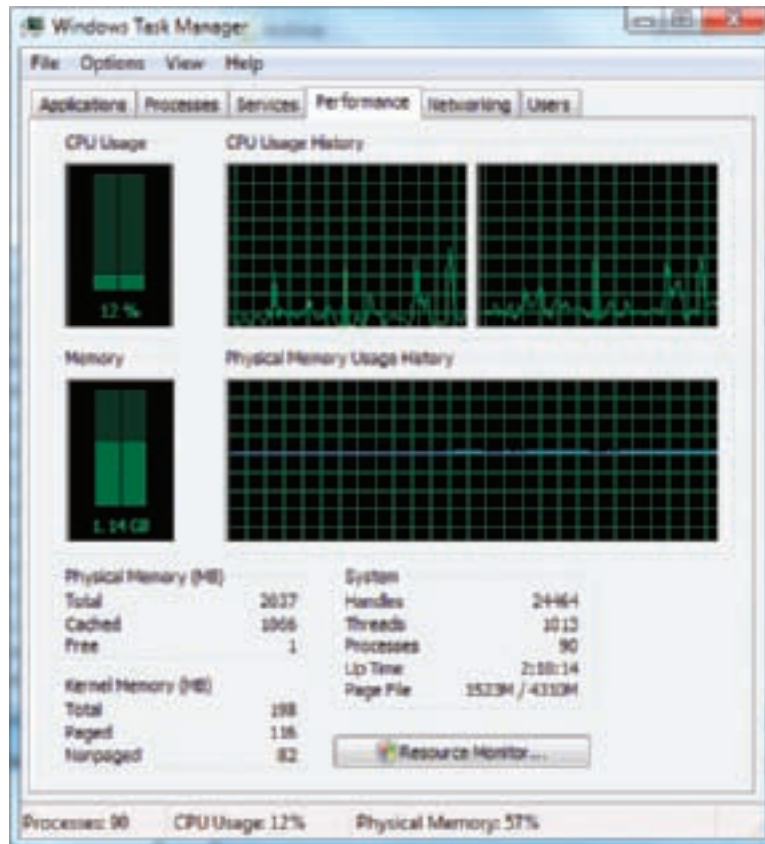


Figure 14-8 The Performance tab window shows details about how system resources are being used. Courtesy: Course Technology/Cengage Learning

On the Performance tab, you'll find five graphs near the top of the window and three frames near the bottom of the window. Here is an explanation of how they are used:

- ▲ The *CPU Usage* graph indicates the percentage of time the CPU is currently being used.
- ▲ The *CPU Usage History* graphs show this same percentage of use over recent time.
- ▲ The left *Memory* graph shows the amount of memory currently used.
- ▲ The right *Physical Memory Usage History* shows how much memory has recently been used. If this blue bar is a flat line near the top of the graph, you need to add more RAM to the system.
- ▲ The *Physical Memory (MB)* frame lists Total (amount of RAM), Cached (RAM that has recently been cached), and Free (RAM that recently has not been used).

A+
220-701
3.2

- ▲ The *Kernel Memory* frame indicates how much RAM and virtual memory the core kernel components of Windows are using. This frame lists Total (sum of RAM and virtual memory), Paged (how much of the paging file the kernel uses), and Nonpaged (how much RAM the kernel uses).
- ▲ The *System* frame gives information about the overall system status. This frame lists Handles (number of running objects used by all processes), Threads (number of subprocesses), Processes (number of running processes), Up Time (time since the computer was last restarted), and Page File (the first number is the amount of RAM and virtual memory currently in use, and the second number is total RAM and virtual memory).

To get even more detailed information about how Windows is performing, click the **Resource Monitor** button. You will be taken to the Resource Monitor window, discussed later in the chapter.

NETWORKING TAB

The Networking tab lets you monitor network activity and bandwidth used. You can use it to see how heavily the network is being used by this computer. For example, in Figure 14-9,

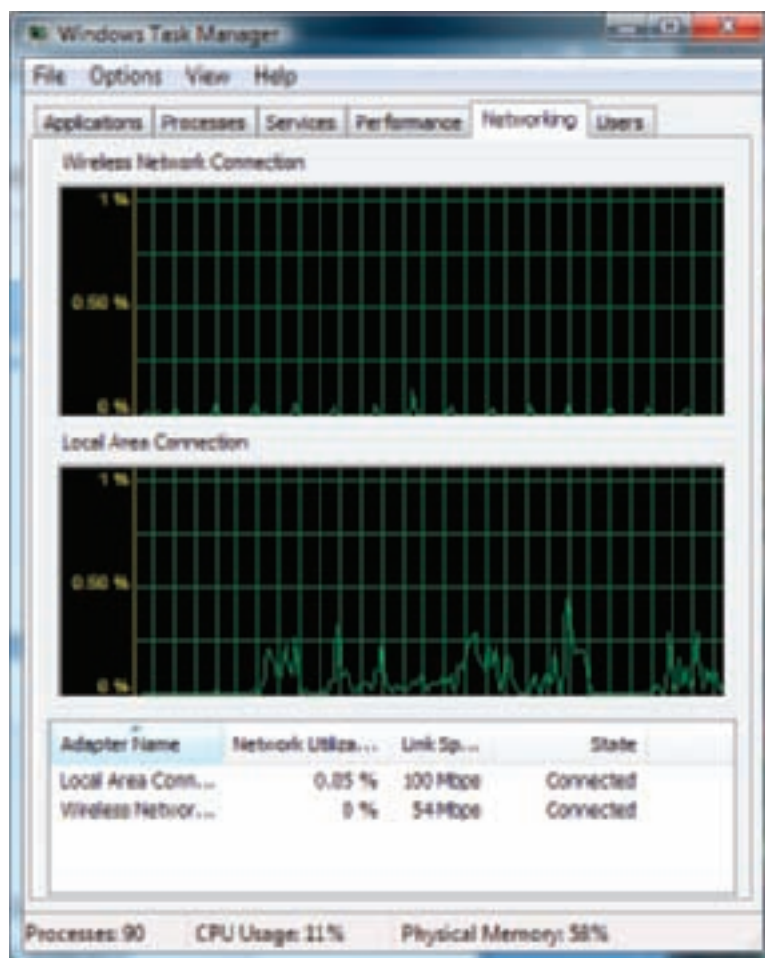


Figure 14-9 Use the Networking tab of Task Manager to monitor network activity
Courtesy: Course Technology/Cengage Learning

A+
220-701
3.2

you can see that the wireless connection is running at 54 Mbps, while the local (wired) connection is running at 100 Mbps. You can also see moderate network activity.

USERS TAB

The Users tab shows all users currently logged on the system. To improve Windows performance or just before you shut down the system, you can log off a user. To log off a user, first select the **Processes** tab and click **Show processes from all users** and respond to the UAC box. Then return to the Users tab, select the user, and click **Logoff**. The dialog box shown in Figure 14-10 appears, warning that unsaved data might be lost. Click **Log off user** to complete the operation.

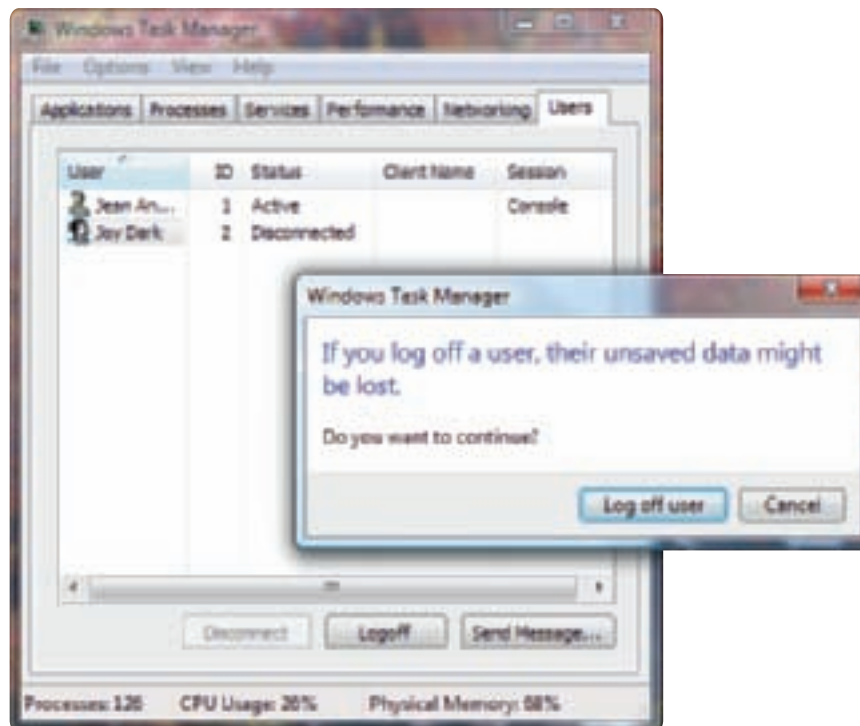


Figure 14-10 Use Task Manager to log off a user
Courtesy: Course Technology/Cengage Learning

APPLYING CONCEPTS

Suppose a friend asks you to help her solve a problem with her Windows XP system that is moving very slowly. You open Task Manager, select the **Processes** tab, and see a window similar to that in Figure 14-11. Notice that the Ccapp.exe process is using 99 percent of CPU time. When you click the **Performance** tab, you see why the system is running so slowly (see Figure 14-12). This one process is consistently using most of the CPU resources.

When you try to lower the priority of this process, you discover the process will not relinquish priority (see Figure 14-13). The next step is to investigate the process. Is it legitimate? Is it a virus? Can it be better managed or not used? If you do a Google search on Ccapp.exe, you'll discover the process belongs to Norton AntiVirus software. The solution is to disable scanning of outgoing e-mail so the process will not lock up the CPU.

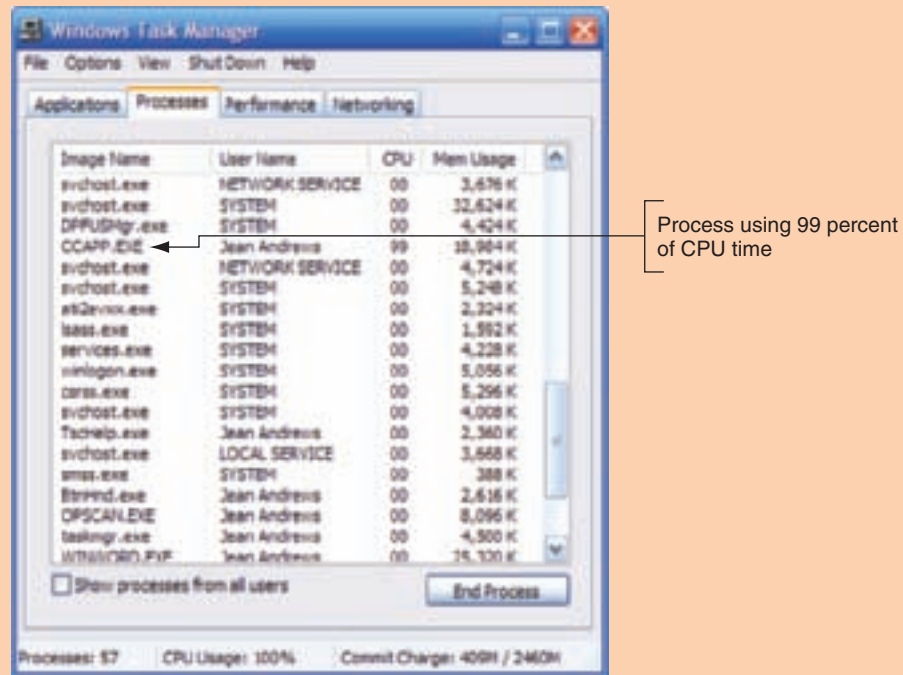


Figure 14-11 The Processes tab of Task Manager shows a process hogging CPU resources
Courtesy: Course Technology/Cengage Learning

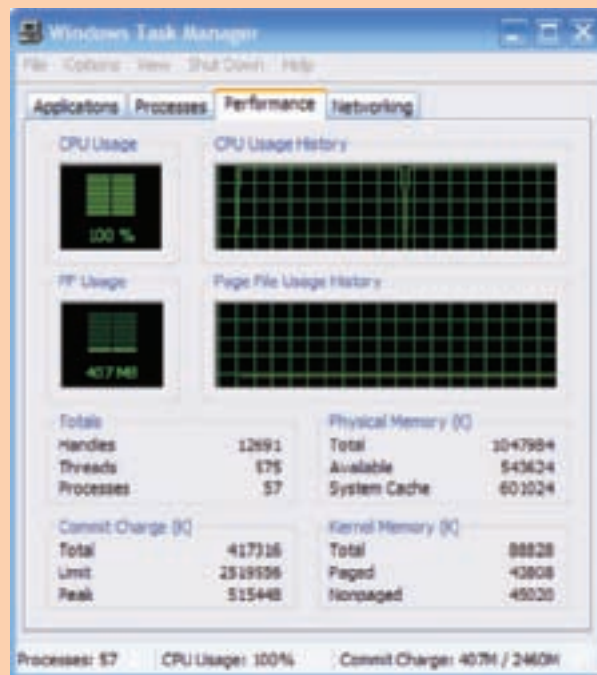


Figure 14-12 The Performance tab shows a heavily used CPU
Courtesy: Course Technology/Cengage Learning

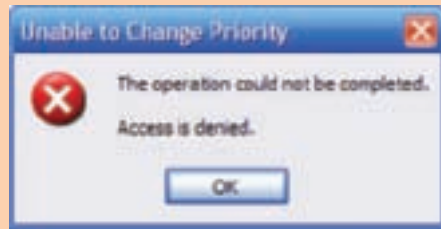
A+
220-701
3.2

Figure 14-13 The priority level of this process cannot be changed
Courtesy: Course Technology/Cengage Learning

Notes Lowering the CPU processing time allowed for an application is called throttling the process.

A+ Exam Tip Task Manager gives good information, but doesn't always give the full picture of running processes. One tool that gives better information than Task Manager is Process Explorer by Microsoft Technet (technet.microsoft.com). The utility is free, and you will learn to use it in Chapter 20.

SYSTEM CONFIGURATION UTILITY (MSCONFIG)

You can use the **System Configuration Utility (Msconfig.exe)**, which is commonly pronounced “M-S-config,” to find out what processes are launched at startup and to temporarily disable a process from loading. This utility is included with Windows Vista and Windows XP, but it is not included with Windows 2000.

MSconfig is a temporary fix to disable a program or service at startup, but it should not be considered a permanent fix. Once you've decided you want to make the change permanent, use other tools to permanently remove that process from Windows startup. Follow these steps to learn to use MSconfig:

1. To start MSconfig, enter **msconfig.exe** in the Vista Start Search box or the XP Run box and press **Enter**. For Vista, respond to the UAC box. The System Configuration box opens.
2. Click the **Services** tab to see a list of all services launched at startup (see Figure 14-14). Notice that this tab has a **Disable all** button. If you use that button, you'll disable all nonessential Windows services as well as third-party services such as virus scan programs. Use it only for the most difficult Windows problems, because you'll disable some services that you might really want, such as Windows Task Scheduler, Print Spooler, Automatic Updates, and the System Restore service.
3. To view only those services put there by third-party software, check **Hide all Microsoft services**. If you have antivirus software running in the background (and you should), you'll see that listed as well as any service launched at startup and put there by installed software. Uncheck all services that you don't want. If you don't recognize a service, try entering its name in a search string at www.google.com for information about the program. If the program is a service, you can permanently stop it by using the Services console, discussed next.
4. Click the **Startup** tab to see a list of programs that launch at startup (see Figure 14-15). To disable all nonessential startup tasks, click **Disable all**. Or you can check and

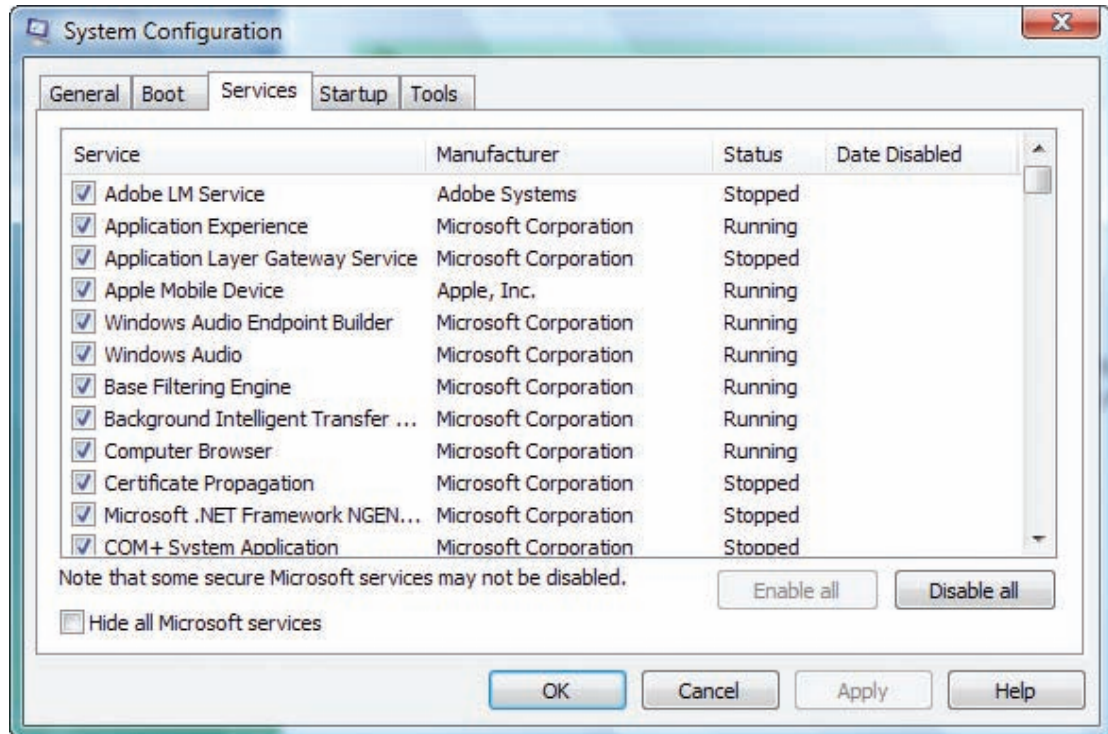


Figure 14-14 Use MSconfig to view and control services launched at startup
 Courtesy: Course Technology/Cengage Learning

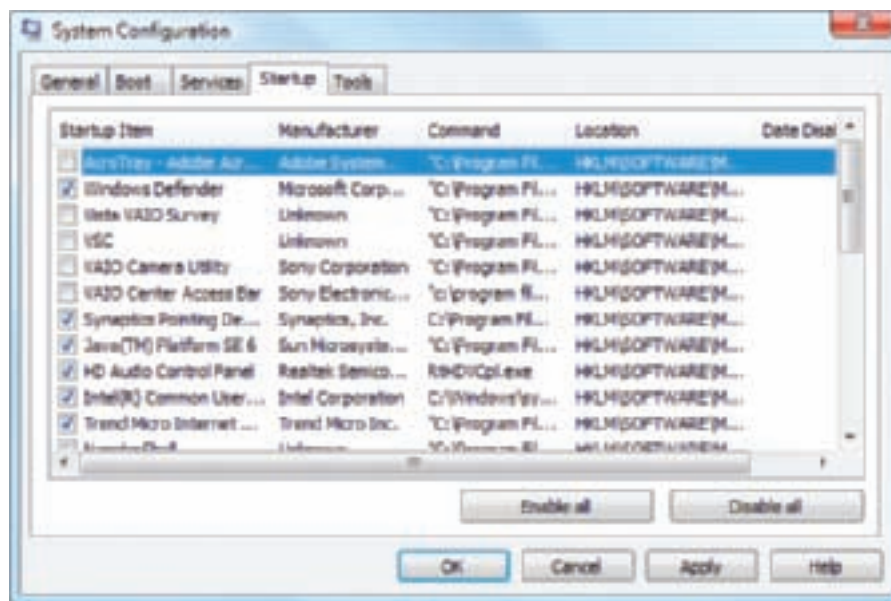


Figure 14-15 Select startup processes to enable or disable
 Courtesy: Course Technology/Cengage Learning

uncheck an individual startup program to enable or disable it. The Startup tab can be useful when trying to understand how a program is launched at startup because it offers the Location column. This column shows the registry key or startup folder where the startup entry is made. How to find and change registry keys is covered later in the chapter.

A+
220-701
3.2

5. Click **Apply** to apply your changes. Now click the **General** tab and you should see Selective startup selected, as shown in Figure 14-16. MSconfig is now set to control the startup process. Click **OK** to close the MSconfig box.

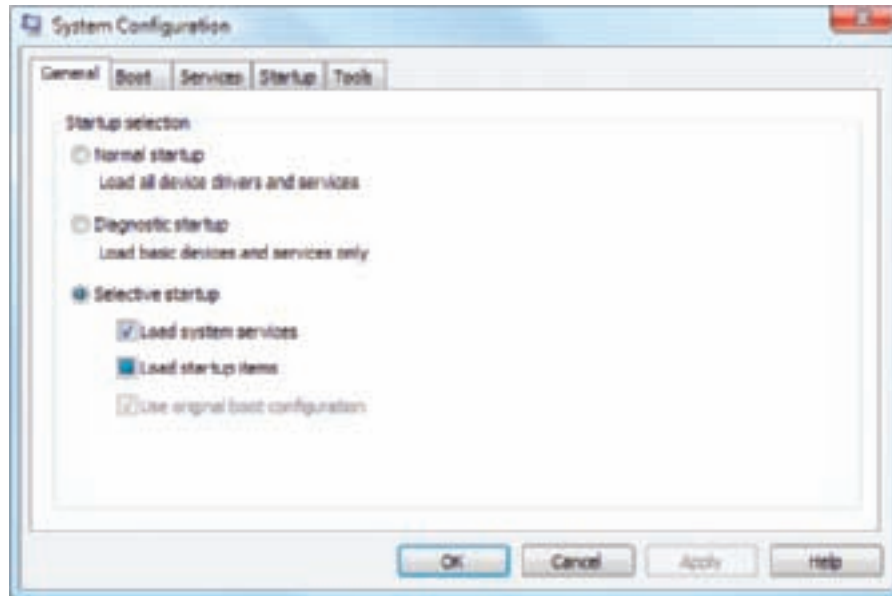


Figure 14-16 MSconfig is set to control the Windows startup programs
Courtesy: Course Technology/Cengage Learning

6. After you make a change in the MSconfig box, reboot so that you can see what happens. When Windows starts up, you'll see the bubble in Figure 14-17 that says Windows has blocked some startup programs. Remember, using MSconfig is recommended only as a temporary fix, and this bubble reminds us of that.

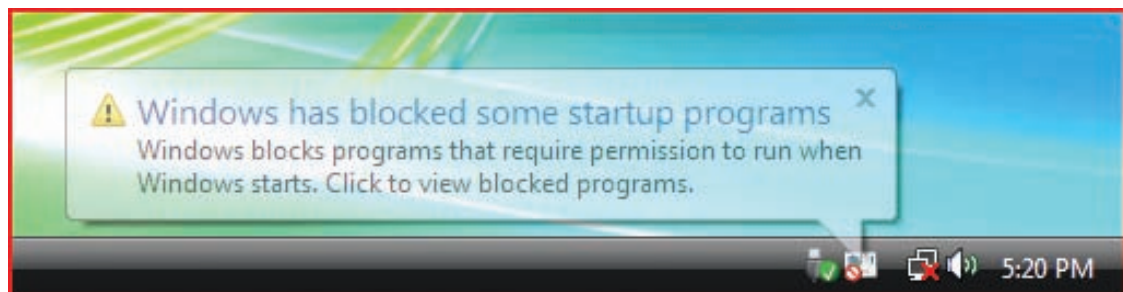


Figure 14-17 The System Configuration utility has blocked some startup programs
Courtesy: Course Technology/Cengage Learning

7. Watch for error messages during the boot that indicate you've created a problem with your changes. For instance, after the boot, you find out you can no longer use that nifty little utility that came with your digital camera. To fix the problem, you need to find out which service or program you stopped that you need for that utility. Go back to the MSconfig tool and enable that one service and reboot. MSconfig should only be used to temporarily disable a program. Use other tools, such as the Services console or startup folders, to permanently remove it from the

A+
220-701
3.2

startup process. Once the program is removed from the startup process, you will no longer need MSconfig and can return it to normal startup mode.

Recall from Chapter 13 that Software Explorer in Windows Vista can also be used to monitor startup programs and to enable and disable a startup program. Software Explorer is more convenient to use than MSconfig.

Notes MSconfig reports only what it is programmed to look for when listing startup programs and services. It looks only in certain registry keys and startup folders, and sometimes MSconfig does not report a startup process. Therefore, don't consider its list of startup processes to be complete.

SERVICES CONSOLE

The Services console is used to control the Windows and third-party services installed on a system. To launch the Services console, type **Services.msc** in the Vista Start Search box or the XP Run box and press **Enter**. For Vista, respond to the UAC box. If the **Extended** tab at the bottom of the window is not selected, click it (see Figure 14-18).

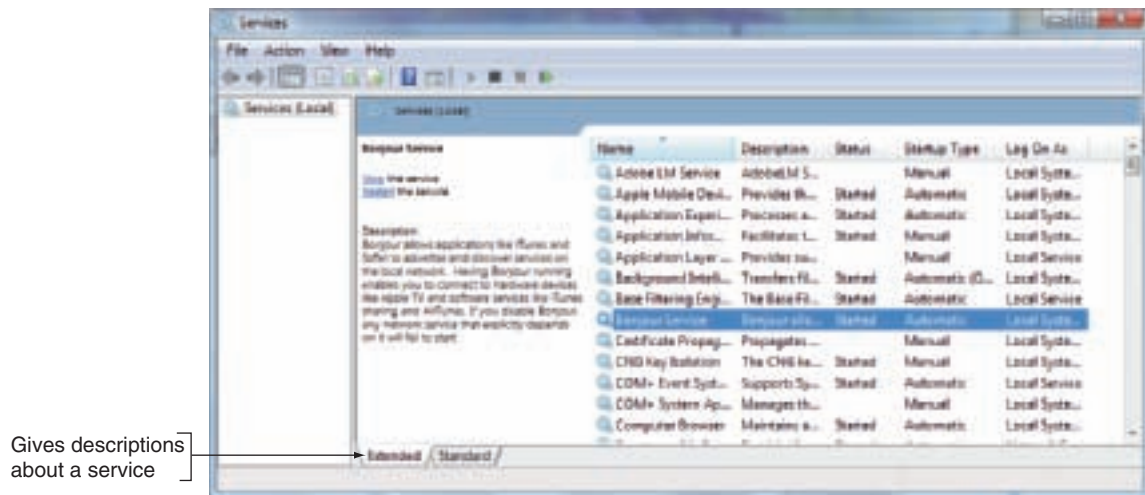


Figure 14-18 The Services window is used to manage Windows services
Courtesy: Course Technology/Cengage Learning

As you select each service, the area on the left describes the service. If the description is missing, most likely the service is a third-party service put there by an installed application. To get more information about a service or to stop or start a service, right-click its name and select **Properties** from the shortcut menu. In the Properties box (see Figure 14-19), the startup types for a service are:

- ▲ *Automatic (Delayed Start)*. Starts shortly after startup, after the user logs on, so as not to slow down the startup process
- ▲ *Automatic*. Starts when Windows loads
- ▲ *Manual*. Starts as needed
- ▲ *Disabled*. Cannot be started

A+
220-701
3.2

Notes If you suspect a Windows system service is causing a problem, you can use MSConfig to disable the service. If this works, then try replacing the service file with a fresh copy from the Windows setup CD or DVD.

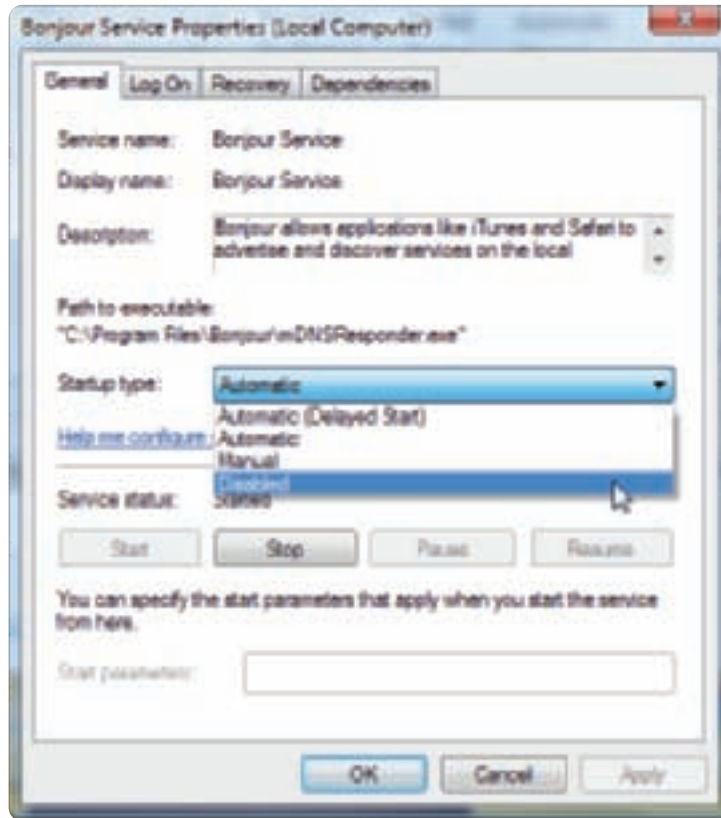


Figure 14-19 Use a service properties box to manage a service
Courtesy: Course Technology/Cengage Learning

When cleaning up a Windows system, one step is to disable or uninstall unwanted services. Research each third-party service whose Startup type is set to Automatic, and decide if you need to disable the service or uninstall the software responsible for the service. For most Windows services, you can use the Control Panel or other Windows utilities to control a particular service. For example, you can stop and start Automatic Updates from the XP System Properties box or uninstall software using the Vista Programs and Features window. Third-party services can often be stopped by using the utility that installed the service. You can access the utility from the Start menu. However, you can also use the Services console to disable a service. In the console, use its Properties box (see Figure 14-19). In the Startup type drop-down list, select **Disabled** and then click **Apply**.

COMPUTER MANAGEMENT

Computer Management (Compmgmt.msc) is a window that consolidates several Windows administrative tools that you can use to manage the local PC or other computers on the network. To use most of these tools, you must be logged on as an administrator, although you can view certain settings and configurations in Computer Management if you are logged on with lesser privileges.

As with most Windows tools, there are several ways to access Computer Management:

- ▲ Enter **compmgmt.msc** in the Vista Start Search box or the XP Run box and press **Enter**. For Vista, respond to the UAC box.
- ▲ Click **Start**, right-click **Computer (My Computer for XP)** and select **Manage** from the shortcut menu. For Vista, respond to the UAC box.
- ▲ In Control Panel, click **System and Maintenance** (for XP, click **Performance and Maintenance**), click **Administrative Tools**, and double-click **Computer Management**. For Vista, respond to the UAC box.

The Computer Management window opens (see Figure 14-20). Using this window, you can access Task Scheduler (Vista only), Event Viewer, Shared Folders, Reliability and Performance, Device Manager, Disk Management, Services console, Indexing Service, and manage user groups (covered in Chapter 20). You can also monitor problems with hardware, software, and security. Several tools available from the Computer Management window are covered in this chapter.

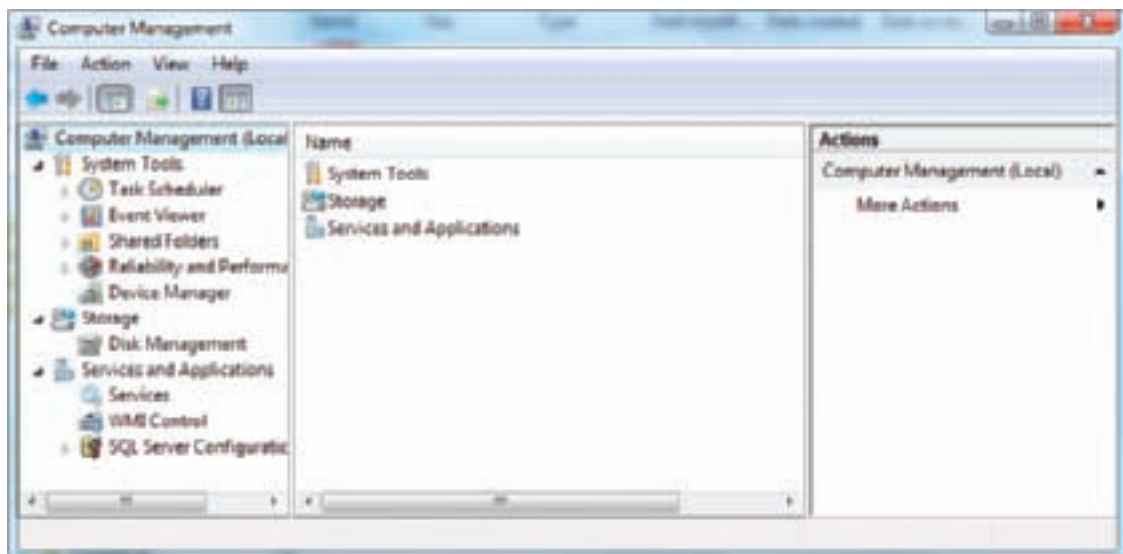


Figure 14-20 Windows Computer Management combines several administrative tools into a single easy-to-access window
Courtesy: Course Technology/Cengage Learning



Notes By default, the Administrative Tools group is found in Control Panel, but you can add the group to the All Programs menu. To do that, right-click the taskbar and select **Properties** from the shortcut menu. The Taskbar and Start Menu Properties box opens. Select the **Start Menu** tab and then click **Customize** (as shown on the left side of Figure 14-21). The Customize Start Menu box opens. Scroll down through the list, select **Display on the All Programs menu**, and click **OK**. Click **Apply** and **OK** to close the Taskbar and Start Menu Properties box. Now, to use the Administrative Tools group, click **Start, All Programs, and Administrative Tools**. (To add the tool to the All Programs menu in Windows XP, in the Customize Start Menu box, click the **Advanced** tab.)

A+
220-701
3.2

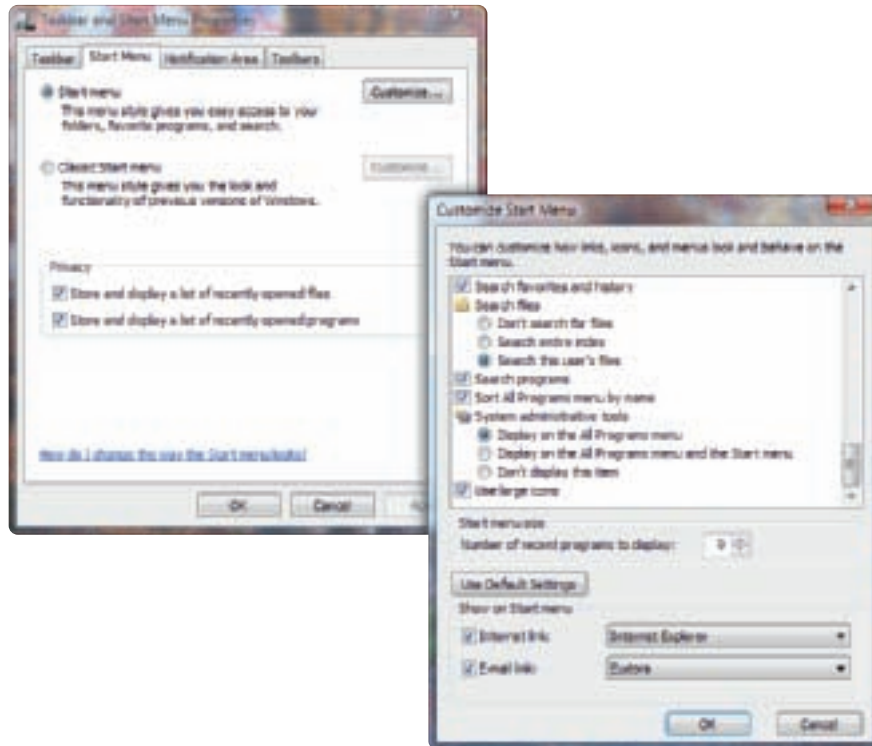


Figure 14-21 Use the Taskbar and Start Menu Properties window to change items on the Start menu
Courtesy: Course Technology/Cengage Learning

MICROSOFT MANAGEMENT CONSOLE (MMC)

Microsoft Management Console (MMC) (the program file is `mmc.exe`) is a Windows utility that can be used to build your own customized console windows. A **console** is a single window that contains one or more administrative tools such as Device Manager or Disk Management. In a console, these individual tools are called **snap-ins**. An example of a console is Computer Management, which has a filename of `Compmgmt.msc`. (Event Viewer, Device Manager, Disk Management, and Task Scheduler are examples of snap-ins that appear in that console.) A console is saved in a file with an `.msc` file extension, and a snap-in in a console can itself be a console. To use all the functions of MMC, you must be logged on with administrator privileges.

You can use MMC to create a console that contains some popular utility tools. Follow these steps for Windows to create a console:

1. Enter `mmc.exe` in the Vista Start Search box or the XP Run box and press **Enter**. For Vista, respond to the UAC box. An empty console window appears, as shown in Figure 14-22.
2. Click **File** on the menu bar and then click **Add/Remove Snap-in**. The Add or Remove Snap-ins box opens, as shown at the top of Figure 14-23.
3. Select a snap-in from the list on the left. Notice a description of the snap-in appears at the bottom of the window. The snap-ins that appear in this list depend on the edition of Vista you have installed and what other components are installed on the system. Click **Add** to add the snap-in to the console. (For Windows XP, in the Add/Remove Snap-In box, click **Add**. A list of snap-ins appears. Select one and click **Add**.)

A+
220-701
3.2

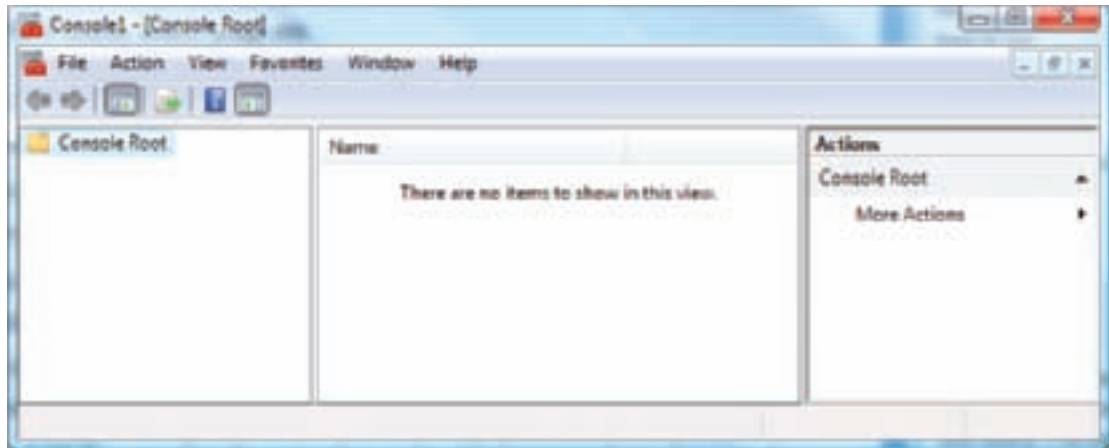


Figure 14-22 An empty console
Courtesy: Course Technology/Cengage Learning

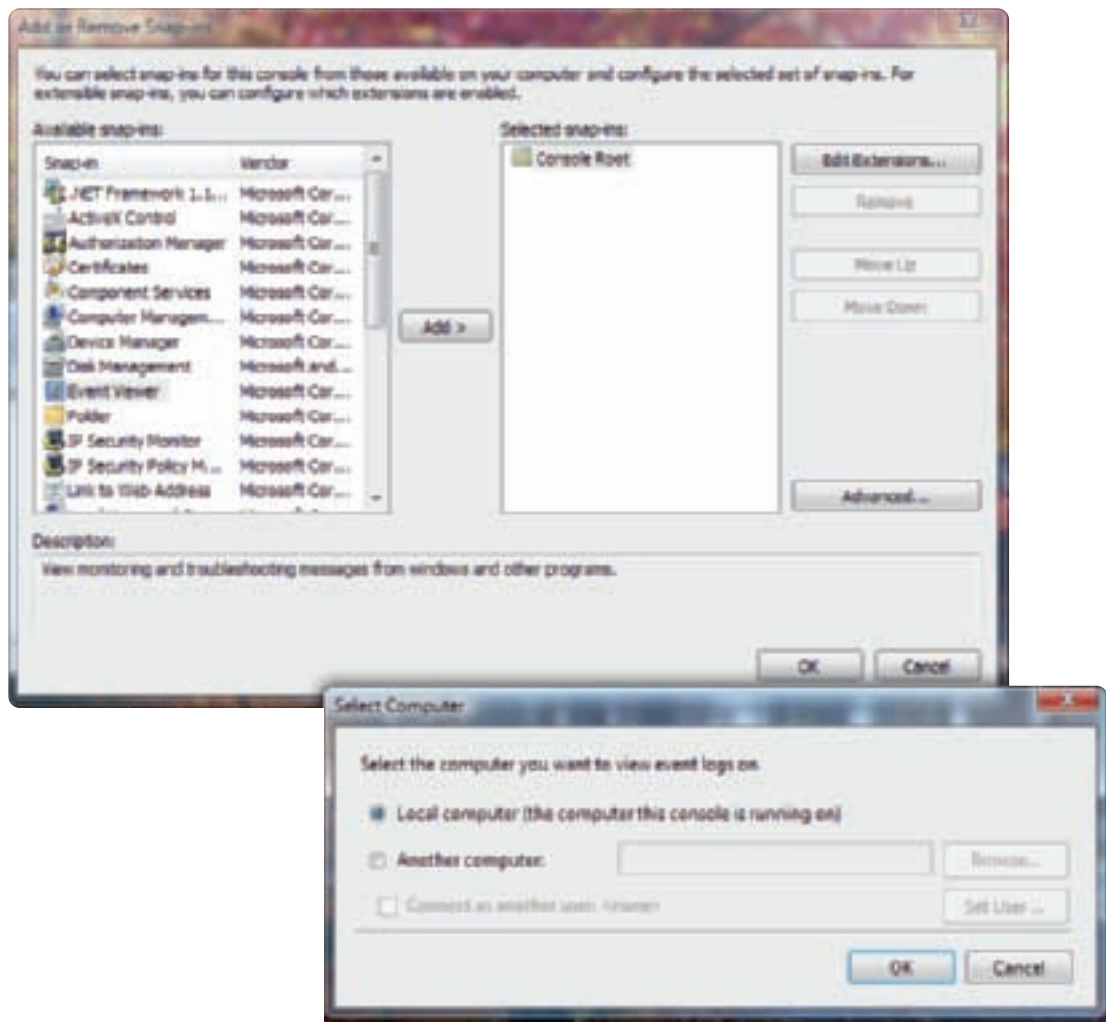


Figure 14-23 Add a snap-in to the new console
Courtesy: Course Technology/Cengage Learning

A+
220-701
3.2

4. If parameters for the snap-in need defining, a dialog box opens that allows you to set up these parameters. The dialog box offers different selections, depending on the snap-in being added. For example, when Event Viewer is selected, the Select Computer box appears, asking you to select the computer that Event Viewer will monitor (see the bottom of Figure 14-23). Select **Local computer (the computer this console is running on)** and click **OK**. (For XP, click **Finish**.) The snap-in now appears in the list of snap-ins for this console.
5. Repeat Steps 3 and 4 to add all the snap-ins that you want to the console. When you finish, click **OK** in the Add or Remove Snap-ins box shown in Figure 14-23.
6. The left side of Figure 14-24 shows a console with two snap-ins added. To save the console, click **File** on the menu bar and then click **Save As**. The Save As dialog box opens, as shown on the right side of the figure.

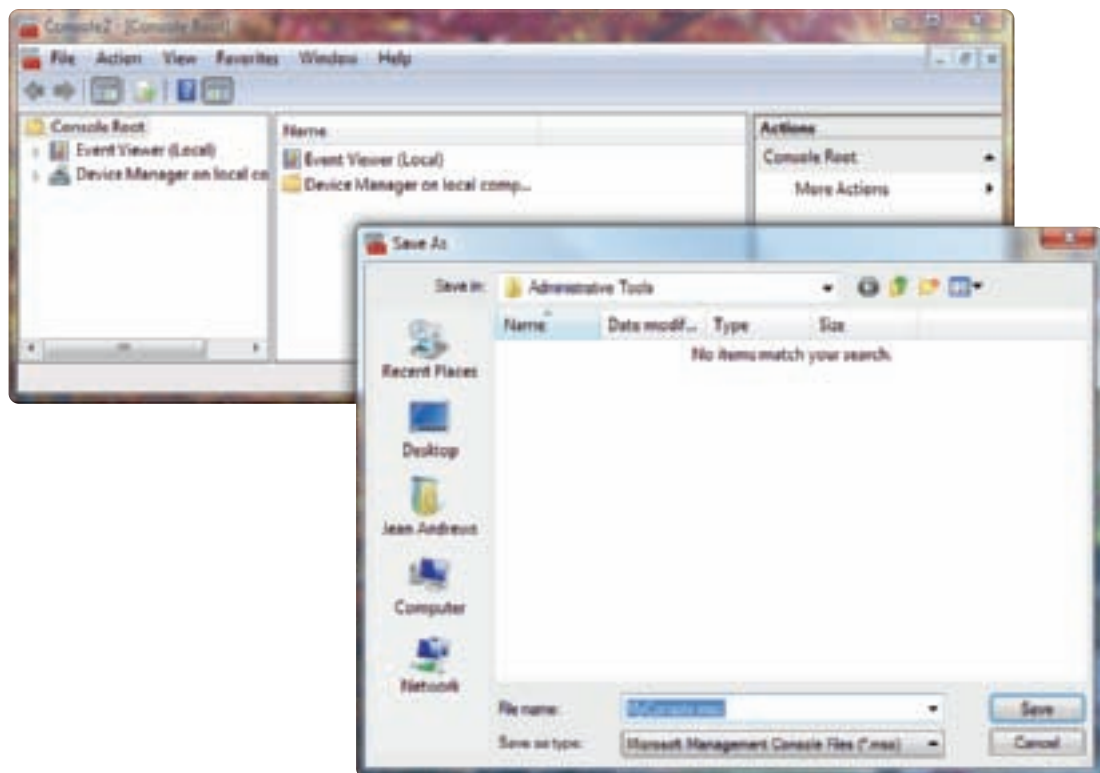



Figure 14-24 Saving a console with two snap-ins
Courtesy: Course Technology/Cengage Learning

7. The default location for the console file is `C:\Users\username\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools`. However, you can save the console to any location, such as the Windows desktop. However, if you save the file to its default location, the console will appear as an option under Administrative Tools on the Start menu. Select the location for the file, name the file, and click **Save**.
8. Close the console window.

 **Notes** After you create a console, you can copy the .msc file to any computer or place a shortcut to it on the desktop.

EVENT VIEWER

Event Viewer (Eventvwr.msc) is a Windows tool useful for troubleshooting problems with Windows, applications, and hardware. Of all these types of problems, it is most useful when troubleshooting problems with hardware. Event Viewer displays logs of significant events such as a hardware or network failure, OS error messages, a device or service that has failed to start, or General Protection Faults.

Note that Event Viewer is also a Computer Management console snap-in. You can open it by using the Computer Management window, by entering **Eventvwr.msc** in the Vista Start Search box or the XP Run box, using the Administrative Tools applet in Control Panel, or by clicking **Start, All Programs, Administrative Tools, Event Viewer**. (This last option assumes Administrative Tools has been added to the All Programs menu.) All of these methods open the window in Figure 14-25 (for Windows Vista after you respond to the UAC box) and the window in Figure 14-26 (for Windows XP).

Event Viewer manages logs of events. The logs that Event Viewer keeps partly depend on the edition of Windows you are using. For example, in Figure 14-26, the Media Center log is kept by Windows XP Media Center Edition. Event Viewer logs can be filtered and sorted in several ways. The different views of logs are listed in the left pane. You can click a triangle beside a view to see subcategories of logs within that view. Depending on the OS version and original equipment manufacturer (OEM) features, Event Viewer shows three or more views of logs. The three most important views of logs are described next:

- ▶ The *Application* log records events about applications and Windows utilities such as when an application was unable to open a file or when Windows created a restore point. The application events recorded depend on what the developer of the application set to trigger a log entry. All users can view this log. (In Vista, the Application log is a subcategory to the Windows Logs.)

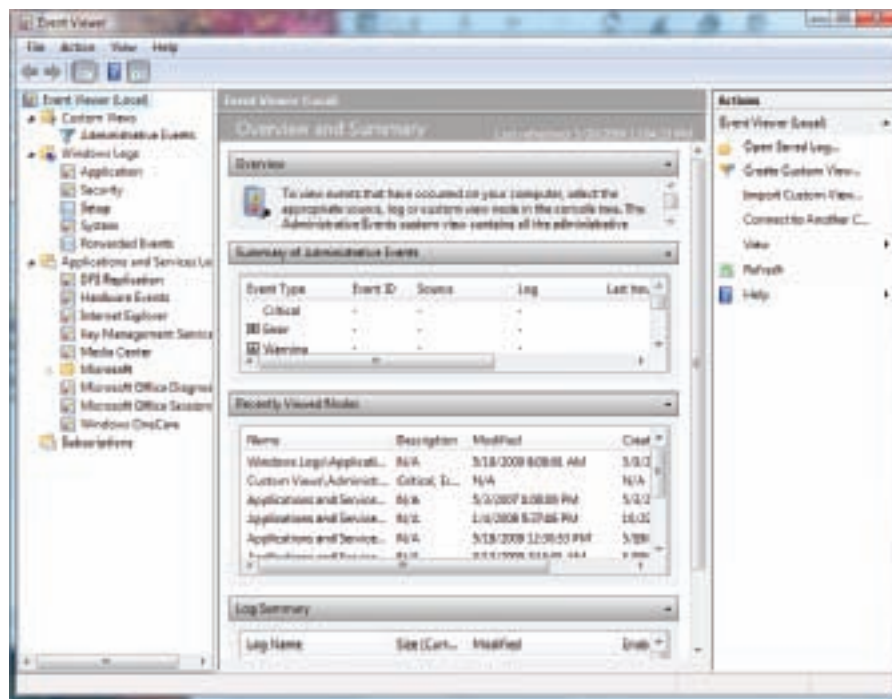


Figure 14-25 Use Event Viewer to see information about events with hardware, Windows, security, and applications
 Courtesy: Course Technology/Cengage Learning

A+
220-701
3.2

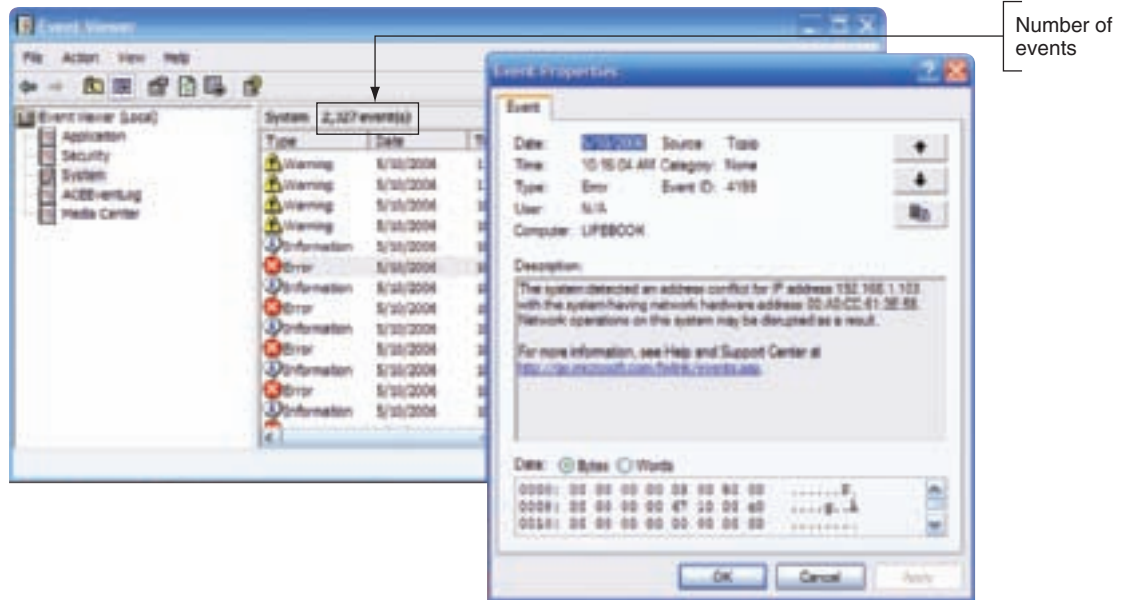


Figure 14-26 Event Viewer in Windows XP works about the same way as the Vista Event Viewer
Courtesy: Course Technology/Cengage Learning

- ▲ The *Security* log records events based on audit policies, which an administrator sets to monitor user activity such as successful or unsuccessful attempts to access a file or log on to the system. Only an administrator can view this log. (In Vista, the Security log is a subcategory to the Windows Logs.)
- ▲ The *System* log records events triggered by Windows components, such as a device driver failing to load during the boot process or a problem with hardware. Windows determines which events are recorded in this log. All users can access this log file. (In Vista, the System log is a subcategory to the Windows Logs.)

The following logs are new to Windows Vista:

- ▲ *Custom Views* allows you to select the type of event to appear in a view. Too much information is not a good thing, and the logs can get very long and give lots of unimportant information. By creating a Custom View, you can decide which types of events you want to see. (It is possible to create similar custom views in Windows XP, but only by using more advanced tools.)
- ▲ The *Setup* log records events about installing an application. The log is a subcategory to the Windows Logs.
- ▲ The *Forwarded Events* records events logged by remote computers. The log is a subcategory to the Windows Logs.
- ▲ The *Applications and Services Logs* are a group of several logs, each devoted to a particular Windows component or application.
- ▲ The *Subscriptions* log can be customized to collect certain events you require that are not normally collected by Event Viewer.

Unless you are trying to solve a problem with security, the most important event log for other problems is the System log. It records three types of events:

- ▲ *Information* events are recorded when a driver, service, or application functions successfully.

A+
220-701
3.2

- ▲ *Warning* events are recorded when something happens that may indicate a future problem but does not necessarily indicate that something is presently wrong with the system. For example, low disk space might trigger a warning event.
- ▲ *Error* events are recorded when something goes wrong with the system, such as a necessary component failing to load, data getting lost or becoming corrupted, or a system or application function ceasing to operate.

To view a log within Event Viewer, click the log that you want to view in the left pane. This generates a summary of events that appears on the right. For Windows Vista, select an event to see information about it in the lower pane of Event Viewer. Figure 14-27 shows an event in the System log about a conflict in IP addresses with another computer on the network, and gives a suggestion as to how to handle the problem. For Windows XP, double-click an event to see details about it (refer back to Figure 14-26).

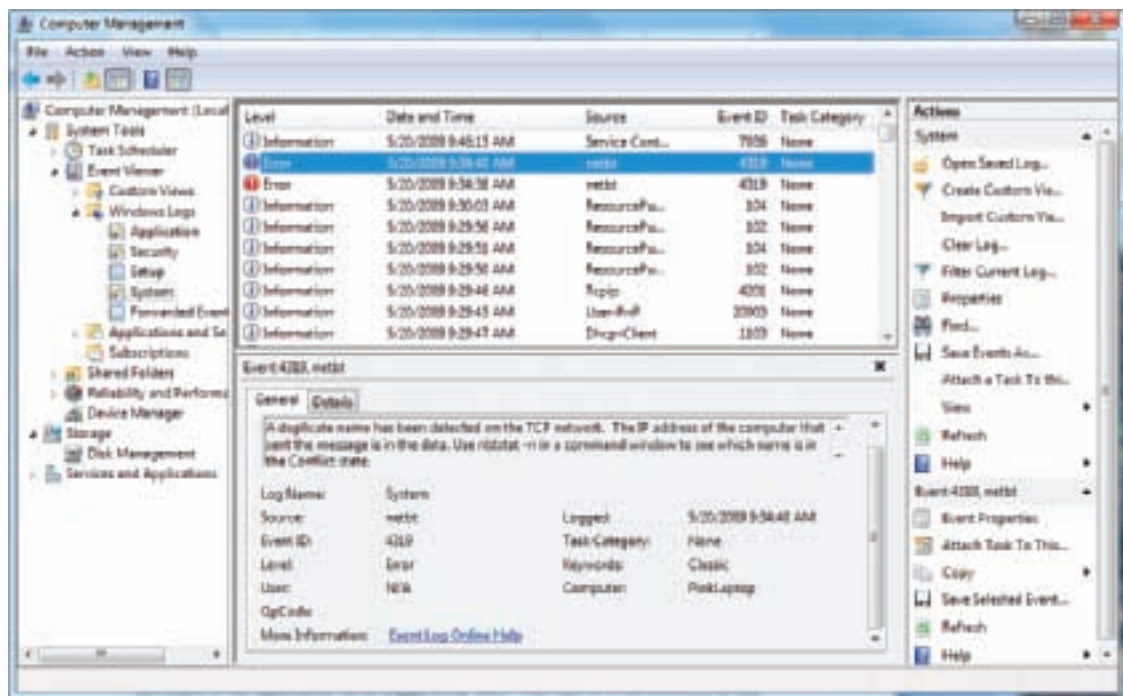


Figure 14-27 A conflicting IP address triggers an error event
Courtesy: Course Technology/Cengage Learning

When you are trying to solve a Windows, hardware, application, or security problem, Event Viewer can be your first source of information about the nature of the problem. You can find out if the problem is recent or has been going on for some time. Sometimes, you can even see what just occurred to the system when the problem started and see what other problems started at the same time. All this can be useful information to track the source of a problem.

To save time, you might want to view only certain events and not the entire list to make your search easier. Fortunately, you can filter events so only certain ones are listed. To do that, right-click a log in the left pane and select **Filter Current Log** from the shortcut menu.

A+
220-701
3.2

(For Windows XP, select **Properties** from the shortcut menu and then click the **Filter** tab.) The Filter Current Log box appears. See Figure 14-28 for Vista; the XP box looks and works about the same way.

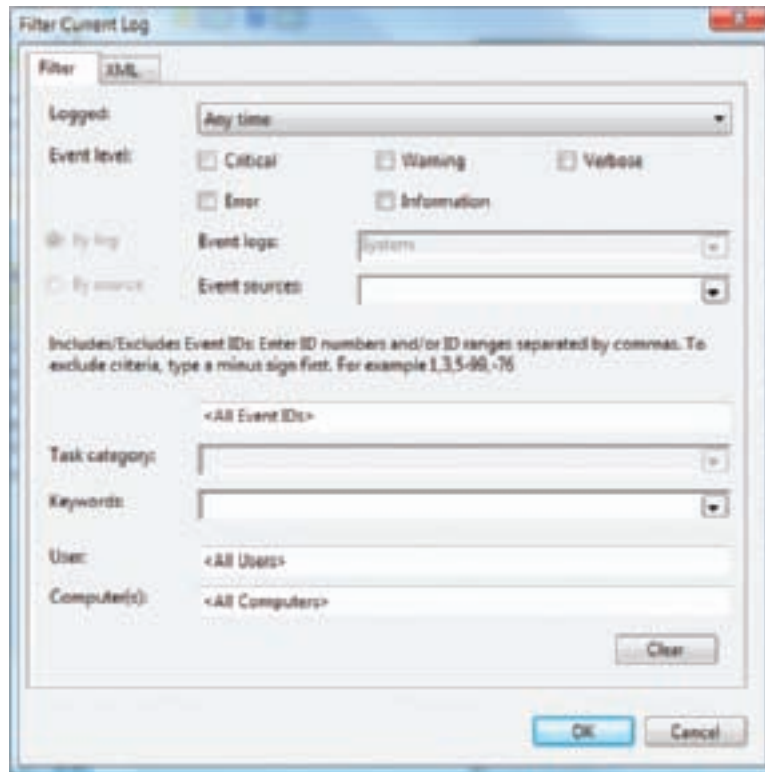


Figure 14-28 Criteria to filter events in Event Viewer
Courtesy: Course Technology/Cengage Learning

You can filter events on the time logged, the event level (critical, error, warning, information, or verbose), event source (for example, application, driver, service, or Windows component), event ID (identifies the type of event, such as a service has failed to load), keyword, user, and computer. To view the most significant events to troubleshoot a problem, check **Critical** and **Error** under the Event level. Critical events are those errors that Windows believes are affecting critical Windows processes.

Another way you can avoid a ballooning log file is to set a size limit, and specify what happens when the log reaches this limit. To control the size of a log file and see general information about the log, right-click the log, select **Properties** on the shortcut menu, and click the **General** tab (see Figure 14-29). You can set the maximum size of the log file. You can also set the log to overwrite events as needed, archive the log when full, and clear the log manually. To clear the log manually, click **Clear Log**. Before clearing the log, Event Viewer gives you a chance to save it.

Event Viewer can be useful when you suspect someone is attempting to illegally log onto a system and you want to view login attempts, or the network is giving intermittent problems. But Event Viewer is most useful in solving intermittent hardware problems. For example, on our network we have a file server and several people in the office update Microsoft Word documents stored on the server. For weeks, people complained about these Word documents

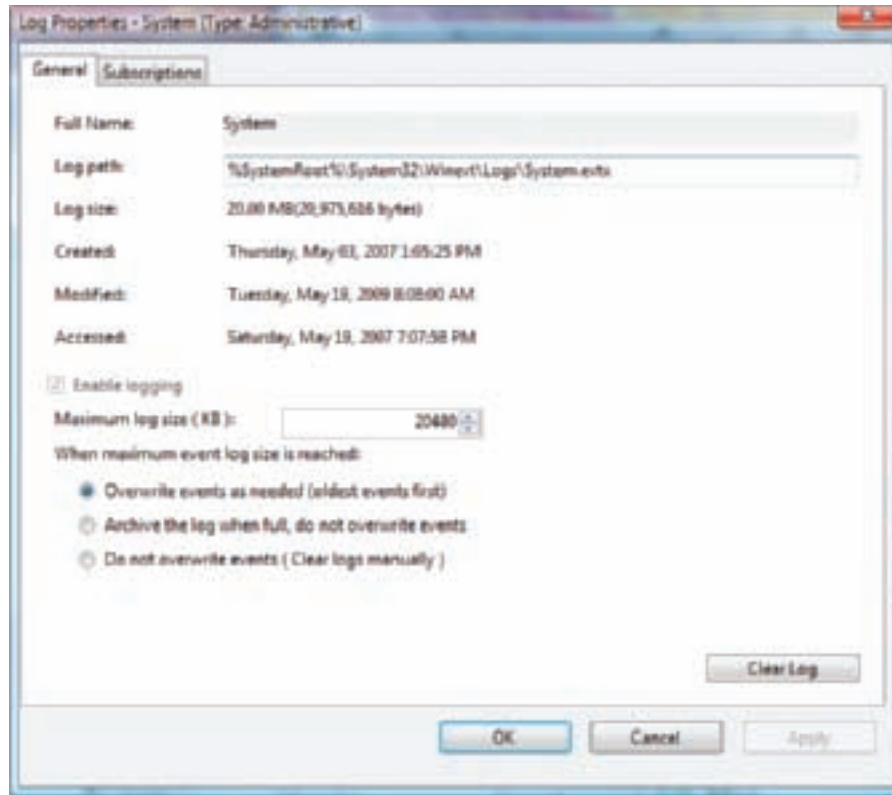


Figure 14-29 View information about a log, including maximum size of the log file in the Log Properties box
Courtesy: Course Technology/Cengage Learning

getting corrupted. We downloaded the latest patches for Windows and Microsoft Office and scanned for viruses, thinking that the problem might be with Windows or the application. Then we suspected a corrupted template file for building the Word documents. But nothing we did solved our problem of corrupted Word documents. Then one day someone thought to check Event Viewer on the file server. The Event Viewer had faithfully been recording errors when writing to the hard drive. What we had suspected to be a software problem was, in fact, a failing hard drive, which was full of bad sectors. We replaced the drive and the problem went away.

RELIABILITY AND PERFORMANCE MONITOR

Windows **Reliability and Performance Monitor** is another MMC snap-in (**Perfmon.msc**) that collects, records, and displays events. In Windows XP, this monitor is called the Performance Monitor or the System Monitor. These events, called Data Collector Sets, help you track the performance and reliability of Windows. To start the monitor, you can use the Administrative Tool applet in Control Panel, open the Computer Management Console, or enter **perfmon.msc** in the Vista Start Search box or the XP Run box. If Administrative Tools is added to the All Programs menu, you also can click **Start, All Programs, Administrative Tools, Reliability and Performance Monitor** (for XP, click **Performance**). The monitor window is shown in Figure 14-30 for Windows Vista after you respond to the UAC box. The XP Performance monitor is set up differently, but provides similar information, and is shown in Figure 14-31.

A+
220-701
3.2

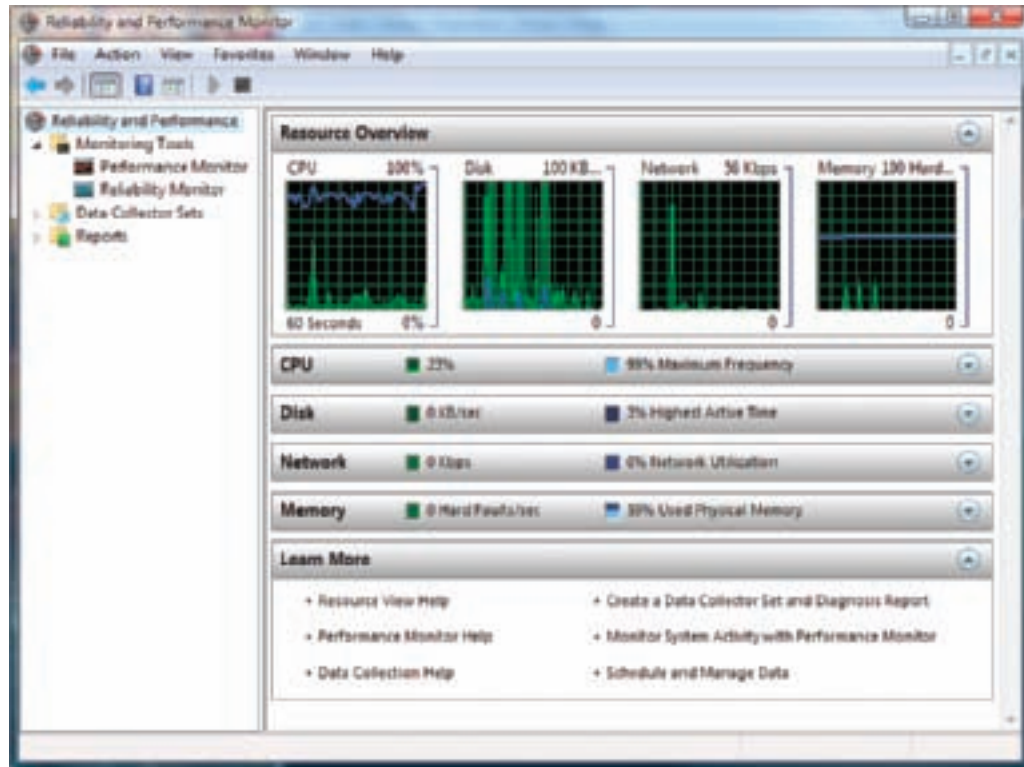


Figure 14-30 Reliability and Performance Monitor window shows the Resource Overview screen
Courtesy: Course Technology/Cengage Learning

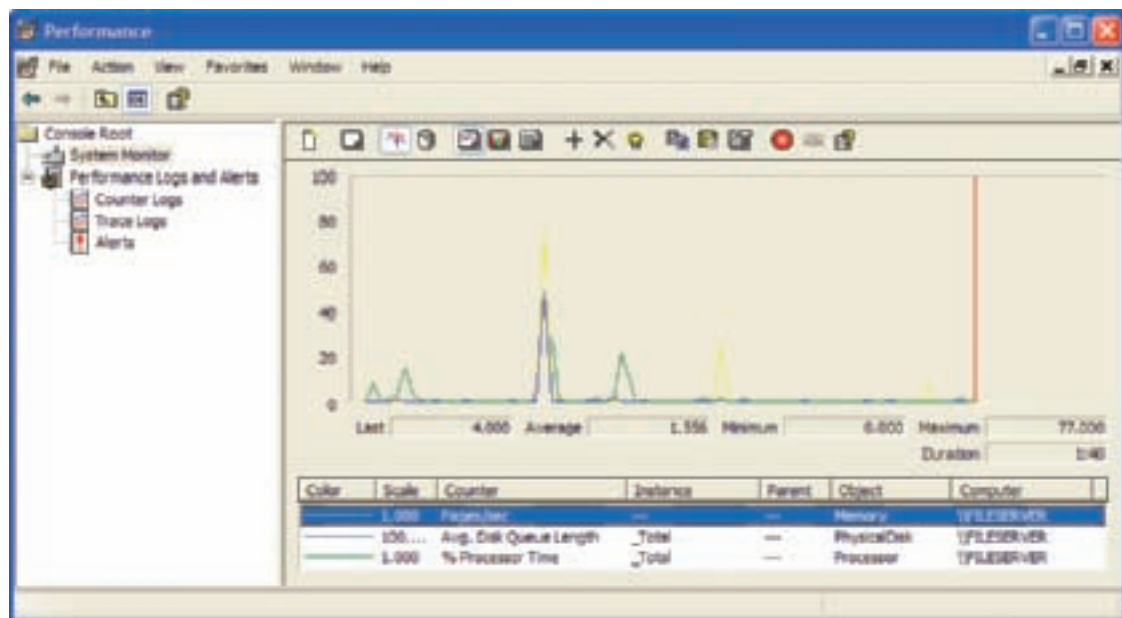


Figure 14-31 Windows XP Performance Monitor (also called the System Monitor)
Courtesy: Course Technology/Cengage Learning

The Reliability and Performance Monitor for Vista contains three monitoring tools:

- ▲ In the window shown in Figure 14-30, click **Performance Monitor** to see a real-time view of Windows performance counters (see Figure 14-32). You can add your own performance counters to this view by clicking the green plus sign, called the Add button, at the top of the Performance Monitor pane.

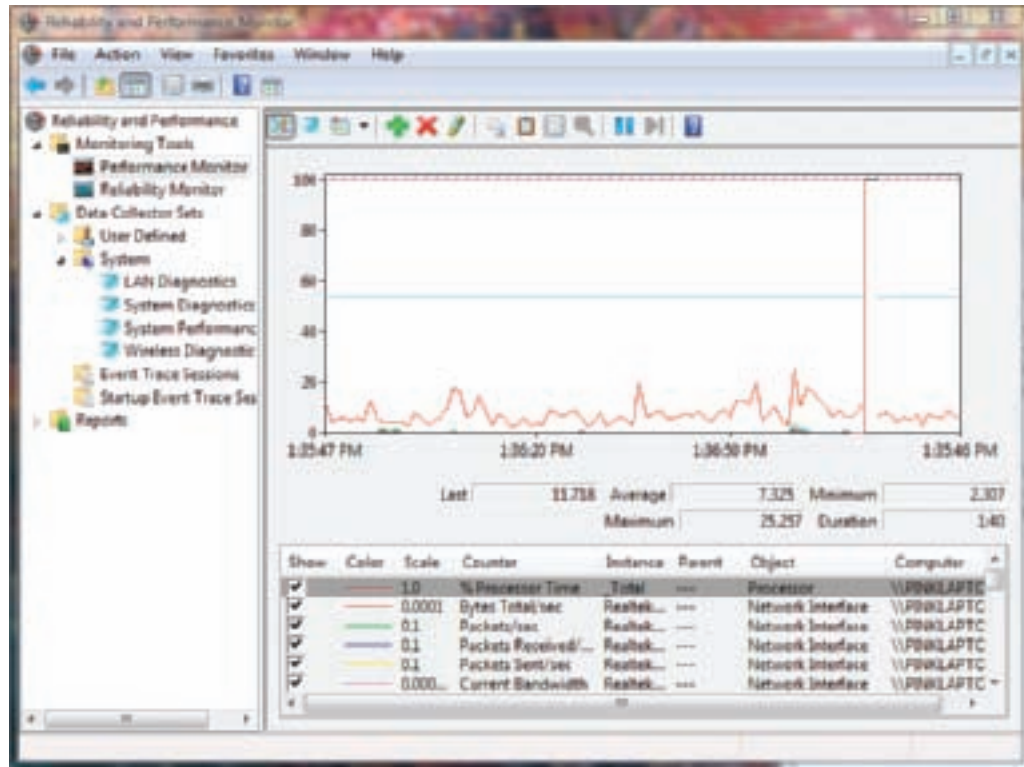


Figure 14-32 Performance monitor view shows real-time tracking of Windows performance counters
Courtesy: Course Technology/Cengage Learning

- ▲ Click **Reliability Monitor** to see a view of historical data that shows how stable the Windows system is. To get detailed information about a problem, click a day that shows an error and then click the plus sign beside the error's category. For example, in Figure 14-33, there was a Windows failure on May 1, 2009. When you click that date and then click the plus sign beside Windows Failures in the lower part of the pane, you can see what happened to Windows that day.
- ▲ The **Data Collector Sets** utility can be used to collect your own data about the system. Click **Data Collector Sets** and drill down to a subcategory that appears in the right pane (see Figure 14-34). Right-click a category and select **Start** from the shortcut menu shown in the figure. Wait while data is collected and then fills the middle pane. In our example, we're using System Diagnostics.

To view the system diagnostics data as a report, right-click **System Diagnostics** and select **Latest Report** from the shortcut menu. The report for one system is shown in Figure 14-35, which reports the system is experiencing excessive paging and needs more memory. (In this situation, note that the Reliability and Performance Monitor was started in the Computer Management console.)

THE REGISTRY EDITOR

Many actions, such as installing application software or hardware, can result in changes to the registry. These changes can create new keys, add new values to existing keys, and change existing values. For a few difficult problems, you might need to edit or remove a registry key. This part of the chapter looks at how the registry is organized, which keys might hold entries causing problems, and how to back up and edit the registry using the **Registry Editor** (*regedit.exe*). Let's first look at how the registry is organized, and then you'll learn how to back up and edit the registry.

A+
220-701
3.2

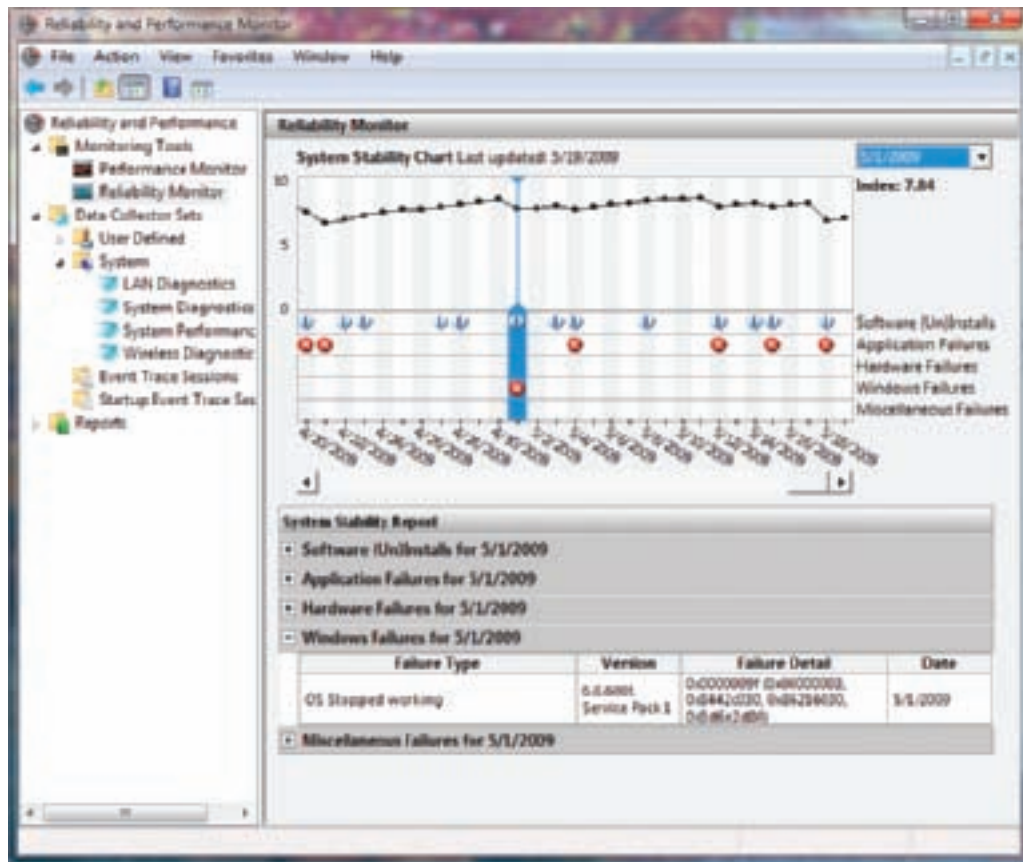


Figure 14-33 Reliability Monitor shows a history of the system that can help identify problems with the stability of Windows
Courtesy: Course Technology/Cengage Learning

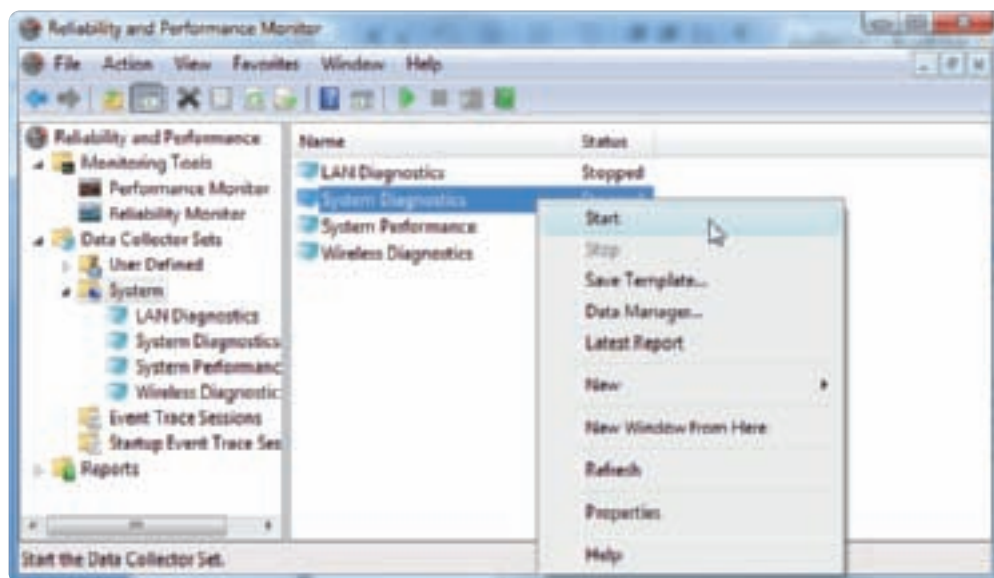


Figure 14-34 Collect data from a Data Collector Set to analyze
Courtesy: Course Technology/Cengage Learning

A+
220-701
3.2

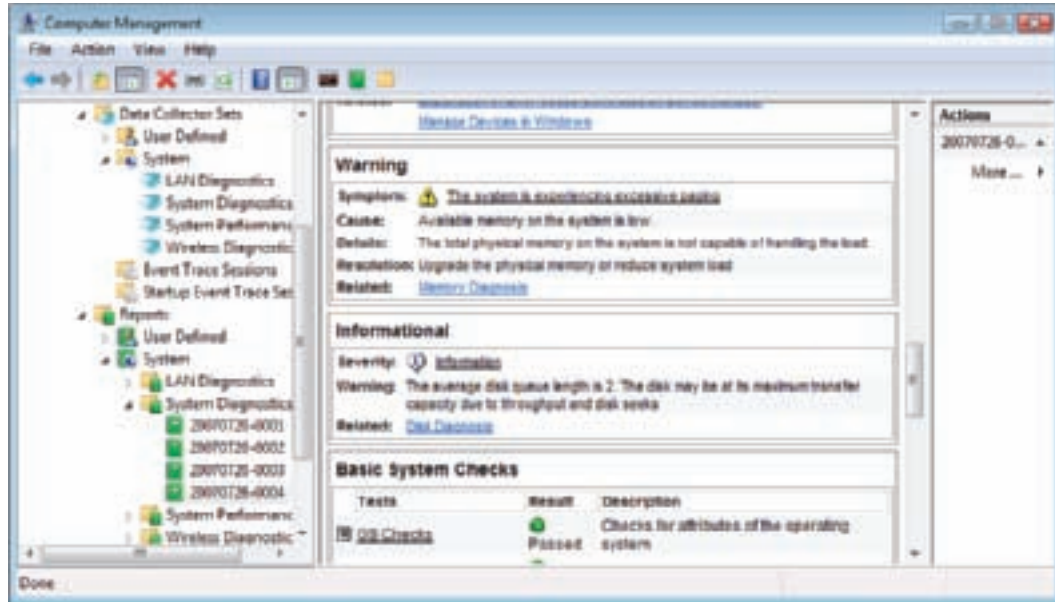


Figure 14-35 Reported results of collecting data about System Diagnostics
Courtesy: Course Technology/Cengage Learning

HOW THE REGISTRY IS ORGANIZED

The most important Windows component that holds information for Windows is the registry. The **registry** is a database designed with a treelike structure (called a hierarchical database) that contains configuration information for Windows, users, software applications, and installed hardware devices. During startup, Windows builds the registry in memory and keeps it there until Windows shuts down. During startup, after the registry is built, Windows reads from it to obtain information to complete the startup process. After Windows is loaded, it continually reads from many of the subkeys in the registry.

Windows builds the registry from the current hardware configuration and from information it takes from these files:

- ▲ Five files stored in the C:\Windows\System32\config folder; these files are called hives, and they are named the SAM (Security Accounts Manager), Security, Software, System, and Default hives. (Each hive is backed up with a log file and a backup file, which are also stored in the C:\Windows\System32\config folder.)
- ▲ For Windows Vista, the C:\Users\username\Ntuser.dat file, which holds the preferences and settings of the currently logged on user.
- ▲ Windows XP uses information about the current user stored in two files:
 - C:\Documents and Settings\username\Ntuser.dat
 - C:\Documents and Settings\username\Local Settings\Application Data\Microsoft\Windows\Usrclass.dat

After the registry is built in memory, it is organized into five treelike structures (see Figure 14-36). Each of the five segments is called a key. Each key can have subkeys, and subkeys can have more subkeys and can be assigned one or more values. The way data is organized in the hive files is different from the way it is organized in registry keys. Figure 14-37 shows the relationship between registry keys and hives.

A+
220-701
3.2

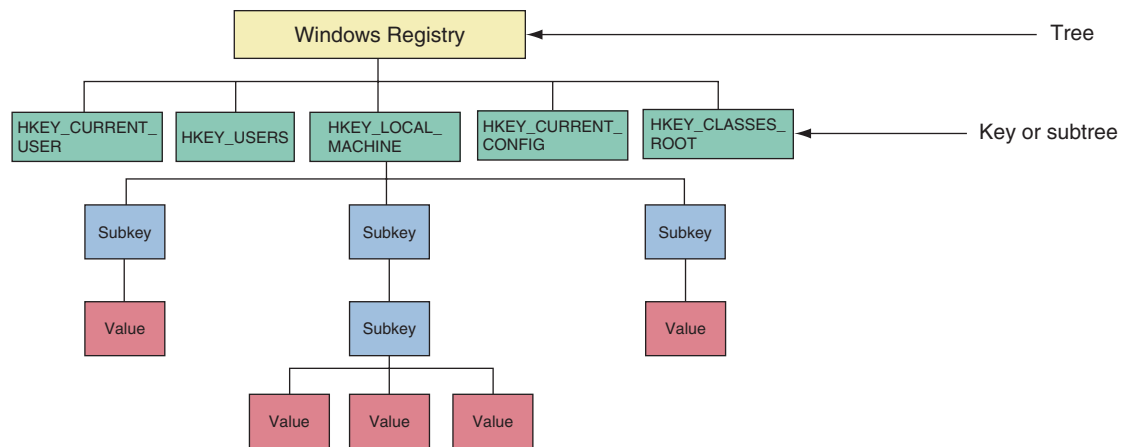


Figure 14-36 The Windows registry is logically organized in an upside-down tree structure of keys, subkeys, and values
Courtesy: Course Technology/Cengage Learning

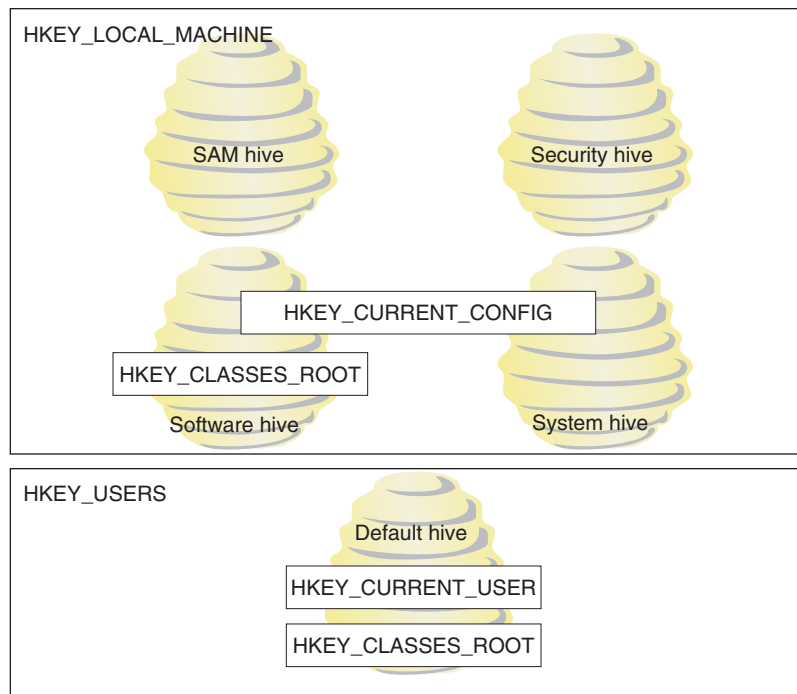


Figure 14-37 The relationship between registry subtrees (keys) and hives
Courtesy: Course Technology/Cengage Learning

Here are the five keys, including where they get their data and their purposes:

- ▶ **HKEY_LOCAL_MACHINE (HKLM)** is the most important key and contains hardware, software, and security data. The data is taken from four hives: the SAM hive, the Security hive, the Software hive, and the System hive. In addition, the HARDWARE subkey of HKLM is built when the registry is first loaded, based on data collected about the current hardware configuration.
- ▶ **HKEY_CURRENT_CONFIG (HKCC)** contains Plug and Play information about the hardware configuration that is used by the computer at startup. Information that identifies each hardware device installed on a PC is kept in this area. Some of the data

is gathered from the current hardware configuration when the registry is first loaded into memory. Other data is taken from the HKLM key, which got its data primarily from the System hive.

- ▲ **HKEY_CLASSES_ROOT (HKCR)** stores information that determines which application is opened when the user double-clicks a file. This process relies on the file's extension to determine which program to load. For example, this registry key might hold the information to cause Microsoft Word to open when a user double-clicks a file with a .doc file extension. Data for this key is gathered from HKLM key and the HKCU key.
- ▲ **HKEY_USERS (HKU)** contains data about all users and is taken from the Default hive.
- ▲ **HKEY_CURRENT_USER (HKCU)** contains data about the current user. The key is built when a user logs on using data kept in the HKEY_USERS key and data kept in the Ntuser.dat file of the current user.



Notes Device Manager reads data from the HKLM\HARDWARE key to build the information it displays about hardware configurations. You can consider Device Manager to be an easy-to-view presentation of this HARDWARE key data.

BEFORE YOU EDIT THE REGISTRY, BACK IT UP!

As you investigate startup problems and see a registry entry that needs changing, remember that it is important to use caution when editing the registry. If possible, make the change from the Windows tool that is responsible for the key—for example, by using the Vista Programs and Features window in Control Panel. If that doesn't work and you must edit the registry, always back up the registry before attempting to edit it. Changes made to the registry are implemented immediately. *There is no undo feature in the Registry Editor, and no opportunity to change your mind once the edit is made.*

Here are the ways to back up the registry:

- ▲ **Use System Protection to create a restore point.** A restore point keeps information about the registry. You can restore the system to a restore point to undo registry changes, as long as the registry is basically intact and not too corrupted. Also know that, if System Protection is turned on, Windows Vista automatically makes a daily backup of the registry hive files to the C:\Windows\System32\Config\RegBack folder.
- ▲ **Back up a single registry key just before you edit the key.** This method, called exporting a key, should always be used before you edit the registry. How to export a key is coming up in this chapter.
- ▲ **Make an extra copy of the C:\Windows\System32\config folder.** This is what I call the old-fashioned shotgun approach to backing up the registry. This backup will help if the registry gets totally trashed. You can boot from the Windows setup CD or DVD and use the Vista Recovery Environment or the XP Recovery Console to restore the folder from your extra copy. This method is drastic and not recommended except in severe cases. But, still, just to be on the safe side, I make an extra copy of this folder just before I start any serious digging into the registry.
- ▲ **For Windows XP, back up the system state.** Use Ntbackup in Windows XP or 2000 to back up the system state, which also makes an extra copy of the registry hives. Windows XP stores the backup of the registry hives in the C:\Windows\repair folder. Windows 2000 stores the backup in the C:\Windows\repair\RegBack folder.

A+
220-701
3.2

In some situations, such as when you're going to make some drastic changes to the registry, you'll want to play it safe and use more than one backup method. Extra registry backups are always a good thing! You learned how to create a restore point and back up the system state in Chapter 13. Now let's look at how to back up an individual key in the registry, and then you'll learn how to edit the registry.

Notes Although you can edit the registry while in Safe Mode, you cannot create a restore point in Safe Mode.

Backing Up and Restoring Individual Keys in the Registry

A less time-consuming method of backing up the registry is to back up a particular key that you plan to edit. However, know that if the registry gets corrupted, having a backup of only a particular key most likely will not help you much when trying a recovery. Also, although you could use this technique to back up the entire registry or an entire tree within the registry, it is not recommended.

To back up a key along with its subkeys in the registry, follow these steps:

1. Open the Registry Editor. To do that, click **Start** and type **regedit** in the Start Search dialog box, press **Enter**, and respond to the UAC box. Figure 14-38 shows the Registry Editor with the five main keys and several subkeys listed. Click the triangles on the left to see subkeys. When you select a subkey, such as **KeyboardClass** in the figure, the names of the values in that subkey are displayed in the right pane along with the data assigned to each value.

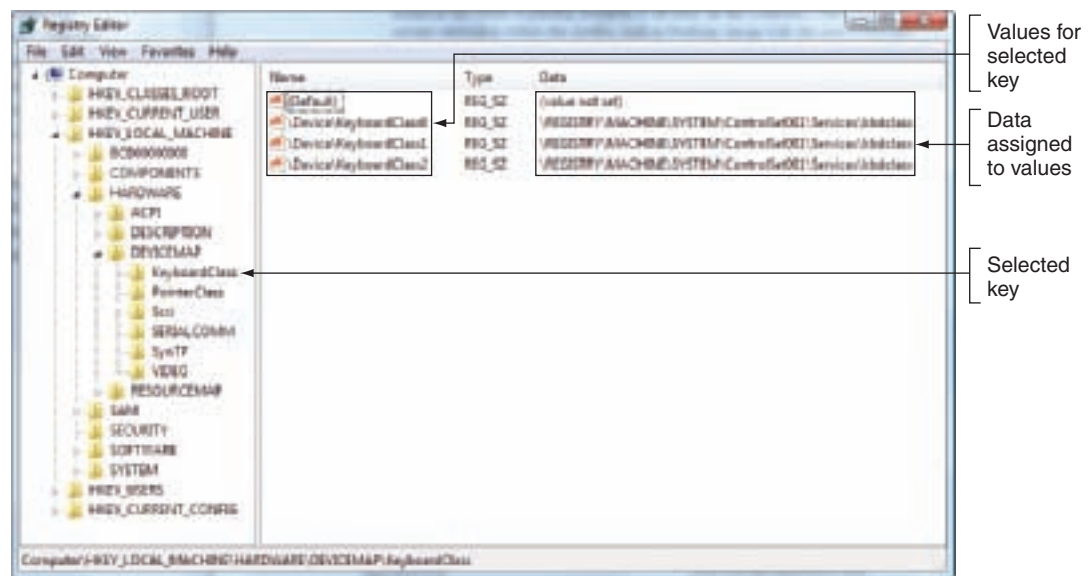


Figure 14-38 The Registry Editor showing the five main keys, subkeys, values, and data
Courtesy: Course Technology/Cengage Learning

2. Suppose we want to back up the registry key that contains a list of installed software, which is `HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall`. (HKLM stands for `HKEY_LOCAL_MACHINE`.) First click the appropriate triangles to navigate to the key. Next, right-click the key and select **Export** on the shortcut menu, as shown in Figure 14-39. The Export Registry File dialog box appears.

A+
220-701
3.2

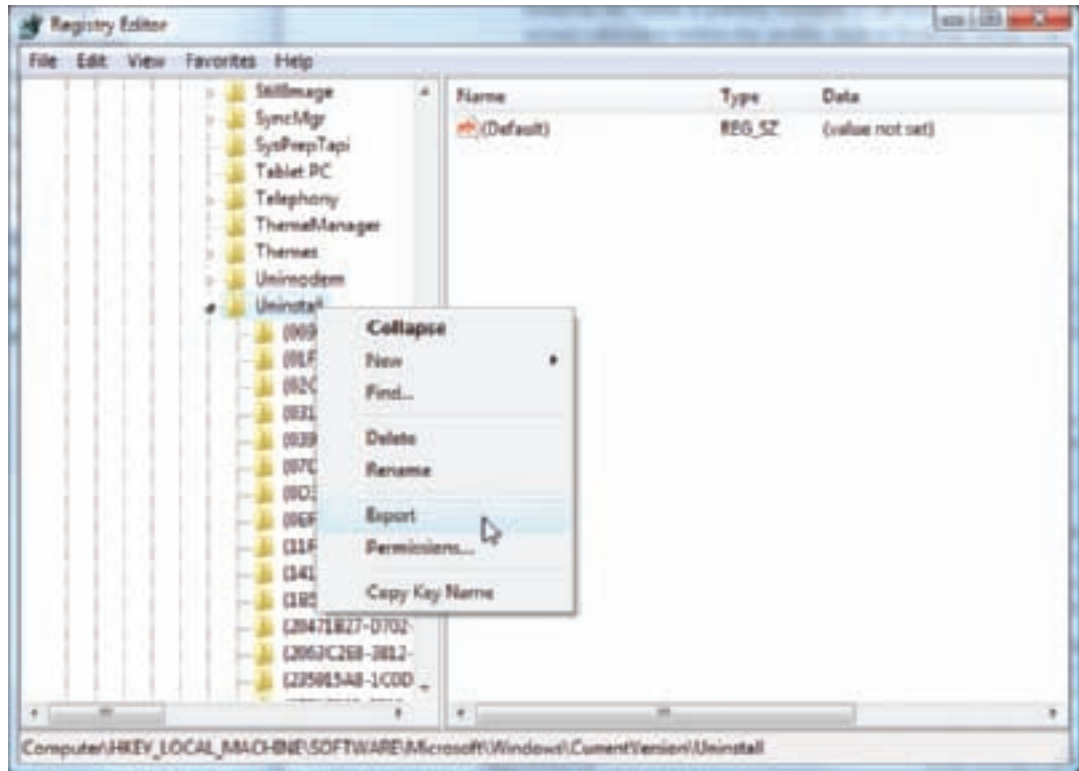


Figure 14-39 Using the Windows Registry Editor, you can back up a key and its subkeys with the Export command
Courtesy: Course Technology/Cengage Learning

3. Select the location to save the export file and name the file. A convenient place to store an export file while you edit the registry is the desktop. Click **Save** when done. The file saved will have a .reg file extension.
4. You can now edit the key. Later, if you need to undo your changes, exit the Registry Editor and double-click the saved export file. The key and its subkeys saved in the export file will be restored. After you're done with an export file, delete it.

Editing the Registry

When you make a change in Control Panel, Device Manager, or many other places in Windows, the registry is modified automatically. This is the only way most users will ever change the registry. However, on rare occasions, you might need to edit the registry manually.

Before you edit the registry, you should use one or more of the four backup methods just discussed so that you can restore it if something goes wrong. To edit the registry, open the Registry Editor (**regedit.exe**), and locate and select the key in the left pane of the Registry Editor, which will display the values stored in this key in the right pane. To edit, rename, or delete a value, right-click it and select the appropriate option from the shortcut menu. For example, in Figure 14-40, I'm ready to delete the value **NapsterShell** and its data. Changes are immediately applied to the registry and there is no undo feature. (However, Windows or applications might need to read the changed value before it affects their operations.) Notice in Figure 14-40 that the selected key is displayed in the status bar at the bottom of the editor window. If the status bar is missing, click **View** on the menu bar and make sure **Status Bar** is checked. To search the registry for keys, values, and data, click **Edit** on the menu bar and then click **Find**.

A+
220-701
3.2

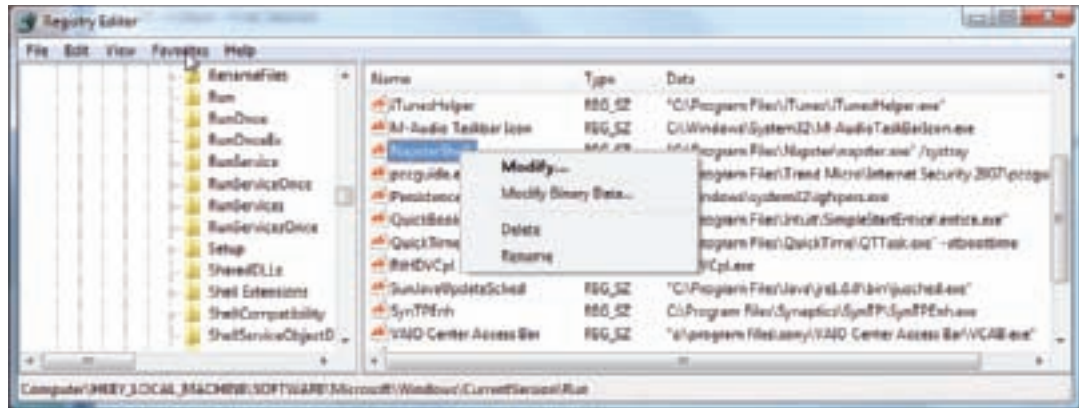


Figure 14-40 Right-click a value to modify, delete, or rename it
Courtesy: Course Technology/Cengage Learning

Caution Changes made to the registry take effect immediately. Therefore, take extra care when editing the registry. If you make a mistake and don't know how to correct a problem you create, then double-click the exported key to recover. When you double-click an exported key, the registry is updated with the values stored in this key.

A+ Exam Tip Content on the A+ 220-701 Essentials exam ends here and content on the A+ 220-702 Practical Application exam begins.

IMPROVING WINDOWS PERFORMANCE

A+
220-702
2.3
2.4

Sluggish Windows systems are so frustrating, and as a PC support technician, you need to know how to configure the Windows environment for optimum performance using the tools that were introduced in the first part of this chapter and in the last chapter.

In this part of the chapter, you'll learn step-by-step procedures to search for problems affecting performance and how to clean up the Windows startup process that goes beyond the routine maintenance tasks you learned about in Chapter 13. We're assuming you can start Windows with no errors. If you are having trouble loading Windows, it's best to address the error first rather than to use the tools described here to improve performance. How to handle errors that keep Windows from starting is covered in Chapters 15 and 16.

Now let's look at 11 steps you can take to improve Windows performance. After that, you'll learn how to manually remove software and how to use a monitor to alert you of changes that might affect performance.

STEP 1: PERFORM ROUTINE MAINTENANCE

It might seem pretty mundane, but the first things you need to do to improve performance are the obvious routine maintenance tasks that you learned in Chapter 13. These tasks are summarized here:

- ▶ *Verify critical Windows settings.* Make sure Windows updates are current and service packs are installed. Verify that antivirus software is updated and set to routinely scan for viruses. If a recent scan has not been performed or you suspect a virus is present,

download the latest updates to the antivirus software and scan the system. Make sure Windows Firewall is turned on. How to use antivirus software and Windows Firewall is covered in later chapters.

- ▲ *Clean up the hard drive.* Make sure at least 15 percent of drive C is free.
- ▲ *Defrag the hard drive.* Vista automatically does that weekly, but XP does not. A seriously fragmented hard drive can significantly affect performance.
- ▲ *Check the hard drive for errors.* Run Chkdsk to check the hard drive for errors and recover data.
- ▲ *Disable or remove unwanted startup programs.* For Vista, use Software Explorer to view and disable startup programs. For XP, check the startup folders for programs that you can remove from these folders to speed up the startup process. If you find programs that are no longer needed, use the Vista Programs and Features window or the XP Add or Remove Programs window to uninstall them.
- ▲ *Back up data.* As always, if valuable data is not backed up, back it up before you do anything else. Recall from Chapter 13 that you can use the Vista Backup and Restore Center or the Windows XP Ntbackup utility to back up data. Don't risk the data without the user's permission.



Notes Viruses, adware, worms, and other malicious software can use Windows resources and pull a system down. Keep antivirus software running in the background. If you see a marked decrease in Windows performance, scan the hard drive for viruses, worms, and adware.

STEP 2: CHECK IF THE HARDWARE CAN SUPPORT THE OS

The system might be slow because the OS does not have the hardware resources it needs. Use the Vista Windows Experience Index, upgrade advisors, and System Information to find out if the system can support the OS. If you find that the system does not meet the minimum requirements or hardware is not compatible, discuss the situation with the user. You might be able to upgrade the hardware or install another OS that is compatible with the hardware that is present.

WINDOWS VISTA EXPERIENCE INDEX

Windows Experience Index, under Windows Vista, is a summary index designed to measure the overall performance of a system. You can use it to compare systems and identify performance bottlenecks in a particular system. To use it, click **Start**, right-click **Computer**, and select **Properties** from the shortcut menu. In the System window, click **Windows Experience Index**. The Performance Information and Tools window appears. Figure 14-41 shows the window for a system with performance issues, and Figure 14-42 shows the window for a high-end system. Currently, index scores range from 1.0 to 5.9 for Windows Vista.

The base score is the lowest score of all components and identifies the bottleneck for the system. In the case of the computer in Figure 14-41, this bottleneck is memory. Therefore, to improve performance on this system, a memory upgrade should be considered. However, don't always assume a hardware upgrade is necessary. If the bottleneck appears to be graphics, the problem might be solved by updating the graphics drivers or by updating Windows. Try updating the graphics drivers before you consider upgrading the video card.

CHECK FOR HARDWARE OR SOFTWARE COMPATIBILITY

To make sure that all hardware or software installed on the system is compatible with Windows Vista, use the **Vista Upgrade Advisor**. Download the program from the Microsoft

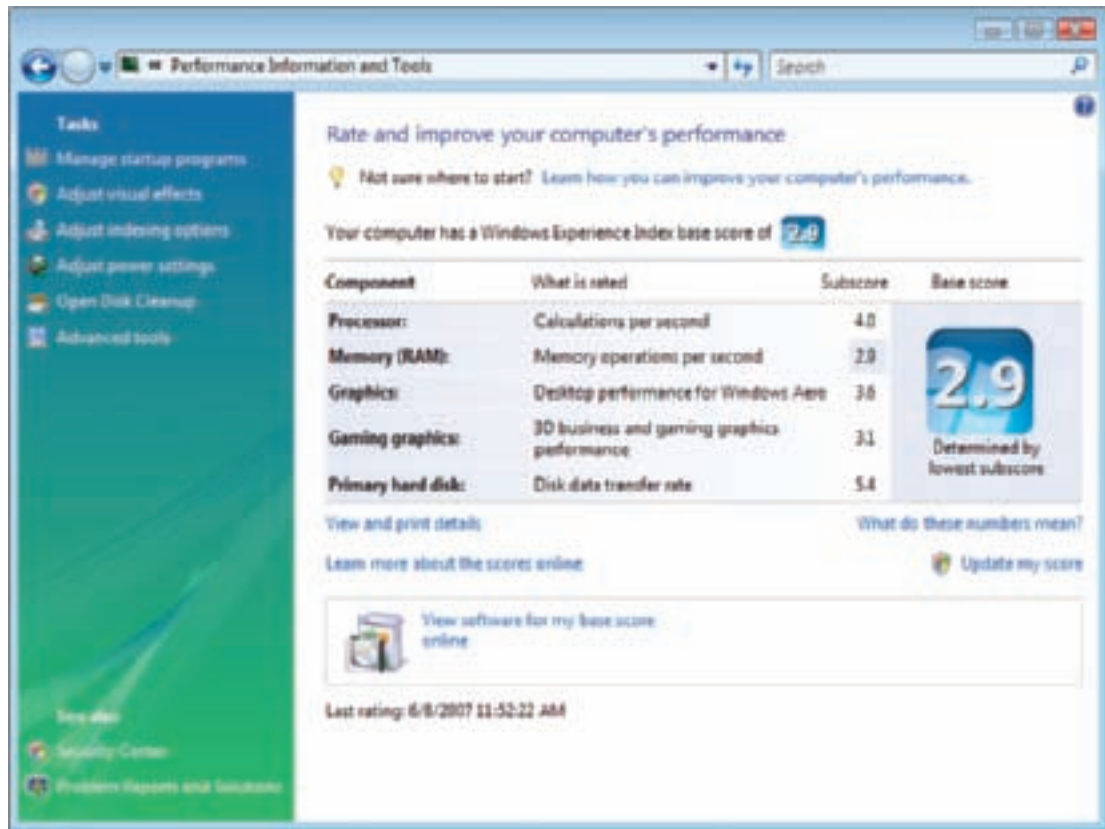


Figure 14-41 Use the Windows Experience Index to get a snapshot of a computer's performance and identify potential bottlenecks
Courtesy: Course Technology/Cengage Learning



Figure 14-42 The Windows Experience Index for this system reports no potential bottlenecks
Courtesy: Course Technology/Cengage Learning

A+
220-702
2.3
2.4

Web site at www.microsoft.com/windows/windows-vista/get/upgrade-advisor.aspx. Be sure to connect your printer and USB devices before you use the program to scan the system. If the scan finds software or hardware that has compatibility issues with Vista, it might report an update that you can use. Follow any guidelines it gives to solve the problem.

For Windows XP, the upgrade advisor is no longer available on the Microsoft Web site, but you can find it on the XP setup CD. Run this program from a command prompt window: `D:\I386\Winnt32 /checkupgradeonly`. You might need to substitute a different drive letter for your optical drive.

You can also use the System Information Utility (`msinfo32.exe`) to find information about the installed processor and its speed, how much RAM is installed, and free space on the hard drive. Compare all these values to the minimum and recommended requirements for Windows listed in Chapter 12.

If you suspect the processor is not fast enough for the system, you can use Performance Monitor to see how well it's performing. Following instructions given earlier in the chapter, open the Reliability and Performance Monitor. To get more detailed information, click Performance Monitor, which is tracking CPU activity (see Figure 14-43). Leave the window open on the screen as you perform various operations and watch the percentage activity of the CPU.

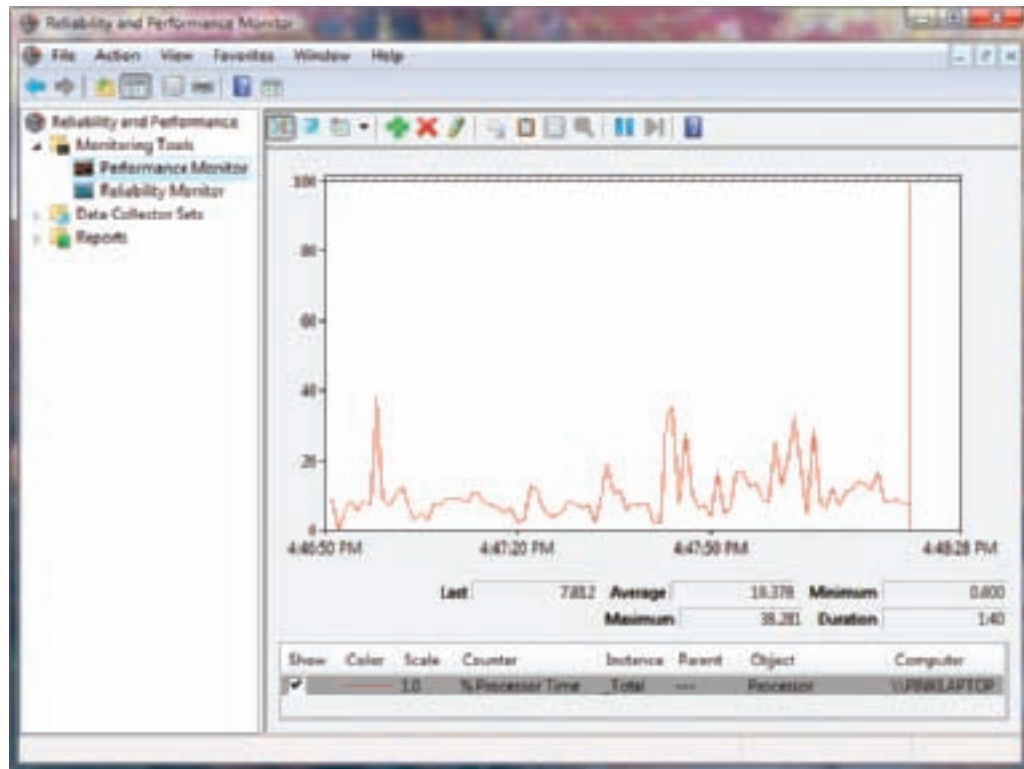


Figure 14-43 The Performance monitor tracking CPU performance
Courtesy: Course Technology/Cengage Learning

STEP 3: CHECK FOR PERFORMANCE WARNINGS

Windows Vista tracks issues that are interfering with performance. To see these warnings, click **Advanced tools** in the Windows Experience Index window shown in Figures 14-41 and 14-42. The Advanced Tools window appears, as shown in Figure 14-44. If Windows knows of performance issues, they are listed at the top of this window. For the computer in Figure 14-44, four issues are reported.

A+
220-702
2.3
2.4

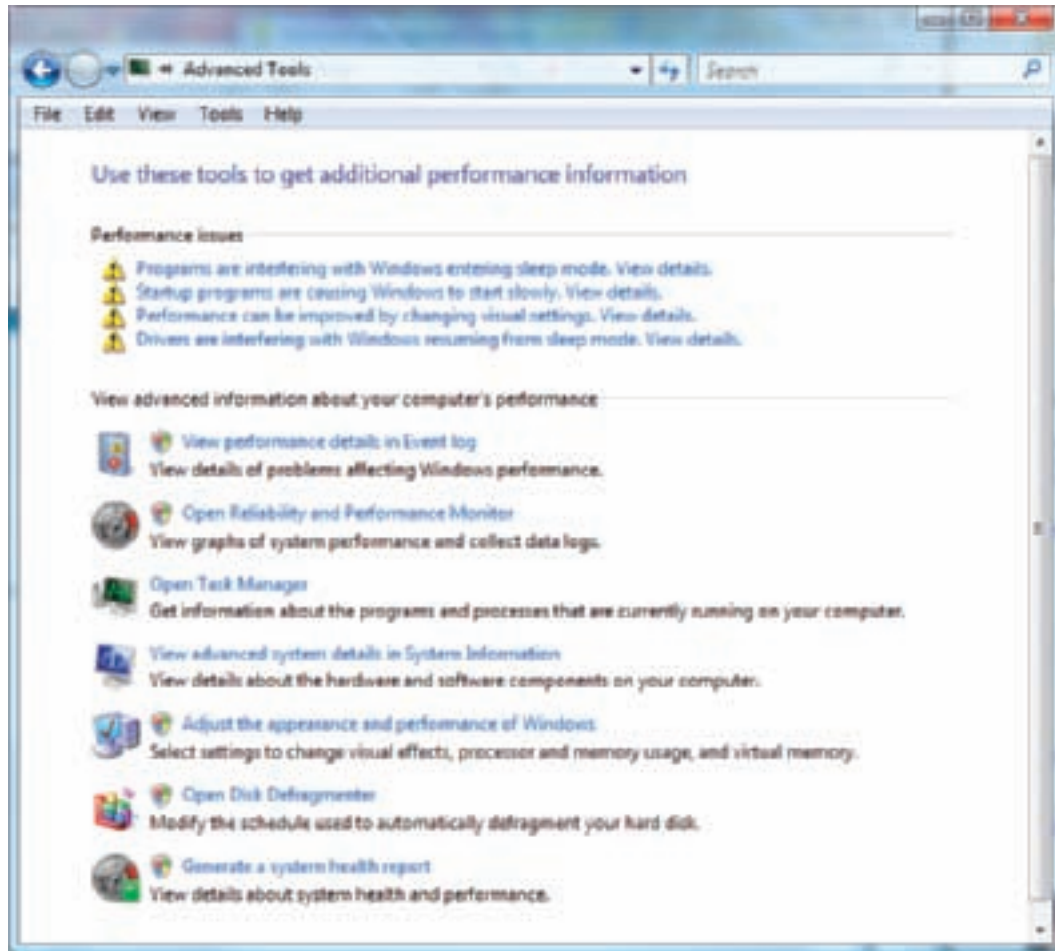


Figure 14-44 Vista provides these warnings and tools to improve Vista performance
Courtesy: Course Technology/Cengage Learning

When you click an issue, a dialog box appears that describes the issue and gives suggestions to resolve it. The four dialog boxes that will appear when you click the four issues listed in Figure 14-44 are shown in Figure 14-45. You will need to investigate each issue. Depending on the situation, you might be able to resolve an issue by updating a driver, disabling a device you don't need, or changing a setting in Windows or in an application. After you have made a change to the system, restart Windows before tackling the next issue. If a startup program is causing startup to be slow, consider removing it from the startup process and starting it manually as needed. After you have resolved an issue or have decided to live with it, you can click **Remove from list** so that it will no longer appear in the list of issues.

Tools that can help you improve Windows performance are listed in the lower part of the Advanced Tools window. When you click **View performance details in Event log**, you are taken to a log that tracks error events and warning events that are affecting performance (see Figure 14-46). Other tools that can be accessed through the Advanced Tools window are the Reliability and Performance Monitor, Task Manager, System Information, the Performance Options box, and Disk Defragmenter.

Windows XP does not offer the Advanced Tools window. For XP, open the Computer Management console and click Event Viewer. Then click the System log

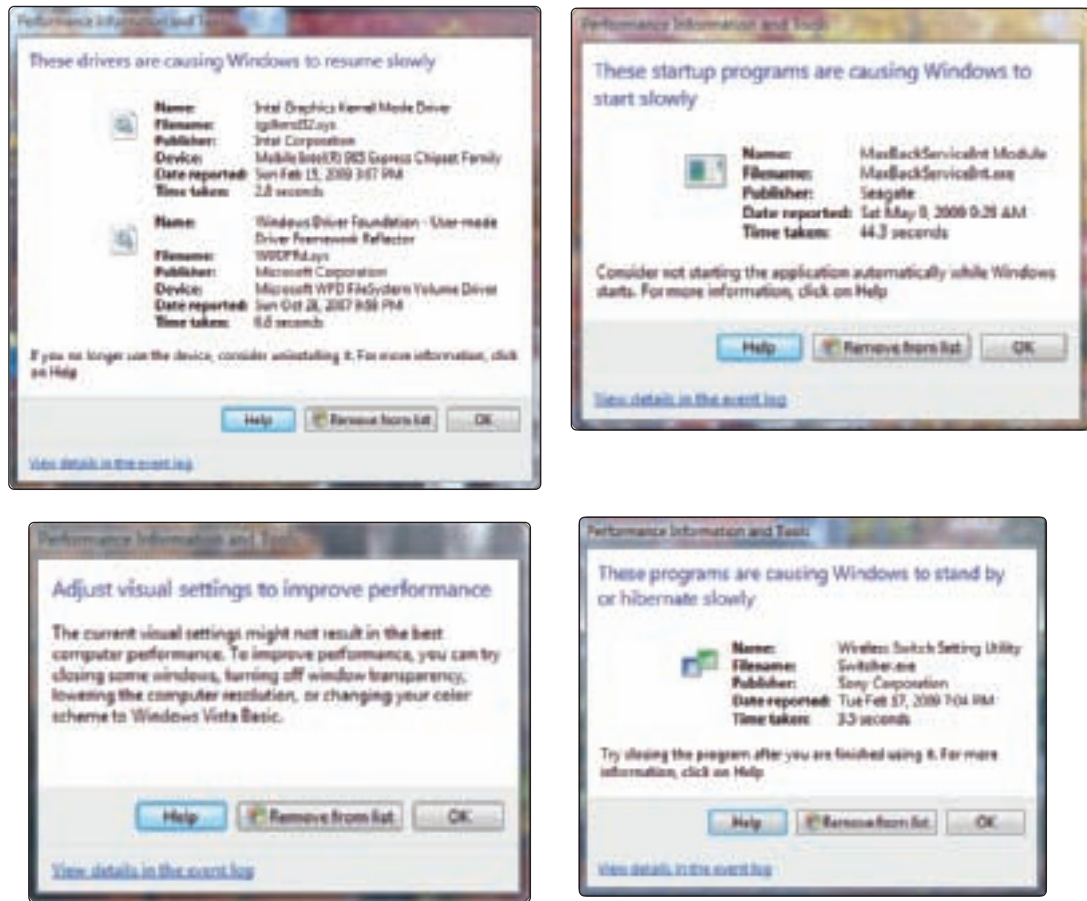


Figure 14-45 Windows reports four issues that are affecting performance
Courtesy: Course Technology/Cengage Learning

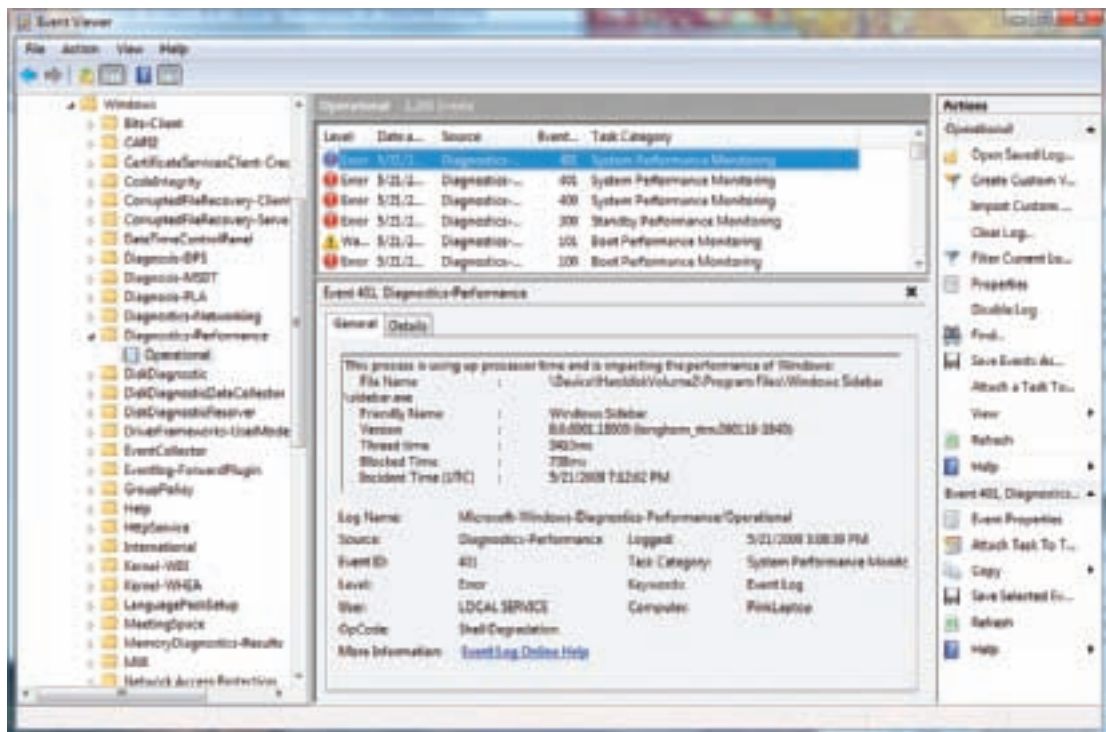


Figure 14-46 Event Viewer log reporting warning and error events affecting performance
Courtesy: Course Technology/Cengage Learning

A+
220-702
2.3
2.4

(see Figure 14-47). To sort the events by type, click the Type column. Look for events that might indicate a performance problem. To see details about an event, double-click it. The Event Properties box opens, shown on the right side of Figure 14-47. You can then scroll through the details of events by clicking the up and down arrows in the top-right side of this box.

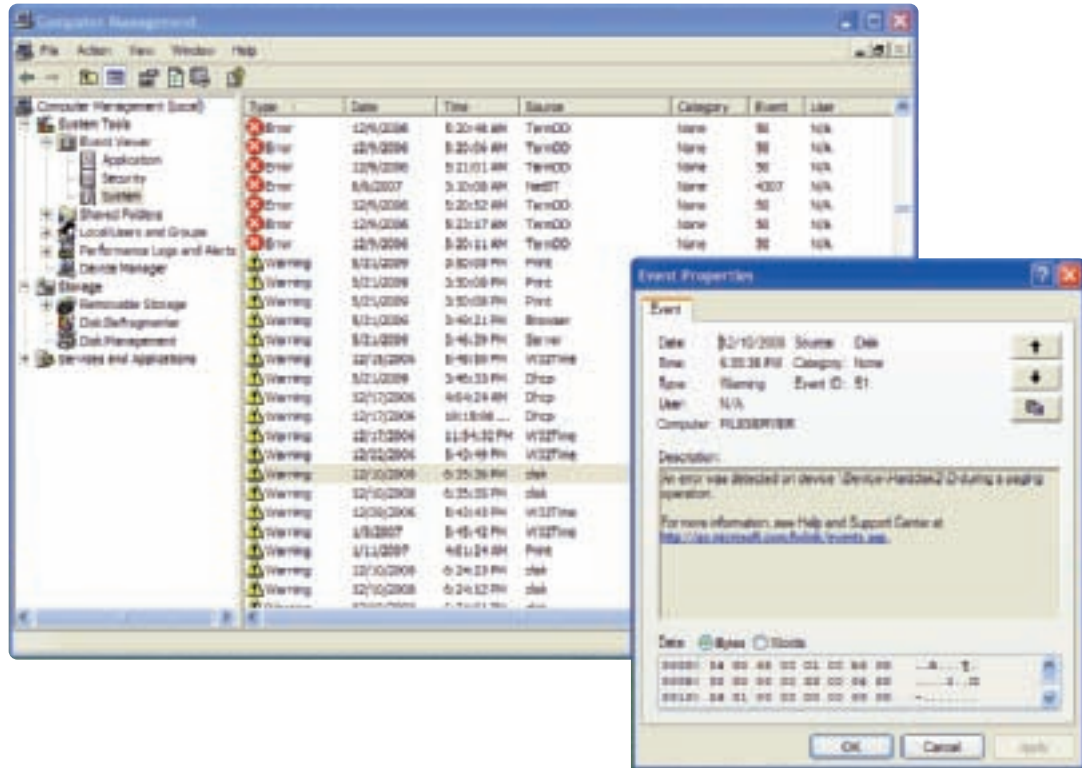


Figure 14-47 Windows XP Event Viewer shows events sorted by type
Courtesy: Course Technology/Cengage Learning

STEP 4: CHECK THE RELIABILITY MONITOR

The next step to improve performance is to try to determine if a problem with a hardware or software installation is affecting performance. You need to know if Windows performance has always been slow, or if poor performance began sometime after Windows was installed. If the problem began after Windows was installed, it might be caused by a hardware or software installation that has a problem or is not compatible with Windows. Try to determine about the time the problem started. Then do the following:

1. Open the **Reliability and Performance Monitor** and click the **Reliability Monitor** (see Figure 14-48). This monitor has faithfully been recording events since Windows was installed.
2. Scroll through the graph to find the day that the problem began. Look for failures related to software installations, applications, hardware, Windows, and other failures that happened about the time the problem occurred. To see details about

A+
220-702
2.3
2.4

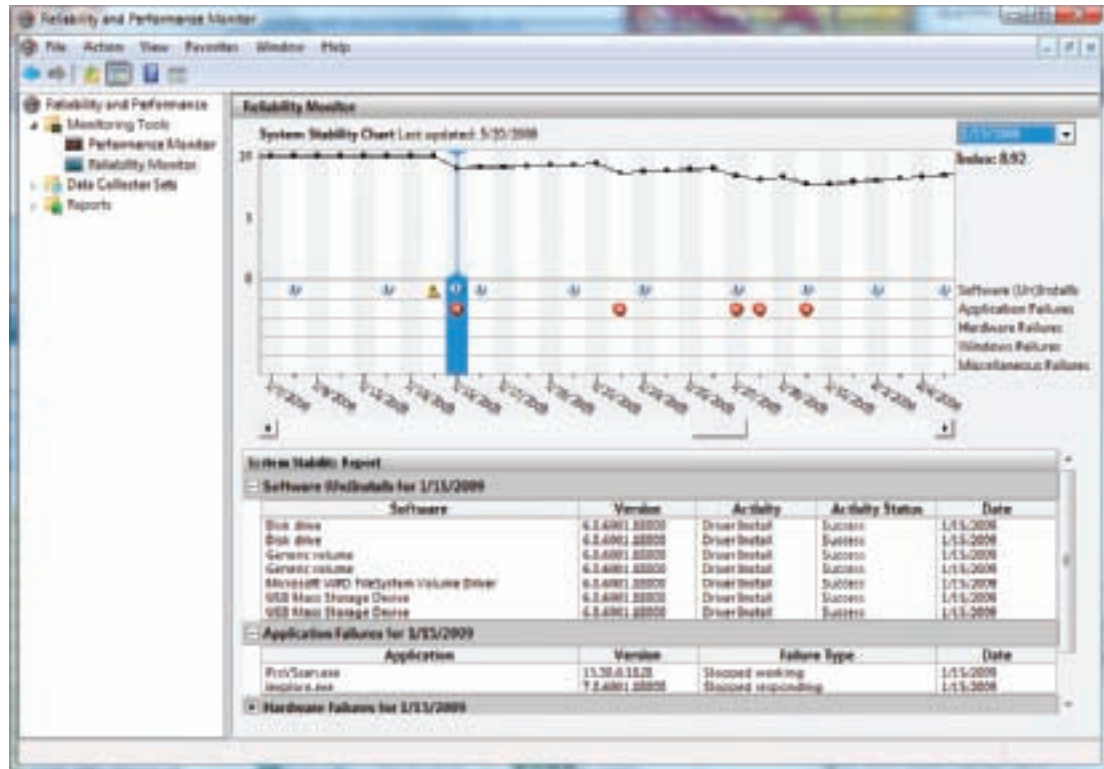


Figure 14-48 Use Reliability Monitor to search for when a problem began
Courtesy: Course Technology/Cengage Learning

the failure, click it. Also look for a dip in the line graph at the top of the Reliability Monitor graph. You can see such a dip in Figure 14-48 when drivers were installed. These drivers were installed for a Maxtor external hard drive that automatically makes backups of user data on this computer. Looking back at Figure 14-45, you can see that the Maxtor backup service is slowing down Windows startup. Options to fix the problem are to update the drivers or stop the service from launching at startup.

STEP 5: DISABLE THE INDEXER FOR WINDOWS SEARCH

The Windows indexer is responsible for maintaining an index of files and folders on a hard drive to speed up Windows searches. The indexing service has a low priority and only works when it senses that the hard drive is not being accessed by a service with a higher priority. However, it might still slow down performance. Do the following to find out if this service is causing a performance problem:

1. Find out if the indexing service is currently indexing the system. To do that, enter Index in the Vista Start Search box and select Indexing Options from the programs list. The Indexing Options box opens. If you see the indexing status is *Indexing speed is reduced due to user activity* (see Figure 14-49), know that indexing is in progress. Wait until the status changes to *Indexing complete*. You can now stop the indexing service.
2. To stop the indexing service, click **Start** and enter **services** in the Start Search box and press **Enter**. Respond to the UAC box. The Services console opens (see the left side of Figure 14-50).

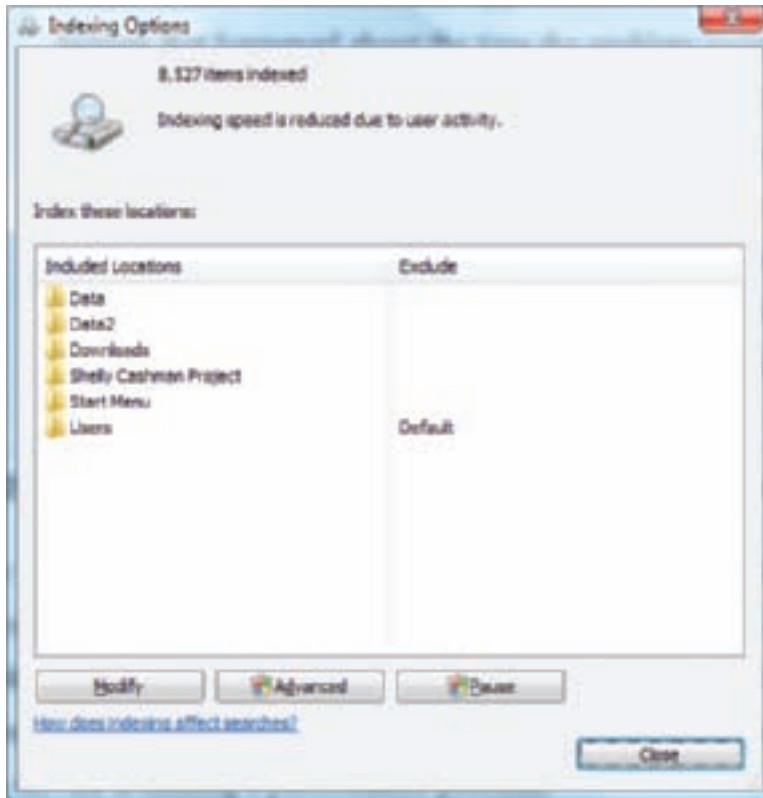


Figure 14-49 Indexing is in progress
Courtesy: Course Technology/Cengage Learning

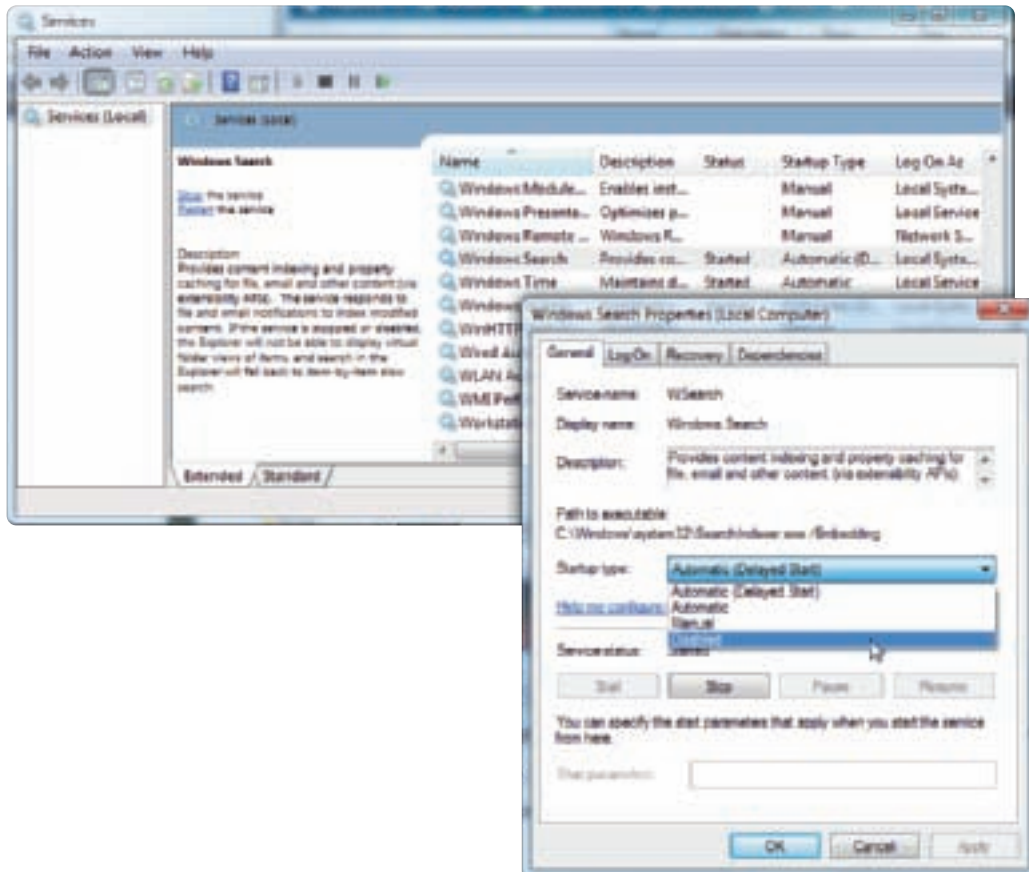


Figure 14-50 Windows Search service Startup type is Automatic (Delayed Start)
Courtesy: Course Technology/Cengage Learning

A+
220-702
2.3
2.4

3. Scroll down to and right-click the **Windows Search** service. Select **Properties** from the shortcut menu. The properties box opens. Change the Startup type to **Disabled** (see the right side of Figure 14-50). Click **Stop** to stop the service.
4. Click **Apply** and **OK** to close the properties box. Close the Services console window. Restart the computer.
5. Run the system for a while and see if performance improves.
6. If performance does not improve, restart the indexing service. To do that, use the Services console to set the status of the Windows Search service to **Automatic (Delayed Start)** and start the service. Then move on to the next section, *Step 6: Disable the Vista Aero Interface*.
7. If performance does improve, it is possible that the problem was caused by a corrupted index database. To rebuild the database, first use the Services console to set the Windows Search service status back to **Automatic (Delayed Start)** and to start the service.
8. Open the Indexing Options box, click **Advanced**, and respond to the UAC box. The Advanced Options box opens (see Figure 14-51).
9. To rebuild the indexing database, click **Rebuild**. A dialog box appears warning you that this can take some time. Click **OK**. Close the Indexing Options box.
10. After running the system for a while, if the performance problem returns, you can disable the Windows Search service and leave it disabled. However, know that searching will not be as fast without indexing.

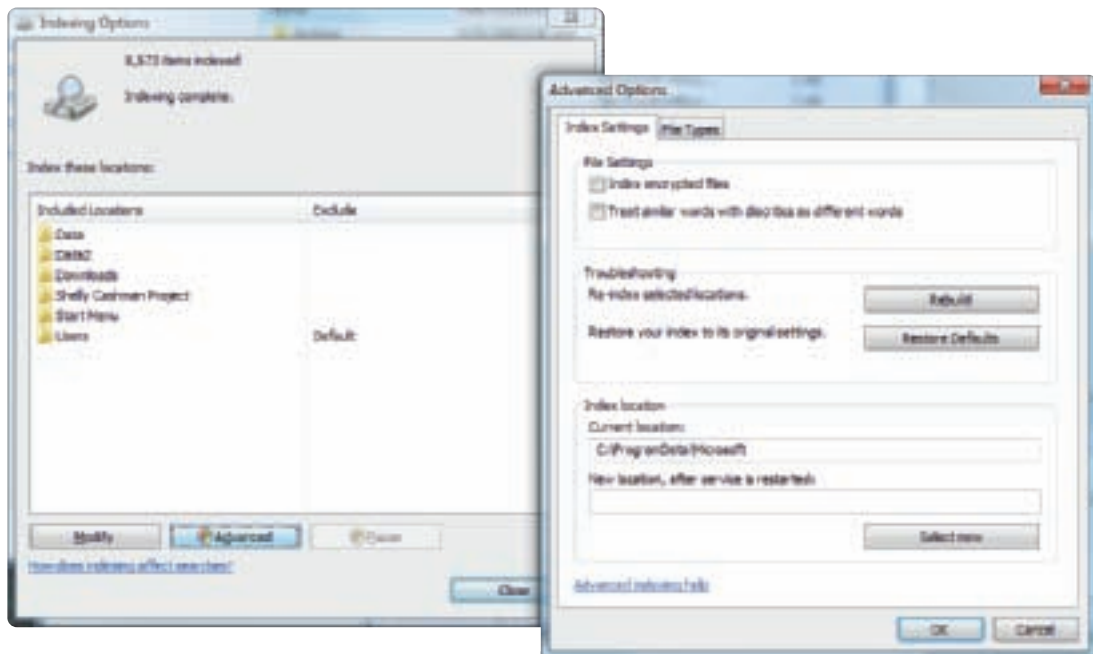


Figure 14-51 Rebuild the indexing database
Courtesy: Course Technology/Cengage Learning

A+
220-702
2.3
2.4

STEP 6: DISABLE THE VISTA AERO INTERFACE

The Vista Aero interface (also called the Aero Glass) might be slowing down the system because it uses memory and computing power. Try disabling it. If performance improves, you can conclude that the hardware is not able to support the Aero interface. At that point, you might want to upgrade memory, upgrade the video card, or leave the Aero interface disabled. To disable the Aero interface, do the following:

1. Right-click the desktop and select **Personalize** from the shortcut menu. The Personalization window opens. Click **Window Color and Appearance**. Then click **Open classic appearance properties for more color options**. The Appearance Settings box opens, shown on the right of Figure 14-52.
2. Under Color scheme, select **Windows Vista Basic** and click **Apply**. Close the dialog box and window.

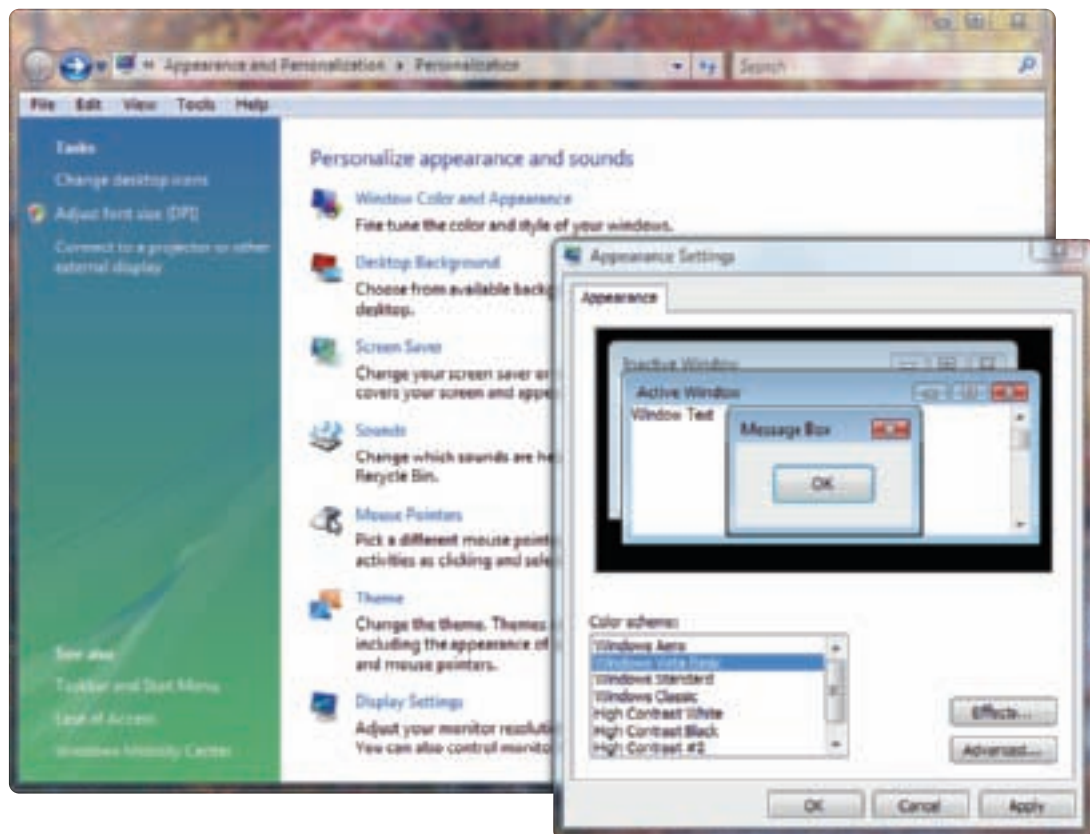


Figure 14-52 Disable Aero Glass to conserve system resources
Courtesy: Course Technology/Cengage Learning

STEP 7: DISABLE THE VISTA SIDEBAR

Recall that the Vista sidebar appears on the Windows desktop to hold miniapplications called gadgets. You might see a slight improvement in performance if you disable the sidebar. To do that, right-click the sidebar and select **Properties** from the shortcut menu. The

A+
220-702
2.3
2.4

Windows Sidebar Properties box appears (see Figure 14-53). Uncheck **Start Sidebar when Windows starts**. Then click **Apply** and **OK** to close the box.



Figure 14-53 Disable the Vista sidebar to improve performance
Courtesy: Course Technology/Cengage Learning

STEP 8: PLUG UP ANY MEMORY LEAKS

If you notice that performance slows after a system has been up and running without a restart for some time, suspect a memory leak. A memory leak is caused when an application does not properly release memory allocated to it that it no longer needs and continually requests more memory than it needs. To see how much memory an application has allocated to it that is not available to other programs, open the Reliability and Performance Monitor. Click the down arrow on the Memory bar. For example, in Figure 14-54, you can see that the sidebar.exe program (Vista sidebar) is using a significant amount of memory compared to other running applications.

Another way to search for a memory leak is to use Task Manager. Open Task Manager and click the **Processes** tab. On the menu bar, click **View, Select Columns**. Verify that the Memory Private Working Set, Handles, and Threads columns are checked and click **OK**. If you observe that the values in these three columns increase over time for a particular program, suspect the program has a memory leak. To sort the data by one column, click the column label. For example, the Task Manager window shown in Figure 14-55 is sorted by Memory. To solve the problem of a program that has a memory leak, try to get an update or patch from the program manufacturer's Web site.

A+
220-702
2.3
2.4

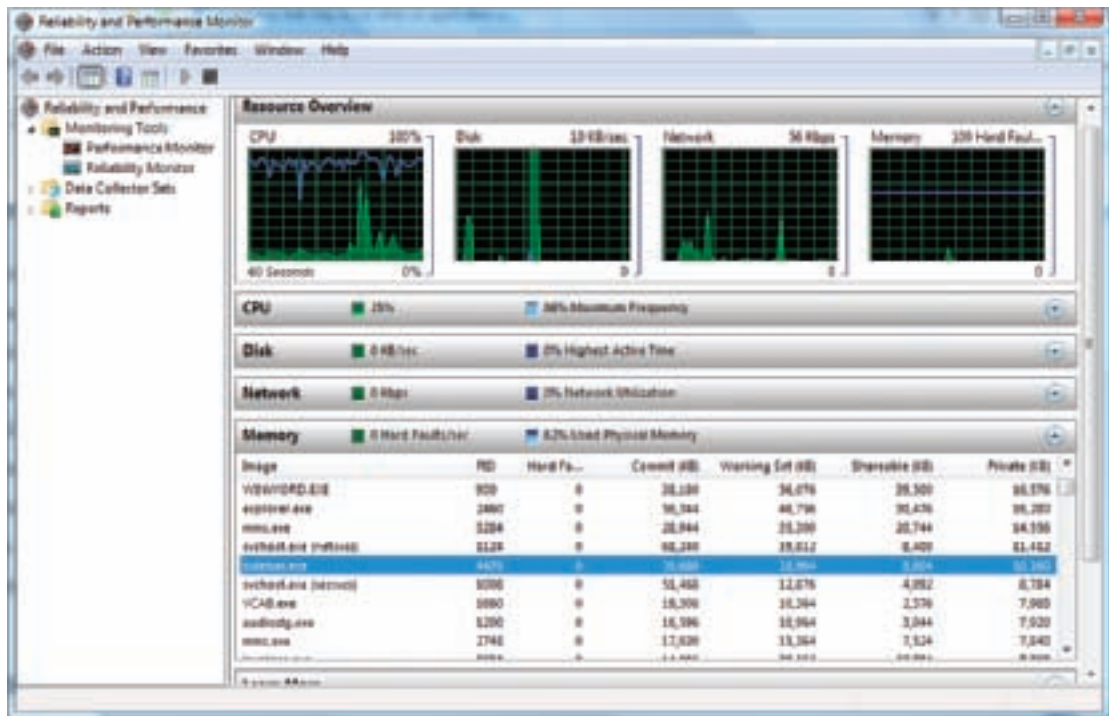


Figure 14-54 Memory allocated to the Vista sidebar program
Courtesy: Course Technology/Cengage Learning

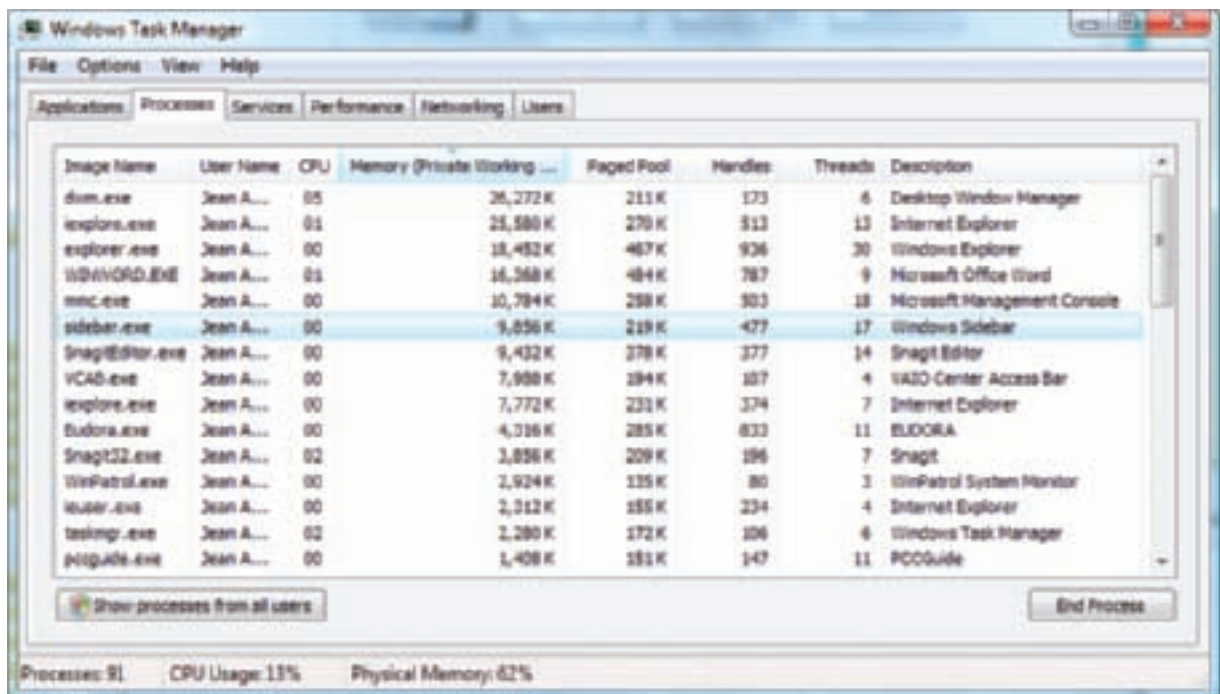


Figure 14-55 Task Manager shows how memory is allocated for an application
Courtesy: Course Technology/Cengage Learning

A+
220-702
2.3
2.4

STEP 9: CONSIDER DISABLING THE VISTA UAC BOX

One task that might slightly improve performance on a Vista system is to disable the UAC box. Even though you might see a slight performance gain, disabling it is not recommended. The UAC box can protect your system against users making unauthorized changes and against malware installing itself without your knowledge. It's best to keep it up and running. However, if you do decide to disable it, here's how:

1. Open Control Panel and click **User Accounts and Family Safety**. In the window that opens, click **User Accounts**. In the User Accounts window (see Figure 14-56), click **Turn User Account Control on or off**. Respond to the UAC box.
2. Uncheck **Use User Account Control (UAC) to help protect your computer**. Click **OK**. Close the User Accounts window.

STEP 10: CONSIDER USING VISTA READYBOOST

Windows Vista **ReadyBoost** uses a flash drive or secure digital (SD) memory card to boost hard drive performance. The faster flash memory is used as a buffer to speed up hard drive access time. You see the greatest performance increase using ReadyBoost when you have a slow hard drive (running at less than 7200 RPM). To find out what speed your hard drive is using, use System Information (Msinfo32.exe) and drill down to the Storage Disks (see Figure 14-57). The model of the hard drive appears in the right pane. Use Google to search on this brand and model; a quick search shows this drive runs at 5400 RPM. It's, therefore, a good candidate to benefit from ReadyBoost.

When you first connect a flash device, Windows will automatically test it to see if it qualifies for ReadyBoost. To qualify, it must have a capacity of 256 MB to 4 GB with at least 256 MB of free space, and run at about 2 MB/sec of throughput. If the device qualifies, Windows will ask you permission to use the device for ReadyBoost, which will tie up at least 256 MB



Figure 14-56 Control the User Account Control box
Courtesy: Course Technology/Cengage Learning

A+
220-702
2.3
2.4

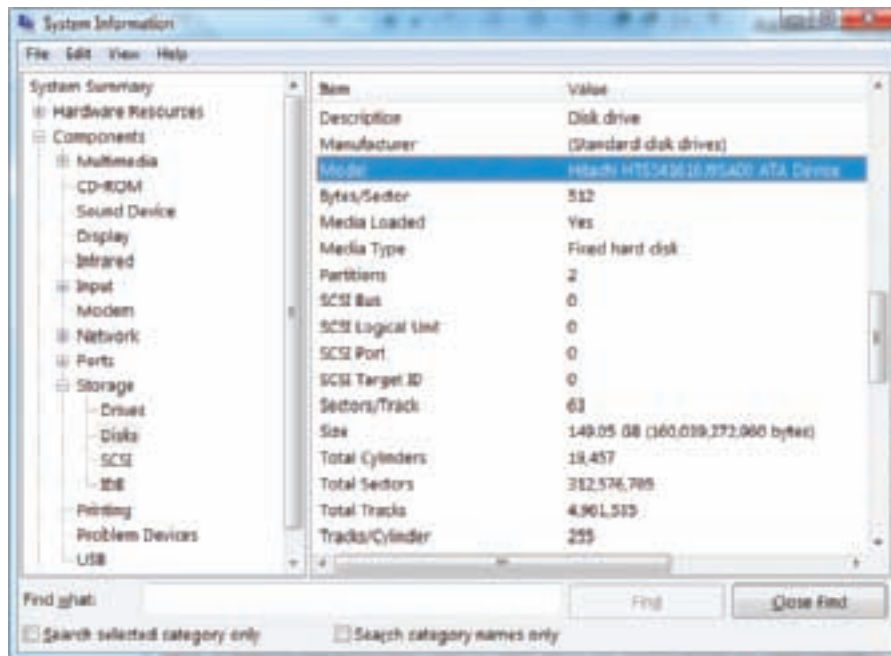


Figure 14-57 Use the System Information window to find out the brand and model of your hard drive
Courtesy: Course Technology/Cengage Learning

of free space. You can manually have Windows test a memory card or flash drive for ReadyBoost by right-clicking the device and selecting Properties from the shortcut menu. On the device properties window, click the **ReadyBoost** tab, as shown in Figure 14-58.

The best flash devices to use for ReadyBoost are the ones that use the faster buses. For example, an onboard memory card reader in a laptop will be faster than a USB 1.1 external

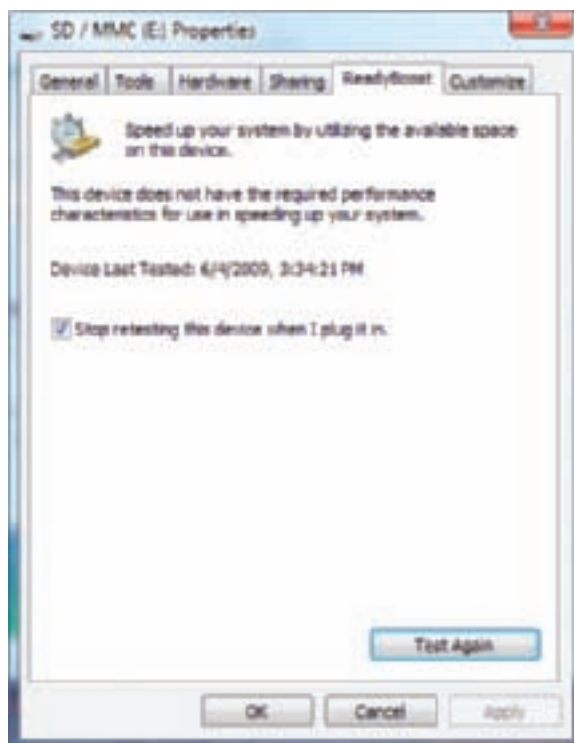


Figure 14-58 Offer a device for Windows to use for ReadyBoost
Courtesy: Course Technology/Cengage Learning

A+
220-702
2.3
2.4

memory card reader. When you remove the device, no data is lost because the device only holds a copy of the data.

STEP 11: CLEAN WINDOWS STARTUP

As a part of routine maintenance, you need to verify that startup programs are kept to a minimum so as to not slow down Windows startup or Windows performance. These routine chores include checking startup folders in Windows XP and Software Explorer in Windows Vista. If you still need to improve Windows performance, you can dig deeper into startup processes to make sure that unnecessary programs are not using up resources. To clean Windows startup, you can use Safe Mode and MSconfig to find out more about the problem, and then you can disable or uninstall programs causing the problem. So let's get started.

OBSERVE PERFORMANCE IN SAFE MODE

To find out if programs and services are slowing down Windows startup, boot the system in Safe Mode and watch to see if performance improves. Recall that Safe Mode loads a minimum configuration of hardware and software. If performance improves when you start the system in Safe Mode, you can assume that nonessential startup programs are slowing down the system when Windows boots normally. If you have a stopwatch or a watch with a second hand, you can time a normal Windows startup from the moment you press the power button until the wait icon on the Windows desktop disappears. Then time the system when it boots into Safe Mode. If the difference is significant, follow the steps in this part of the chapter to reduce Windows startup to essentials. To boot the system in Safe Mode, press F8 while Windows is loading and then select Safe Mode with Networking from the boot options menu (see Figure 14-59).

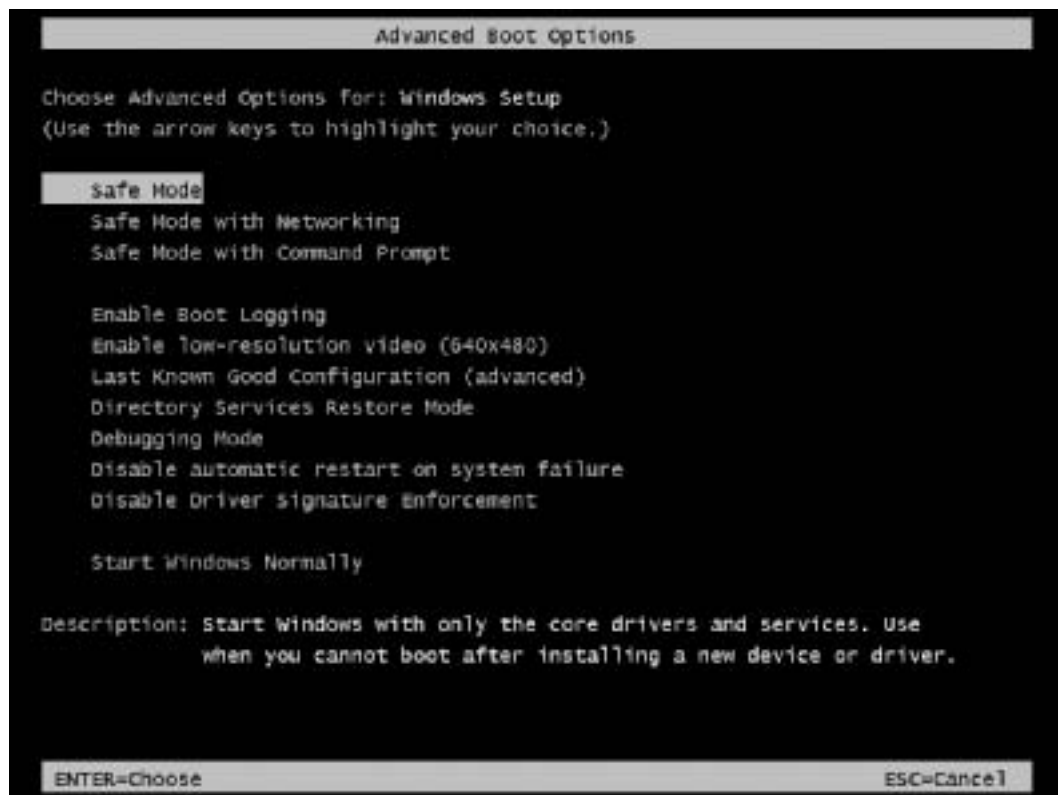


Figure 14-59 Windows Advanced Boot Options menu allows you to launch Safe Mode
Courtesy: Course Technology/Cengage Learning

A+
220-702
2.3
2.4

If the performance problem still exists in Safe Mode, then you can assume that the problem is with a hardware device, a critical driver, or a Windows component. How to solve problems with these components is covered in Chapters 15 and 16. If the problem does not occur when booting into Safe Mode, then use the tools discussed next to find the nonessential service or program causing the problem.

A+
220-702
2.3
2.4
2.1

USE MSCONFIG TO FIND A STARTUP PROGRAM AFFECTING PERFORMANCE

You can use the MSConfig utility to zero in on the service or other program that is slowing down startup. The process of using MSConfig to find the programs causing the problem is described in Figure 14-60. The recommended strategy uses a search technique called a half-again search.

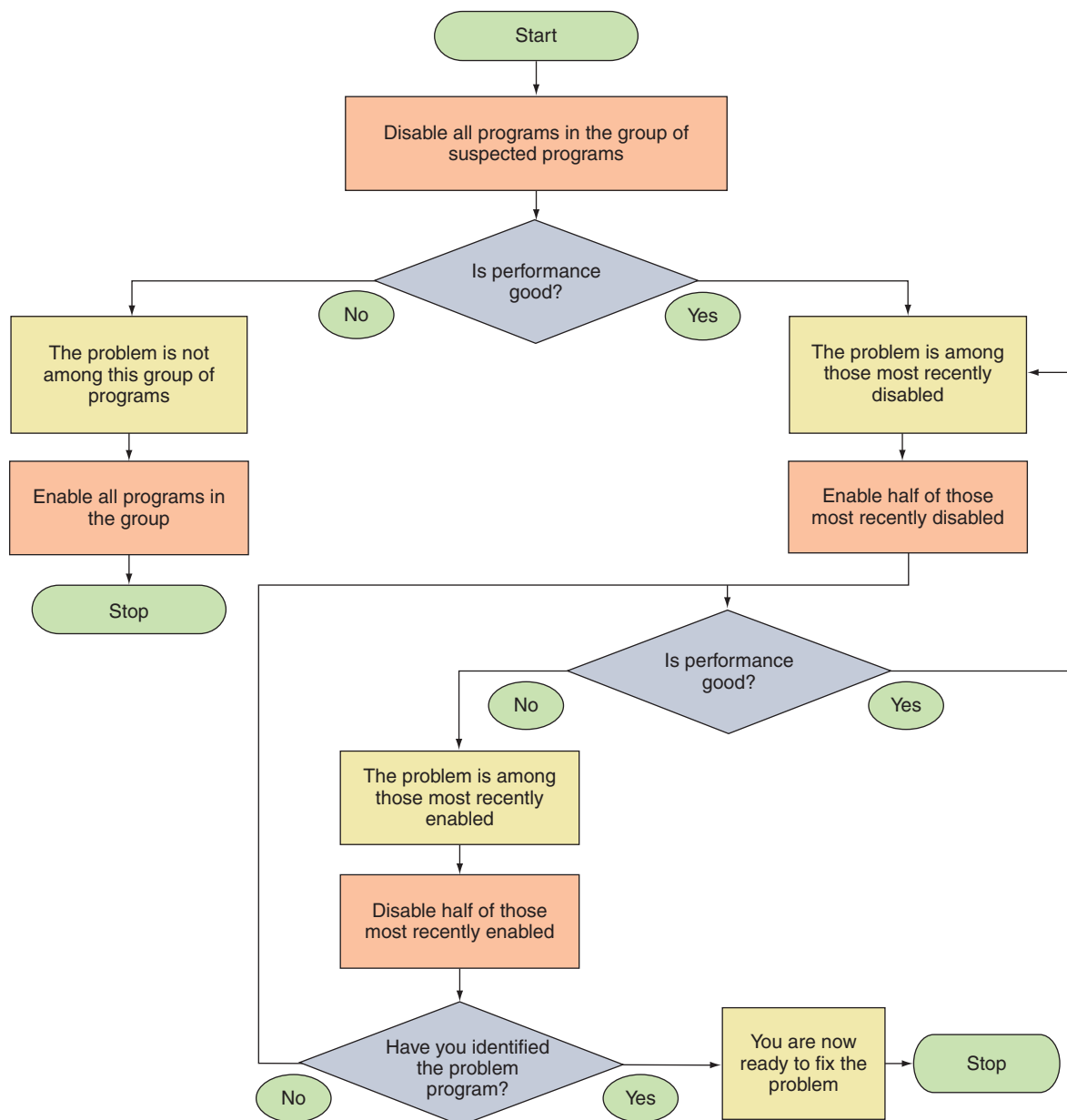


Figure 14-60 Strategy to identify the program(s) causing the problem
Courtesy: Course Technology/Cengage Learning

APPLYING CONCEPTS

You can demonstrate the effectiveness of the half-again search technique (also called a binary search) by playing the number guessing game with a friend. Tell your friend to pick a number between one and 1,000,000. Tell him you can guess the number if he will answer no more than 21 questions. The first question is “Is the number between one and 500,000?” If the answer is “No,” then you know the number is between 500,000 and 1,000,000. The next half-again question is, “Is the number between 500,000 and 750,000?” Using this technique, you can zero in on the answer in fewer than 21 questions.

Follow these steps using MSconfig to identify one or more programs as the source of the problem:

1. To launch the utility, enter `msconfig.exe` in the Vista Start Search box or the XP Run box and press **Enter**. For Vista, respond to the UAC box.
2. To look for the problem among the non-Microsoft services, click the **Services** tab (see Figure 14-61). Check **Hide all Microsoft services**, and then click **Disable all**. Click **Apply**. Close the System Configuration window and restart the computer.

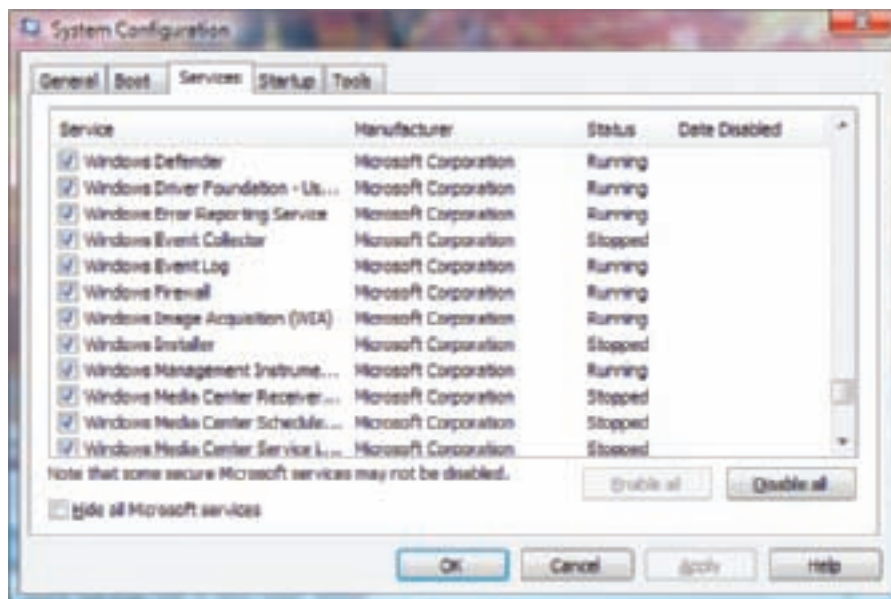


Figure 14-61 Use the System Configuration Utility (MSconfig) to temporarily disable services
Courtesy: Course Technology/Cengage Learning

3. Has performance improved? If so, you can assume that one or more services you disabled are the source of the problem. You can find out which service is causing the problem by enabling them one at a time, restarting the system each time, until the problem returns. This process can take a lot of time! A faster approach is to use the half-again technique. With this technique, use MSconfig to enable half the services you disabled and then restart the system. Did the problem return? If so, disable half of those you just enabled and restart again. If not, enable half of the disabled services. Restart the system and look for a performance improvement.

A+
220-702
2.3
2.4
2.1

4. Keep repeating Step 3 until you have identified the service that is causing the problem. Next, try to update the service, or, if it is nonessential, consider uninstalling or permanently disabling it. To permanently disable a service, use the Services console.
5. If performance does not improve by disabling all services, you can assume the problem is not with the services. In that case, enable them all and select the Startup tab.
6. Disable all the programs listed on the Startup tab and restart the system. If performance improves, begin the process diagramed in Figure 14-60 to enable half the programs that are disabled until you zero in on the problem.
7. If no non-Microsoft service or startup program caused the problem, then you can assume the problem is caused by a Microsoft service. Disable all services, including the Microsoft services and test performance. If performance improves, use MSConfig to keep enabling services until you find the Microsoft service causing the problem. You can then update the service or replace it using tools described in Chapters 15 and 16.
8. Remember that you don't want to permanently leave MSConfig in control of startup. After you have used MSConfig to identify the problem, use other tools such as the Services console or startup folders to permanently remove them from startup. After the problem is fixed, return MSConfig to a normal startup.

**Caution**

Be aware that when you disable all Microsoft services, you are disabling Networking, Event Logging, Error Reporting, Windows Firewall, Windows Installer, Windows Backup, Print Spooler, Windows Update, System Protection, and other important services. These services should only be disabled when testing for performance problems and then immediately enabled when the test is finished. Also, know that if you disable the Volume Shadow Copy service, all restore points kept on the system will be lost. If you intend to use System Restore to fix a problem with the system, don't disable this service. If you are not sure what a service does, read its description in the Services console before you change its status.

A+
220-702
2.3
2.4

DISABLE OR UNINSTALL BACKGROUND PROCESSES AND STARTUP PROGRAMS

Recall that you can stop a service or other program using Task Manager, and you can use MSConfig to stop it from starting at startup. You can also use Task Manager to view resources a program is using and change the priority level of a running program. However, all these solutions should be considered temporary fixes. To permanently manage a service, use the services console or the Windows component responsible for the service, such as an applet in Control Panel. For third-party services, such as software to update an application or software to download digital photos, the application is likely to have a management utility to control the service or background process.

When investigating a service, try using a good search engine on the Web to search for the name of the service or the name of the program file that launches the service. Either can give you information you need to snoop out unwanted services. If you're not sure you want to keep a certain service, use MSConfig to temporarily disable it at the next boot so that you can see what happens.

**Notes**

One service you might want to disable in the Services console is the Windows Installer service that is responsible for uninstalling and installing software. You can then manually start the service if you need to install or uninstall software.

A+
220-702
2.3
2.4

When you permanently disable a service using the Services console or some other tool, don't forget to reboot to make sure everything works before moving on to the next tool to use in cleaning up startup: Task Scheduler.

CHECK FOR UNWANTED SCHEDULED TASKS

Home and business editions of Windows Vista and Windows XP Professional offer a **Task Scheduler** that can be set to launch a task or program at a future time, including at startup. Task Scheduler stores tasks in a file stored in the C:\Windows\System32\Tasks folder. For example, in Figure 14-62, there are four scheduled tasks showing and other tasks are stored in three folders.

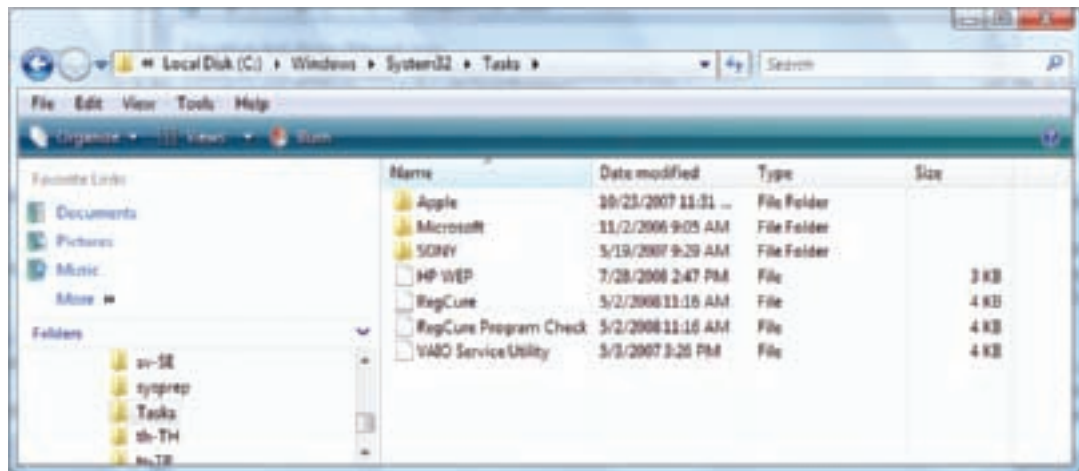


Figure 14-62 The Tasks folder can contain tasks that launch at startup
Courtesy: Course Technology/Cengage Learning

To view a list of scheduled tasks, click **Start, All Programs, Accessories, System Tools, and Task Scheduler**. The Task Scheduler window opens as shown in Figure 14-63 for Vista after you have responded to the UAC box. For a bare-bones Vista system, the Microsoft folder will be the only item listed in the Task Scheduler Library on the left. But for this system, other folders and tasks are present. To see details about a task,

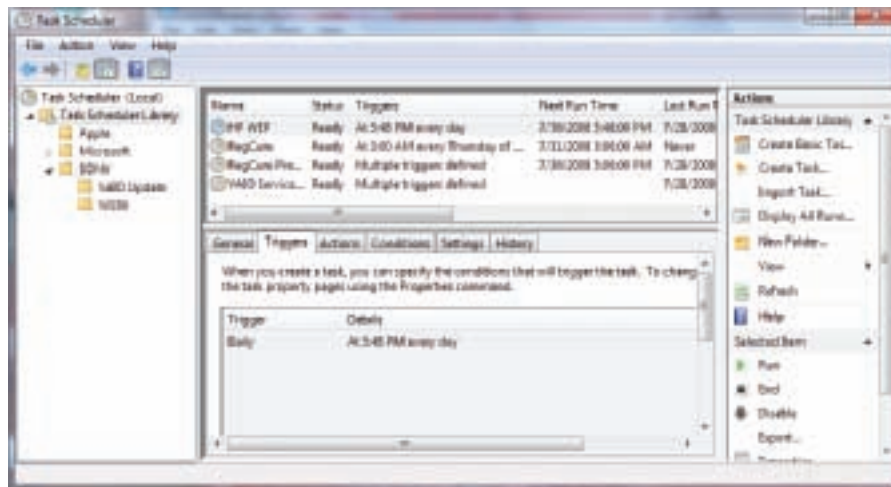




Figure 14-63 View and manage tasks from the Task Scheduler window
Courtesy: Course Technology/Cengage Learning

A+
220-702
2.3
2.4


including what triggers it, what actions it performs, the conditions and settings related to the task, and the history of past actions, select the task and then click the tabs in the lower-middle pane. For example, in Figure 14-63 you can see that the HP WEP task is scheduled to run at 5:48 PM daily.

 **Notes** Windows Vista automatically runs Disk Defragmenter weekly, but Windows XP does not offer this feature. For XP, you can use Task Scheduler to schedule Disk Defragmenter to run weekly.

Tasks can be scheduled to run when users log on, when Windows launches, or at a particular time of day, week, or month. Tasks can be scheduled to run one time or many times. Tasks can be applications, services, or other background processes. Tasks can be scheduled to download e-mail or open Internet Explorer and download a Web page. Tasks can also consist of batch programs or Windows scripting. Using the Task Scheduler window, you can add, delete, or change a task, and these actions can also be performed at a command prompt.

 **Notes** Tasks can be hidden in the Task Scheduler window. To be certain you're viewing all scheduled tasks, unhide them. In the menu bar, click **View**, and then **Show Hidden Tasks**.

All this information is helpful when researching scheduled tasks to unravel the mystery of processes or activities that fail or bog down a system. In cleaning up startup, be sure to check the Task Scheduler window *after* you have run antivirus software and disabled or uninstalled all startup programs you don't want. If you still find scheduled tasks present in the Task Scheduler window, research each task by searching for information about it on the Internet. (Be sure you use reliable Web sites to get your information.) If you decide you don't want a task, rather than deleting it, select the task and click **Disable** in the Actions pane so that you can undo your change if necessary. The exception to this rule is if you know the task is malware; in this case, definitely delete it!

 **Notes** When searching the Internet for information about a process, be sure to use reliable Web sites to get your information. Some sites will tell you a good process is a bad one just so you'll purchase their software to scan the system for errors.

In the process of cleaning up startup, you might run into software that you'll want to uninstall. In the next part of the chapter, you'll learn how to manually remove software when normal uninstall methods fail.

HOW TO MANUALLY REMOVE SOFTWARE

In this part of the chapter, we focus on getting rid of programs that refuse to uninstall or give errors when uninstalling. In these cases, you can manually uninstall a program. Doing so often causes problems later, so use the methods discussed in this section only as a last resort after normal uninstall methods have failed.

A+
220-702
2.3
2.4

Notes Before uninstalling software, make sure it's not running in the background. Antivirus software cannot be uninstalled if it's still running. You can use Task Manager to end all processes related to the software, and you can use the Services console to stop services related to the software. Then remove the software.

FIRST TRY THE UNINSTALL ROUTINE

Most programs written for Windows have an uninstall routine which can be accessed from the Vista Programs and Features applet in the Control Panel, the XP Add Remove Programs applet in the Control Panel, or a utility in the All Programs menu. For example, in Figure 14-64 you can see in the All Programs menu that Uninstall is an option for the RegCure software installation. Click this option and follow the directions on-screen to uninstall the software. Alternately, you can use the applet in Control Panel to remove the software.

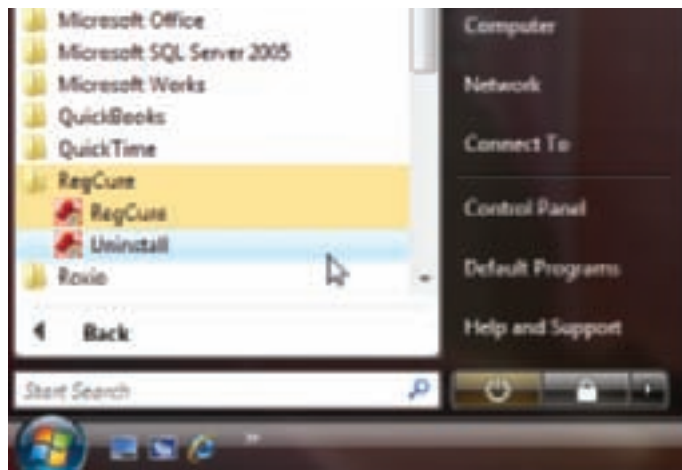


Figure 14-64 Most applications have an uninstall utility included with the software
Courtesy: Course Technology/Cengage Learning

MANUALLY DELETE THE PROGRAM FILES

If the uninstall routine does not work or is missing, as a last resort, you can manually delete the program files and registry entries used by the software you want to uninstall. In our example, we'll use the RegCure software by ParetoLogic, Inc. as the software to be deleted. Follow these steps:

1. Most likely, the program files are stored in the C:\Program Files folder on the hard drive (see Figure 14-65). For 64-bit editions of Vista, also look for program files in the C:\Program Files (x86) folder. Using Windows Explorer, look for a folder in these folders that contains the software. In Figure 14-65, you can see the RegCure folder under the Program Files folder. Keep in mind, however, that you might not find the program files you're looking for in the C:\Program Files or C:\Program Files (x86) folder because when you install software, the software installation program normally asks you where to install the software. Therefore, the program files might be anywhere, and you might need to search a bit to find them.
2. Delete the RegCure folder and all its contents. You'll need to confirm the deletion several times as Windows really doesn't like your doing such things.

A+
220-702
2.3
2.4

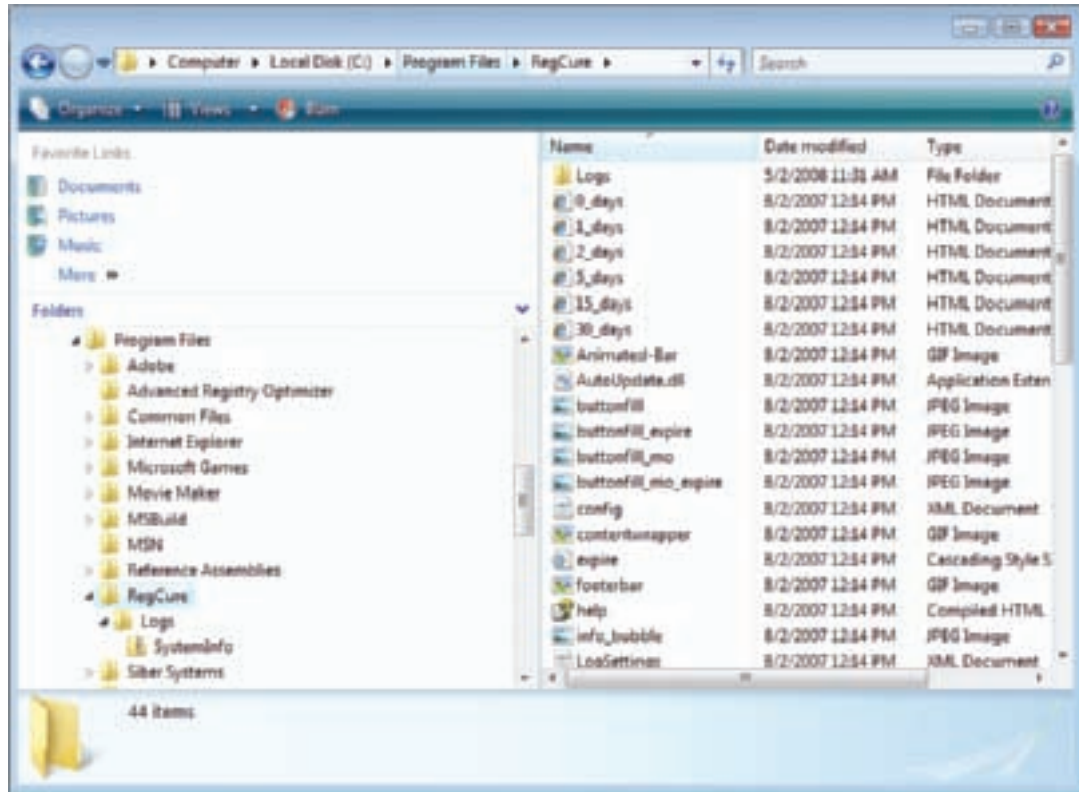


Figure 14-65 Program files are usually stored in the C:\Program Files folder
Courtesy: Course Technology/Cengage Learning

DELETE REGISTRY ENTRIES

Editing the registry can be dangerous, so do this with caution and be sure to back up first! Do the following to delete the registry entries for a program, which cause it to be listed as installed software in the Vista Programs and Features window or the XP Add or Remove Programs window of Control Panel:

1. Using one or more of the following methods, back up the registry: Use Windows XP NTBackup to back up the system state, back up the C:\Windows\System32\config folder, or create a restore point.
2. Click **Start**, type **regedit** in the Vista Start Search box or the XP Run box and press **Enter**. For Vista, respond to the UAC box.
3. Locate this key, which contains the entries that comprise the list of installed software in Control Panel: `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall`.
4. Back up the Uninstall key to the Windows desktop so that you can backtrack if necessary. To do that, right-click the Uninstall key and select **Export** from the shortcut menu (see Figure 14-39 earlier in the chapter).
5. In the Export Registry File dialog box, select the **Desktop**. Enter the filename as **Save Uninstall Key**, and click **Save**. You should see a new icon on your desktop named **Save Uninstall Key.reg**.
6. The Uninstall key can be a daunting list of all the programs installed on your PC. When you expand the key, you might see a long list of subkeys in the left pane, which

A+
220-702
2.3
2.4

have meaningless names that won't help you find the program you're looking for. Select the first subkey in the Uninstall key and watch as its values and data are displayed in the right pane (see Figure 14-66). Step down through each key, watching for a meaningful name of the subkey in the left pane or meaningful details in the right pane until you find the program you want to delete.

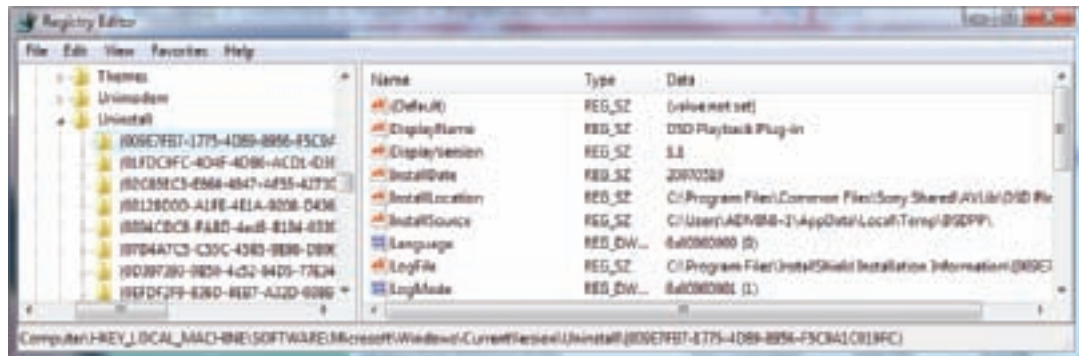


Figure 14-66 Select a subkey under the Uninstall key to display its values and data in the right pane
Courtesy: Course Technology/Cengage Learning

- To delete the key, right-click the key and select **Delete** from the shortcut menu (see Figure 14-67). When the Confirm Key Delete dialog box appears asking you to confirm the deletion, click **Yes**. Be sure to search through all the keys in this list because the software might have more than one key. Delete them all and exit the Registry Editor.

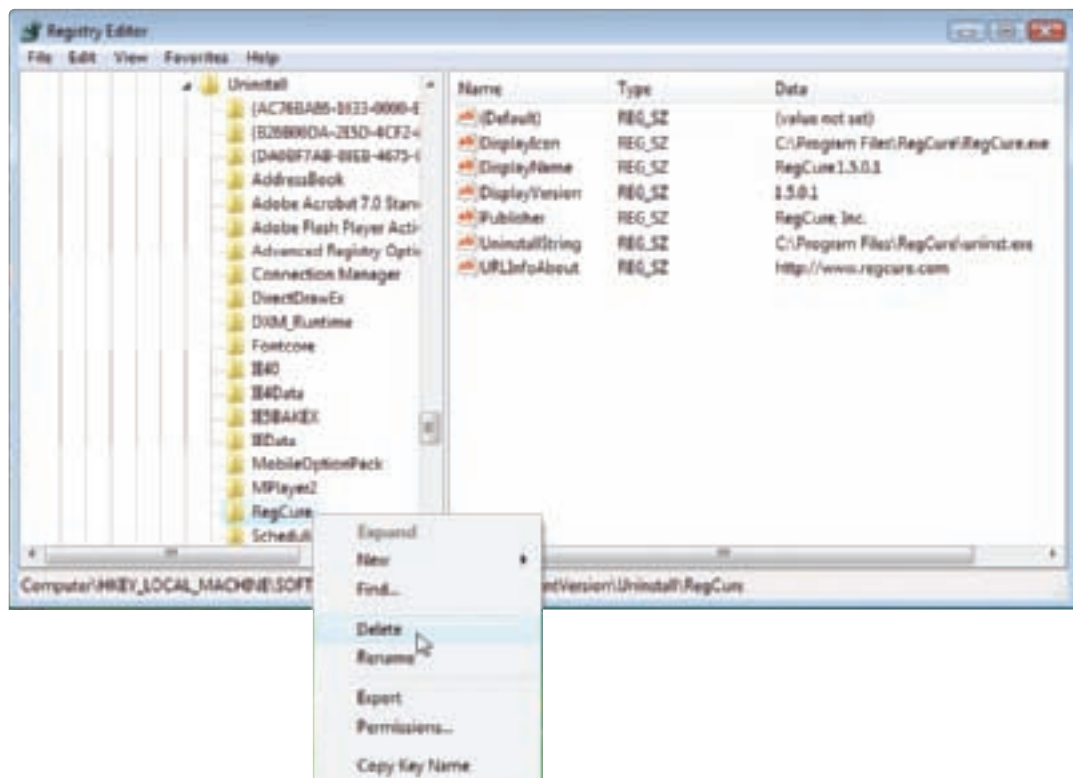


Figure 14-67 Delete the registry key that lists the software as installed software
Courtesy: Course Technology/Cengage Learning

A+
220-702
2.3
2.4

8. Open the Vista Programs and Features window or the XP Add or Remove Programs window and verify that the list of installed software is correct and the software you are uninstalling is no longer listed.
9. If the list of installed software is not correct, to restore the Uninstall registry key, double-click the **Save Uninstall Key.reg** icon on your desktop.
10. As a last step when editing the registry, clean up after yourself by deleting the **Save Uninstall Key.reg** icon and file on your desktop. Right-click the icon and select **Delete** from the shortcut menu.

REMOVE THE PROGRAM FROM THE ALL PROGRAMS MENU

To remove the program from the All Programs menu, right-click it and select **Delete** from the shortcut menu (see Figure 14-68). Click **Yes** and then **Continue** to confirm the deletion and respond to the UAC box.

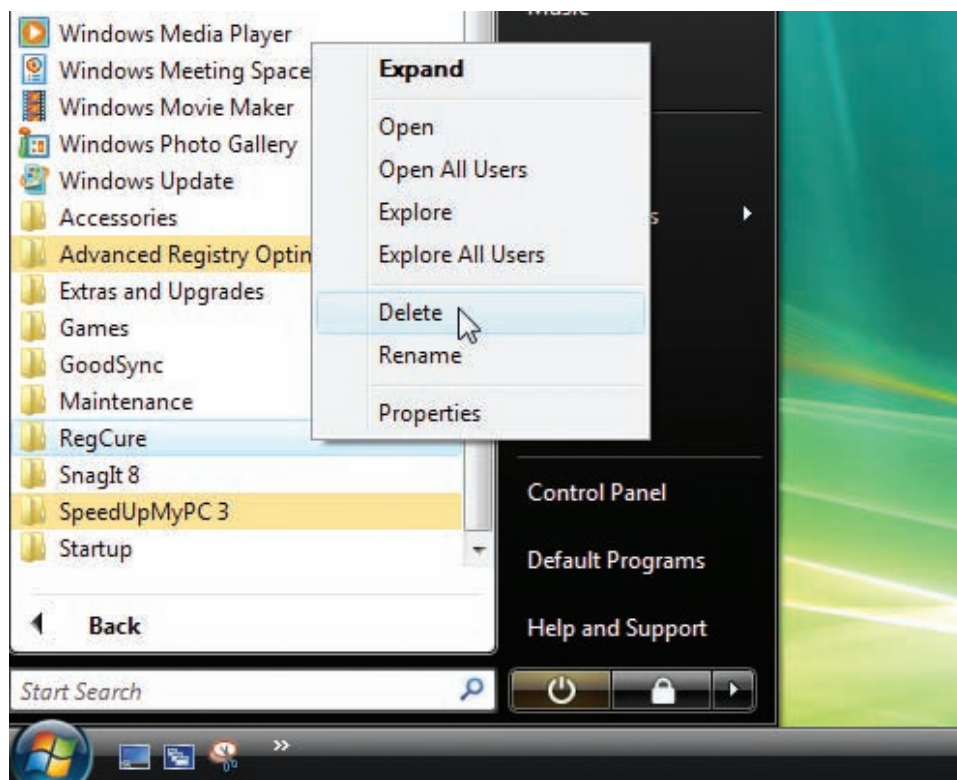


Figure 14-68 Delete the program from the All Programs menu
Courtesy: Course Technology/Cengage Learning

Restart the PC and watch for any startup errors about a missing program file. The software might have stored startup entries in the registry, in startup folders, or as a service that is no longer present and causing an error. If you see an error, use MSconfig to find out how the program is set to start. This entry point is called an orphaned entry. You'll then need to delete this startup entry by editing the registry, deleting a shortcut in a startup folder, or disabling a service using the Services console.

An example of an orphaned entry that resulted in a startup error after software was removed is shown in Figure 14-69. Somewhere in the system, the command to launch `OsioOijw.dll` is still working even though this DLL file has been deleted.

A+
220-702
2.3
2.4

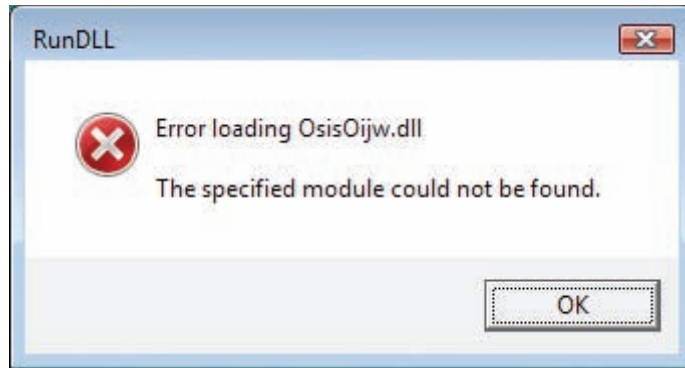


Figure 14-69 Startup error indicates an entry to launch a program has not been removed
Courtesy: Course Technology/Cengage Learning

One way to find this orphaned entry point is to use MSconfig. Figure 14-70 shows the MSconfig window, showing us that the DLL is launched from a registry key.

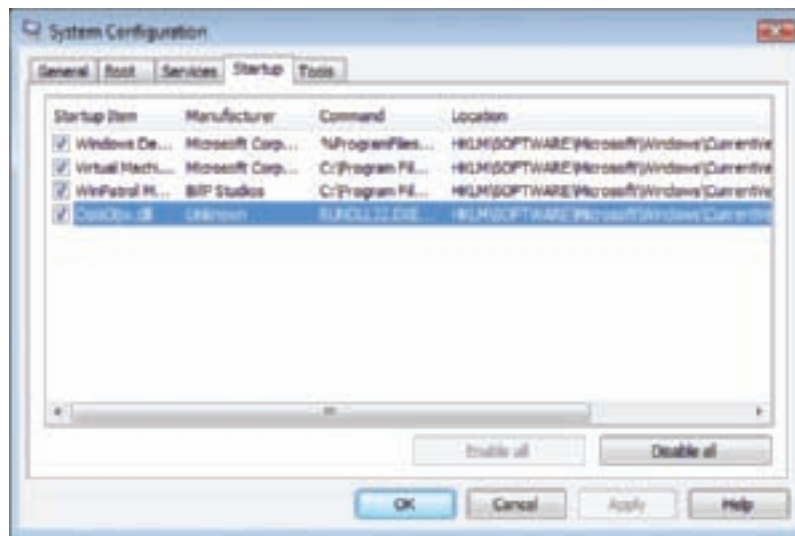


Figure 14-70 MSconfig shows how the DLL is launched during startup
Courtesy: Course Technology/Cengage Learning

The next step is to back up the registry and then use the Registry Editor to find and delete the key (see Figure 14-71).

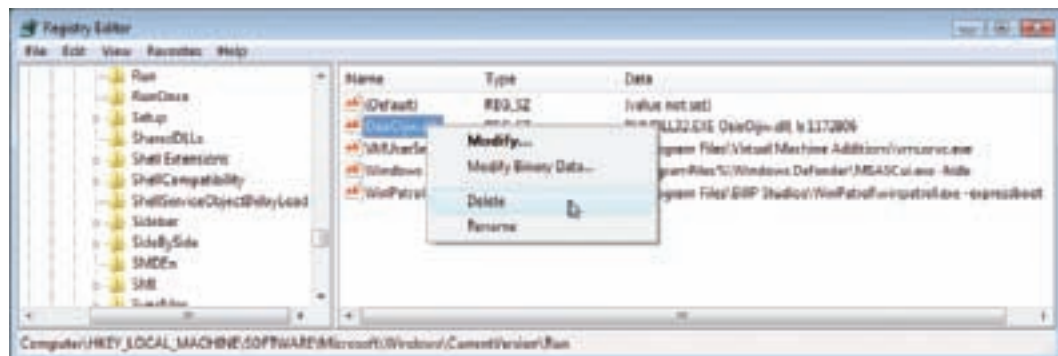


Figure 14-71 Delete the registry key left there by uninstalled software
Courtesy: Course Technology/Cengage Learning

REGISTRY KEYS THAT AFFECT STARTUP AND LOGON EVENTS

You have just seen how you can edit the registry to remove the entries left there by software that you have manually removed. Listed in this section are some registry keys where startup processes can be located. If a system is giving repeated startup errors or you have just removed several programs, you might want to search through these registry keys for processes left there by uninstalled or corrupted software that might be giving startup problems.

As you read through this list of registry keys to search, know that the list is not exhaustive. With experience, you'll learn that the registry is an everchanging landscape of keys and values.

Registry keys that affect the startup and logon events are listed in the bulleted list below. Your registry might or might not have all these keys. As you search the registry for entries in these keys, don't forget to first back up the registry. Because you'll be searching all over the registry and not just in one particular place, it's a good idea to create a restore point as well as back up the C:\Windows\System32\config folder so that the entire registry will be backed up.

These keys cause an entry to run once and only once at startup:

- ▲ HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
- ▲ HKLM\Software\Microsoft\Windows\CurrentVersion\RunServiceOnce
- ▲ HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- ▲ HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

Check each key in the list above and move on to the next list.

Group Policy (an administrator's tool to control what a user can do on a system) places entries in the following keys to affect startup:

- ▲ HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- ▲ HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

Windows loads many DLL programs from the following key, which is sometimes used by malicious software. Entries in this key are normal, so don't delete one unless you know it's causing a problem:

- ▲ HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

Entries in the keys listed next apply to all users and hold legitimate startup entries. Don't delete an entry unless you suspect it to be bad:

- ▲ HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- ▲ HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows
- ▲ HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
- ▲ HKCU\Software\Microsoft\Windows\CurrentVersion\Run

These keys and their subkeys contain entries that pertain to background services that are sometimes launched at startup:

- ▲ HKLM\Software\Microsoft\Windows\CurrentVersion\RunService
- ▲ HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

The following key contains a value named BootExecute, which is normally set to autochk. It causes the system to run a type of Chkdsk program to check for hard drive integrity when it was previously shut down improperly. Sometimes another program adds itself to this

value, causing a problem. For more information about this situation, see the Microsoft Knowledge Base article 151376, “How to Disable Autochk If It Stops Responding During Reboot” at support.microsoft.com.

▲ HKLM\System\CurrentControlSet\Control\Session Manager

Here is an assorted list of registry keys that have all been known to cause various problems at startup. Remember, before you delete a program entry from one of these keys, research the program filename so that you won't accidentally delete something you want to keep:

- ▲ HKCU\Software\Microsoft\Command
- ▲ HKCU\Software\Microsoft\Command Processor\AutoRun
- ▲ HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup
- ▲ HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\load
- ▲ HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
- ▲ HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\System
- ▲ HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Us
- ▲ HKCR\batfile\shell\open\command
- ▲ HKCR\comfile\shell\open\command
- ▲ HKCR\exefile\shell\open\command
- ▲ HKCR\htafile\shell\open\command
- ▲ HKCR\piffile\shell\open\command
- ▲ HKCR\scrfile\shell\open\command

MONITOR THE STARTUP PROCESS

If you keep the startup process clean, you are more likely to keep Windows performing well. You can use several third-party tools to monitor any changes to startup. A good one is WinPatrol by BillP Studios (www.winpatrol.com). Download and install the free program to run in the background to monitor all sorts of things, including changes to the registry, startup processes, Internet Explorer settings, and system files. In Figure 14-72, you can see how WinPatrol gave an alert when it detected that Adobe Update Manager was placing an entry in the registry to launch at startup to update the Adobe software. WinPatrol displays a little black Scotty dog in the notification area of the taskbar to indicate it's running in the background and guarding your system. Also, many antivirus programs monitor the startup process and inform you when changes are made.

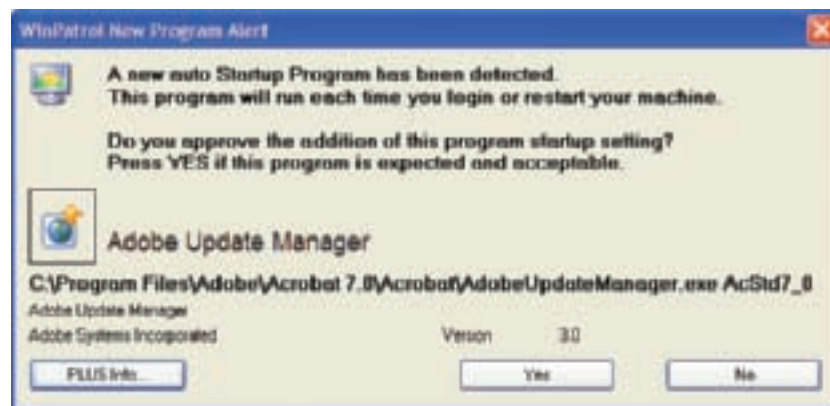


Figure 14-72 WinPatrol by BillP Studios alerts you when the startup process is about to be altered
Courtesy: Course Technology/Cengage Learning

>> CHAPTER SUMMARY

- ▲ Task Manager (Taskmgr.exe) lets you view services and other running programs, CPU and memory performance, network activity, and user activity. It is useful to stop a process that is hung.
- ▲ The MSconfig (Msconfig.exe) tool can be used to temporarily disable startup processes to test for performance improvement and find a startup program causing a problem.
- ▲ The Services console (Services.msc) is used to manage services. When and if a service starts can be controlled from this console.
- ▲ The Computer Management console (Compmgmt.msc) contains a group of Windows administrative tools useful for managing a system.
- ▲ The Microsoft Management Console (MMC) can be used to build your own custom consoles from available snap-ins.
- ▲ Event Viewer (Eventvwr.msc) is a console that displays a group of logs kept by Windows useful for troubleshooting problems with software and hardware and also audits Windows security.
- ▲ The Vista Reliability and Performance Monitor (Perfmon.msc) and the XP Performance Monitor (also called the System Monitor) can be useful when trying to find out the source of a performance drain on the system.
- ▲ The Registry Editor (Regedit.exe) is used to edit the register in real time. There is no way to undo changes you make to the registry. Therefore, you should always make a backup before editing it.
- ▲ The 11 high-level steps to improve Windows performance are (1) routine maintenance, (2) check if hardware can support the OS, (3) check for performance warnings, (4) check the Reliability Monitor, (5) disable indexing for Windows search, (6) disable the Vista Aero glass, (7) disable the Vista sidebar, (8) plug up memory leaks, (9) disable the Vista UAC box, although this is not a recommended best practice, and (10) use ReadyBoost to improve a slow hard drive's performance, and (11) clean up Windows startup.
- ▲ The Windows Vista Experience Index gives a high-level measurement of the overall performance of a system and lists any performance alerts.
- ▲ Disabling the Vista Aero glass and the Vista sidebar can save on system resources and improve performance, especially if memory is low.
- ▲ Memory leaks are caused by poorly written applications that request memory they don't need.
- ▲ Disabling the Vista UAC box is not a recommended best practice because it improves the security of a system.
- ▲ Tools that can be used to investigate and clean up the Windows start process include Safe Mode, MSconfig, Task Manager, Services console, and Task Scheduler.
- ▲ If software does not uninstall using the Vista Programs and Features window or the XP Add or Remove Programs window, you can manually uninstall the software.

>> KEY TERMS

For explanations of key terms, see the Glossary near the end of the book.

| | | |
|---------------------------------------|--|--|
| Computer Management (Compmgmt.msc) | HKEY_LOCAL_MACHINE (HKLM) | snap-ins |
| console | HKEY_USERS (HKU) | System Configuration Utility (Msconfig.exe) |
| Data Collector Sets | Microsoft Management Console (MMC) | Task Manager (Taskmgr.exe) |
| Event Viewer (Eventvwr.msc) | Perfmon.msc | Task Scheduler |
| HKEY_CLASSES_ROOT (HKCR) | ReadyBoost | Vista Upgrade Advisor |
| HKEY_CURRENT_CONFIG (HKCC) | registry | Windows Experience Index |
| HKEY_CURRENT_USER (HKCU) | Registry Editor (Regedit.exe) | |
| | Reliability and Performance Monitor | |

>> REVIEWING THE BASICS

- List four ways to start Task Manager.
- If a program is not responding, how can you stop it?
- If a program is using too much of system resources and bogging down other applications, what can you do to fix the problem?
- How can you get a list of users currently logged onto the computer?
- What is the program filename and extension of the System Configuration utility?
- What tool in Windows Vista, used to temporarily disable a startup program, is not available in Windows XP?
- If a nonessential service is slowing down startup, how can you permanently disable it?
- What should be the startup type of a service that should not load at startup but might be used later after startup? What tool can you use to set the startup type of a service?
- List three snap-ins that can be found in both the Windows Vista and Windows XP Computer Management windows that are used to manage hardware and track problems with hardware.
- What is the file extension of a console that is managed by Microsoft Management Console?
- What are the program filename and extensions of the Microsoft Management Console?
- Which log in Event Viewer would you use to find out about attempted logins to a computer?
- Which log in Event Viewer would you use if you suspect a problem with the hard drive?
- What is the program filename and extension of the Reliability and Performance Monitor?
- What is the path to the Ntuser.dat file in Windows Vista?
- How is the Ntuser.dat file used?
- Which registry key contains information that Device Manager uses to display information about hardware?
- What tool in Windows XP do you use to back up the system state?

19. What is the Vista tool that can give you a quick report of the overall performance of the system?
20. To improve Windows performance, you decide to disable the indexer used for Windows search. Will Windows search still work?
21. What three indicators in Task Manager can be used to find which program has a memory leak?
22. Why is it best to not disable the UAC box?
23. What key do you press at startup to load the system in Safe Mode?
24. If performance improves when Windows is loaded in Safe Mode, what can you conclude?
25. If performance does not improve when Windows is loaded in Safe Mode, what can you conclude?
26. When using MSconfig to stop startup services, including Microsoft services, which service should you not stop so that restore points will not be lost?
27. What is the purpose of the Windows Installer service?
28. In what folder does Task Scheduler keep scheduled tasks?
29. In what folder is most installed software likely to be found?
30. What is the name of the Control Panel applet used to uninstall software in Vista?

>> THINKING CRITICALLY

1. You need to install a customized console on 10 computers. What is the best way to do that?
 - a. When installing the console on the first computer, write down each step to make it easier to do the same chore on the other nine.
 - b. Create the console on one computer and copy the .mmc file to the other nine.
 - c. Create the console on one computer and copy the .msc file to the other nine.
2. What is the name of the program that you can enter in the Vista Start Search box to execute Event Viewer? What is the process that is running when Event Viewer is displayed on the screen? Why do you think the running process is different from the program name?
3. When cleaning up the startup process, which of these should you do first?
 - a. Run MSconfig to see what processes are started.
 - b. If an error message is displayed when you start Windows, investigate the message.
 - c. After you have launched several applications, use Task Manager to view a list of running tasks.
 - d. Run the Defrag utility to optimize the hard drive.
4. Using the Internet, investigate each of the following startup processes. Identify the process and write a one-sentence description.
 - a. Acrotray.exe
 - b. Ieuser.exe

5. Using Task Manager, you discover an unwanted program that is launched at startup. Of the items listed below, which ones might lead you to the solution to the problem? Which ones would not be an appropriate solution to the problem? Explain why they are not appropriate.
 - a. Look at the registry key that launched the program to help determine where in Windows the program was initiated.
 - b. Use Task Manager to disable the program.
 - c. Search Task Scheduler for the source of the program being launched.
 - d. Use MSconfig to disable the program.
 - e. Search the startup folders for the source of the program.

>> HANDS-ON PROJECTS

PROJECT 14-1: Researching Running Processes

Boot to the Windows desktop and then use Task Manager to get a list of all the running processes on your machine. Use the Vista Snipping Tool to save and print the Task Manager screens showing the list of processes. Next, boot the system into Safe Mode and use Task Manager to list running processes. Which processes that were loaded normally are not loaded when the system is running in Safe Mode?

PROJECT 14-2: Monitoring Startup Items with WinPatrol

1. Using the System Configuration Utility (MSconfig), disable all the non-Windows startup items. Restart your computer.
2. Download and install WinPatrol from www.winpatrol.com.
3. Using the System Configuration Utility (MSconfig), enable all of the disabled startup items and restart the computer.
4. Are the startup programs able to start? What messages are displayed on the screen?

PROJECT 14-3: Practicing Launching Programs at Startup

Do the following to practice launching programs at startup, listing the steps you took for each activity:

1. Configure Scheduled Tasks to launch Notepad each time the computer starts and any user logs on. List the steps you took.
2. Put a shortcut in a startup folder so that any user launches a command prompt window at startup.
3. Restart the system and verify that both programs are launched. Did you receive any errors?
4. Remove the two programs from the startup process.

PROJECT 14-4: Practicing Manually Removing Software

To practice your skills of manually removing software, install WinPatrol from www.winpatrol.com. (If you did Project 14-2, the software is already installed.) Then, following directions in the chapter, manually remove the software, listing the steps you used. After you have manually removed the software, reboot the system. Did you get any error messages?

PROJECT 14-5: Editing and Restoring the Registry

Practice editing and restoring the registry by doing the following to change the name of the Recycle Bin on the Windows desktop:

1. Using the Registry Editor, export the registry key `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer` to an export file stored on the desktop. The data entry for this key is set to “Value not set,” which means the default name, Recycle Bin, is used.
2. To change the name of the Recycle Bin on the Windows Vista desktop for the currently logged-on user, click the following subkey, which holds the name of the Recycle Bin: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\645FF040-5081-101B-9F08-00AA002F954E`.
3. To enter a new name for the Recycle Bin, in the right pane, double-click **Default**. The Edit String box appears. The Value data text box in the dialog box should be empty. If a value is present, you selected the wrong value. Check your work and try again.
4. Enter a new name for the Recycle Bin, for example, “Trash Can.” Click **OK**.
5. Move the Registry Editor window so that you can see the Recycle Bin on the desktop. Don’t close the window.
6. Right-click the desktop and select **Refresh** on the shortcut menu. The name of the Recycle Bin changes.
7. To restore the name to its default value, in the Registry Editor window, again double-click the name of the value, delete your entry, and click **OK**.
8. To verify the change is made, refresh the Windows desktop. The Recycle Bin name should return to its default value.
9. Exit the Registry Editor and then delete the exported registry key stored on the desktop.
10. From these directions, you can see that changes made to the registry take effect immediately. Therefore, take extra care when editing the registry. If you make a mistake and don’t know how to correct a problem you create, then you can restore the key that you exported by exiting the Registry Editor and double-clicking the exported key.

PROJECT 14-6: Using the Microsoft Management Console

Using the Microsoft Management Console, follow the step-by-step directions in the chapter to create a customized console. Put two snap-ins in the console: Device Manager and Event Viewer. Store a shortcut to your console on the Windows desktop.

PROJECT 14-7: Finding Windows Utilities

The following table lists some important Windows utilities covered in this chapter. Fill in the right side of the table with the filename and path of each utility. (*Hint:* You can use Windows Explorer or Search to locate files.)

| Utility | Filename and Path in Windows Vista | Filename and Path in Windows XP |
|-------------------------------------|------------------------------------|---------------------------------|
| Task Manager | | |
| System Configuration Utility | | |
| Services Console | | |
| Computer Management | | |
| Microsoft Management Console | | |
| Event Viewer | | |
| Reliability and Performance Monitor | | |
| Registry Editor | | |

>> REAL PROBLEMS, REAL SOLUTIONS**REAL PROBLEM 14-1:** Problems Starting Windows XP

Tim, a coworker who uses many different applications on his Windows XP system, complains to you that his system is very slow starting up and responding when he loads and unloads applications. You suspect the system is loading too many services and programs during startup that are sucking up system resources. What do you do to check for startup processes and eliminate the unnecessary ones? If you have access to a Windows XP system that needs this type of service, test your answers on this system. Write down at least 10 things you should do or try that were discussed in the chapter to speed up a sluggish Windows XP installation.

REAL PROBLEM 14-2: Cleaning Up Startup

Using a computer that has a problem with a sluggish startup, apply the tools and procedures you learned in this chapter to clean up the startup process. Take detailed notes of each step you take and the results. (If you are having a problem finding a computer with a sluggish startup, consider offering your help to a friend, a family member, or a nonprofit organization.)

This page intentionally left blank