Chapter 15

Maintaining and Optimizing Windows 7

If you want an optimized Windows 7 installation, you must monitor its reliability and performance. Windows 7 comes with many tools to track memory, processor activity, the disk subsystem, and the network subsystem, as well as other computer subsystems. Tools are available to provide baseline statistics for each of the subsystems so that you can track changes over time and better evaluate issues that pertain to the Windows 7 machine and make changes to proactively affect declining performance.

In this chapter, you'll learn how to monitor, maintain, troubleshoot, and optimize Windows 7 using the following utilities: Performance Monitor, Reliability Monitor, System Information, Task Manager, several system tools, System Configuration, Task Scheduler, and Event Viewer. Each of these tools provides information about the operating system and hardware status.

Windows 7 has a full backup and restore application to allow you to maintain a backup copy of any of the Windows 7 component files and data files that are considered critical to the operation of your day-to-day business. You can use the backup of the files to restore them if they become unusable (corrupted, deleted, or even modified and you want to go back to the original).

You'll also learn about system recovery and troubleshooting. In this chapter, we'll show you how to safeguard your computer and how to recover from a disaster. The benefit of having a disaster recovery plan is that when you expect the worst to happen and are prepared for it, you can easily recover from most system failures.

In this chapter, you'll learn how to:

◆ Use Performance Monitor to view CPU usage

◆ Maintain Windows 7 with system tools

◆ Schedule a task to launch daily

◆ Back up critical data files

Understanding Windows 7 Performance Optimization

Before you can optimize the performance of Windows 7, you must monitor the operating systems' critical subsystems to determine how each is currently performing and what (if anything) is causing system bottlenecks that negatively affect performance. Windows 7 ships with many tools that you can use to monitor system performance. The monitoring tools enable you to assess your server's current health and determine what requirements to improve its present condition are available.

Performance Monitor is a tool that you can used to perform the following tasks:

◆ Create baselines.

◆ Identify system bottlenecks.

◆ Determine trends.

◆ Test configuration changes or tuning efforts.

◆ Create alert thresholds.

Creating Baselines

A baseline is a snapshot of how your system is currently performing. Suppose that your computer's hardware has not changed over the last six months, but the computer seems to be performing more slowly now than it did six months ago. If you have been using the Performance Monitor utility and taking baseline logs, as well as noting the changes in your workload, you can more easily determine what resources are causing the system to slow down. If you simply note Windows 7 seems to be running more slowly, without any supporting statistics, you will not have any idea what is causing your issues.

You should create baselines at the following times:

◆ When the system is first configured, without any load

◆ At regular intervals of typical usage

◆ Whenever any changes are made to the system's hardware or software configuration

Baselines are particularly useful for determining the effect of changes that you make to your computer. For example, if you are adding more memory to your computer, you should take baselines before and after you install the memory to determine the effect of the change. Along with hardware changes, system configuration modifications can affect your computer's performance, so you should create baselines before and after you make any changes to your Windows 7 configuration.

MAKING CHANGES TO WINDOWS 7

For the most part, Windows 7 is a self-tuning operating system. If you decide to tweak the operating system, take baselines before and after each change. If you don't notice a performance gain after the tweak, consider returning the computer to its original configuration; some tweaks might cause more problems than they solve.

IDENTIFYING SYSTEM BOTTLENECKS

A bottleneck is a system resource that is inefficient compared with the rest of the computer system as a whole. The bottleneck can cause the rest of the system to run slowly.

You need to pinpoint the cause of a bottleneck to correct it. Consider a system that has a Pentium 4 3.0 GHz processor with 1024 MB of RAM. You might consider changing to a more advanced processor. However, if your applications are memory-intensive and lack of memory is your bottleneck, upgrading your processor will not eliminate the bottleneck.

By using Performance Monitor, you can measure the performance of the various parts of your system, which allows you to identify system bottlenecks in a scientific manner. You will learn how to set counters to monitor your network and spot bottlenecks in the ''Managing System Performance'' section later in this chapter.

DETERMINING TRENDS

Many of us tend to manage situations reactively instead of proactively. With reactive management, you focus on a problem when it occurs; with proactive management, you take steps to avoid the problem before it happens. In a perfect world, all management would be proactive. Performance Monitor is a great tool for proactive network management. If you are creating baselines on a regular basis, you can identify system trends. For example, if you notice average CPU utilization increasing 5 percent every month, you can assume that within the next six months, you're going to have a problem. Before performance becomes so slow that your system is not responding, you can upgrade the hardware.

Testing Configuration Changes or Tuning Efforts

When you make configuration changes or tune your computer, you might want to measure the effects of those changes. Performance Monitor allows you evaluate your machines' subsystems before changes are made and while you are in the process of making changes. When you make configuration changes, the following recommendations apply:

Make only one change at a time.   If you are making configuration changes for tuning, and you make multiple changes at one time, it is difficult to quantify the effect of each individual change. In addition, some changes might have a negative impact that, if you have made multiple changes, may be difficult to identify.

Repeat monitoring with each individual change you make.   This will help you determine whether additional tuning is required.

As you make changes, check the Event Viewer event log files.   Some performance changes will generate events within Event Viewer that should be reviewed. Event Viewer is covered in more detail in the ''Using Event Viewer'' section later in this chapter.

Using Alerts for Problem Notification

Performance Monitor provides another tool for proactive management in the form of alerts. Through data collector sets, you can specify alert thresholds (when a counter reaches a specified value) and have the utility notify you when these thresholds are reached. For example, you could specify that if one of your hard drives logical disks has less than 10 percent of free space, you want to be notified. Once alerted, you can add more disk space or delete unneeded

files before you run out of disk space. Setting up Performance Monitor and using its capabilities is a boon to you as an administrator to keep Windows 7 optimized.

Optimizing Windows 7 with Performance Monitor

The Performance Monitor utility is used to measure the performance of a local or a remote computer on the network. Performance Monitor enables you to do the following:

◆ Collect data from your local computer or remote computers on the network. You can collect data from a single computer or multiple computers concurrently.

◆ View data as it is being collected in real time, or historically from collected data.

◆ Have full control over the selection of what data will be collected by selecting which specific objects and counters will be collected.

◆ Choose the sampling parameters that will be used, meaning the time interval that you want to use for collecting data points and the time period that will be used for data collection.

◆ Determine the format in which data will be viewed: inline, histogram bar, or report views.

◆ Create HTML pages for viewing data.

◆ Create specific configurations for monitoring data that can then be exported to other computers for performance monitoring.

VIEWING PERFORMANCE MONITOR ON REMOTE MACHINES

To view data on remote computers, you need to have administrative rights to the remote computer, the Remote Registry Service must be enabled and running on the remote computer, and Windows Firewall must be set to allow the connection.

Through Performance Monitor, you can view current data or data from a log file. When you view current data, you are monitoring real-time activity. When you view data from a log file, you are importing a log file from a previous session.

To access Performance Monitor, choose Start ➢ Control Panel ➢ System And Security ➢ Administrative Tools, and then double-click Performance Monitor; or you can type **perfmon** in the Start menu's search box. Figure 15.1 shows the main Performance Monitor window when it is initially opened without configuration.

When you first start Performance Monitor, the Overview Of Performance Monitor page is displayed. This page gives a quick snapshot of what resources are being used in your computer in the System Summary pane. Notice the four initial resources tracked are Memory, Network Interface, Physical Disk, and Processor Information. You can view detailed information about each resource by clicking the Open Resource Monitor link.
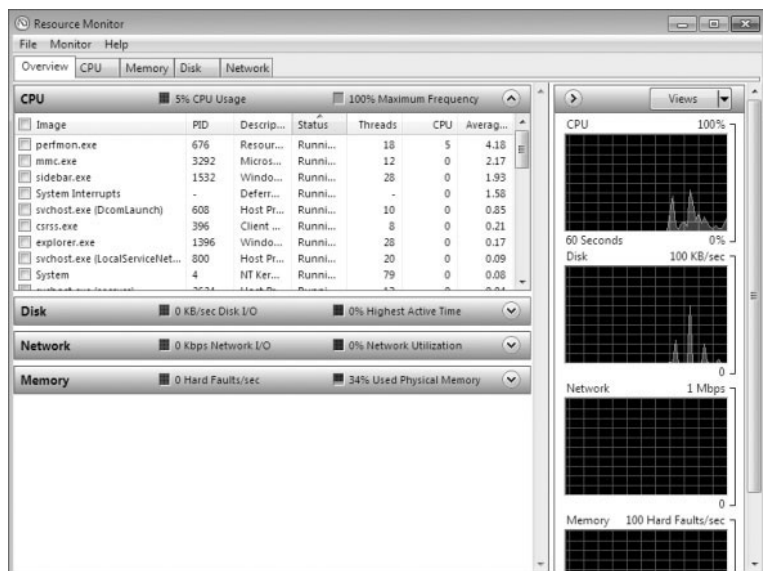
Using Resource Monitor

The Resource Monitor window was integrated into the Reliability and Performance utility of Windows Vista, but has been given its own dialog box in Windows 7. Figure 15.2 shows the Resource Monitor dialog box (which you can open from Performance Monitor or by typing **Resource Monitor** (or **resmon**) into the Start menu's search box.

FIGURE 15.1
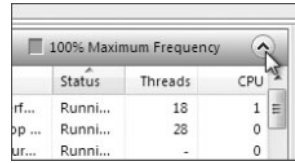Windows 7's
Performance Monitor



FIGURE 15.2
Windows 7's Resource
Monitor

The Overview tab of the Resource Monitor dialog box is open by default and gives you a fair amount of detail. The main window provides an overview of the four major subsystems monitored by default (CPU, Disk, Network, and Memory). You expand or compress each of the four items by clicking the arrow in the left of the item title bar, as shown in Figure 15.3. For example, if you want to view details about the memory being used by the processes of Windows 7, click the arrow to expand Memory and you can view each process, process ID, and memory allocation by physical, shared, and private allotment.

FIGURE 15.3
Expand or collapse
Resource Monitor items.

The other tabs of the Resource Monitor dialog box offer detailed information about each of the major subsystems of Windows 7. The CPU tab displays the individual processes currently running on the machine, the process IDs (PIDs), a brief description, the running status of the process, how many threads the process is running, current CPU utilization, and average CPU utilization. You can also expand the Services, Associated Handles, and Associated Module items for more detail on each of these items. The CPU tab, shown in Figure 15.4, also offers a graphical representation of real-time statistics for CPU total usage by percentage and Service CPU usage as a percentage on the right of the screen.
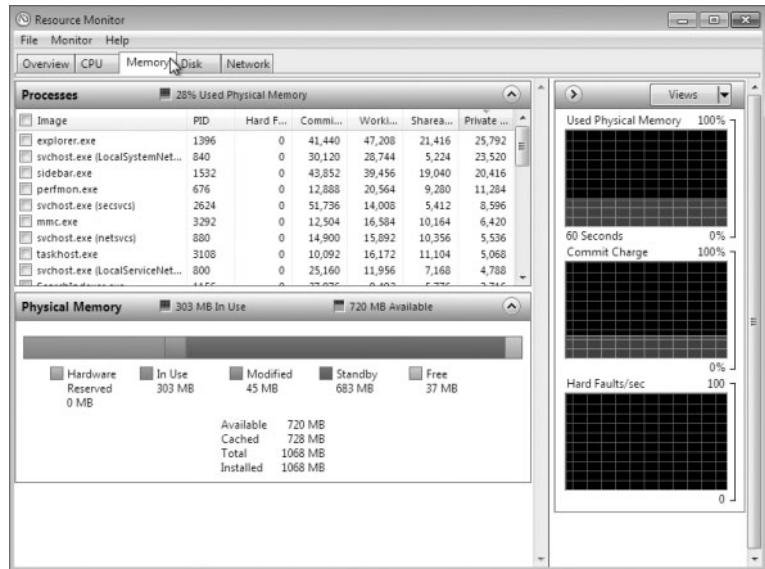
FIGURE 15.4
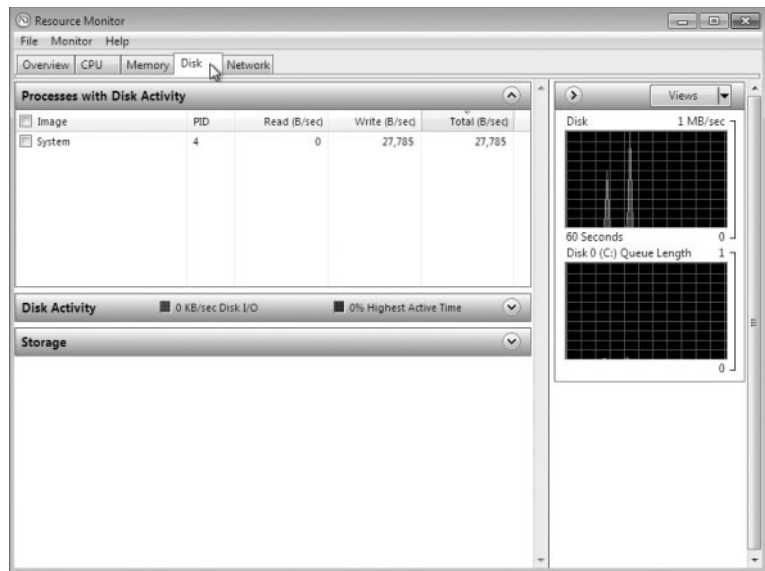The CPU tab of Resource
Monitor
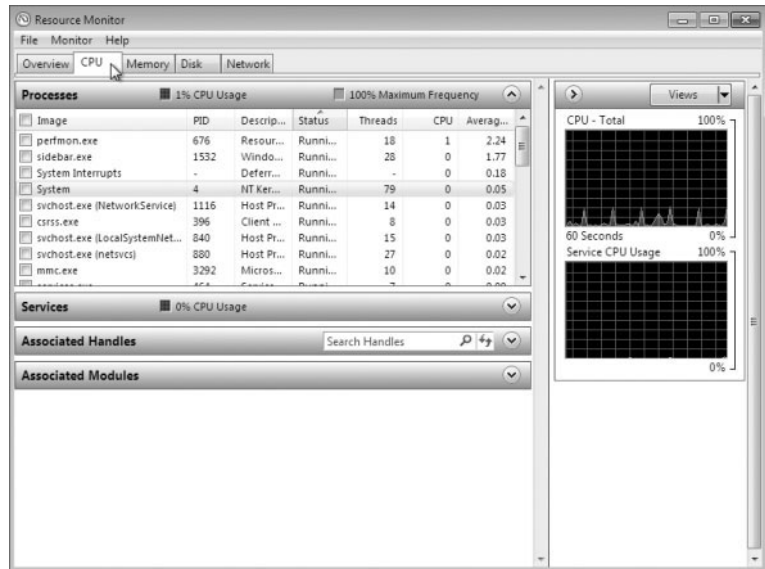
The Memory tab of Resource Monitor shows the process information as displayed on the CPU tab with an overview of memory allocation in the form of a graphical representation. The right side of the display also shows you real-time information of the physical memory and the currently allocated memory, called the Committed Charge and Hard Faults/Sec (the number of memory accesses that are not actually in RAM, but in a page file waiting to be used). The Memory tab is shown in Figure 15.5.

The Disk tab of Resource Monitor (Figure 15.6) is used to display the disk activity of your machine. The items available to view are Processes With Disk Activity, Disk Activity, and Storage. The Disk tab includes a real-time graphical representation of disk transfer in KB/Sec and disk queue length (the amount of transfer currently waiting for transfer to RAM for processing).

FIGURE 15.5
The Memory tab of
Resource Monitor

FIGURE 15.6
The Disk tab of Resource
Monitor

The Network tab of Resource Monitor (Figure 15.7) shows network utilization as well as network protocol information. The items available for detailed information include Processes With Network Activity, Network Activity, TCP Connections, and Listening Ports. We've had this information available to us in previous versions of Windows, but this is one convenient location for a slew of useful network information. The Network tab offers a huge amount of useful network information (we have opened the Listening Ports item in the figure) as well as the real-time graphical information for network data transfer, open TCP connections, and local

area connection usage as a percentage. You can view any of these counters in Resource Monitor as well as Performance Monitor. The key counter value guidelines (what's good/what's not good) are included in the ''Key Counters'' sections later in this chapter.

FIGURE 15.7
The Network tab of
Resource Monitor
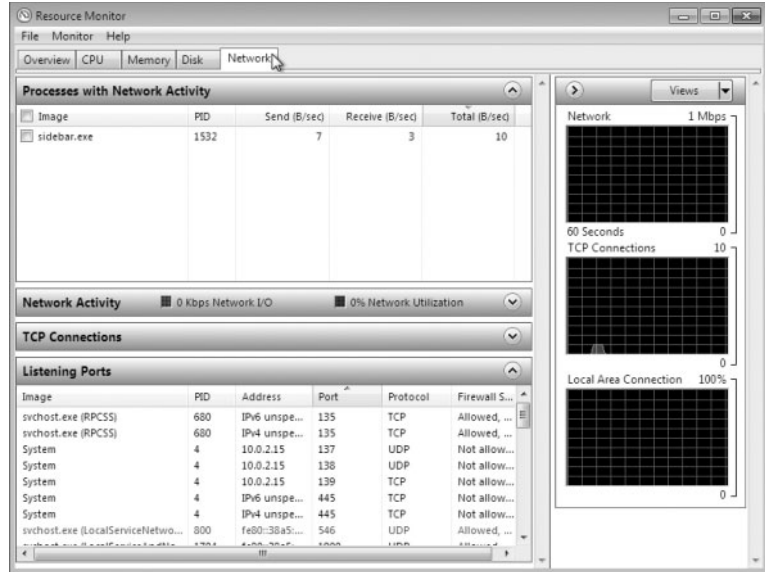
 Real World Scenario

THE GREAT NETWORK TAB IN RESOURCE MONITOR

One of the authors is a packet sniffer and network utilization geek and has been for some time. He constantly talks with other administrators about resources being used in their servers and client machines that are associated with many network attributes. It's always important for him to see just which applications are using the network in terms of the ports they have open on his machine. He uses TCPView on a regular basis (downloadable from `http://technet.microsoft.com`) and has even been known to fire up Netstat (the ever popular command-line utility that shows network status) to see what's happening. Making the association to the ports open, the processes using resources, the applications associated with the ports and processes and just how much bandwidth is being used has always had him looking between applications and utility outputs. The author has a regimen that he uses and recommends to administrators to monitor this information, but Resource Monitor's Network tab has now consolidated this information into one convenient spot with a regular data display as well as real-time graphical views. This author returns to Resource Monitor time and time again to see what his Windows 7 machine is doing and has come across many of his colleagues doing the same thing. If you've ever considered looking at the connections being made into or out of your computer, you will love the Network tab of Resource Monitor (and the other tabs are pretty good too).

For monitoring system activity other than what is provided by the Resource Overview and Resource Monitor, you must use more of the Performance Monitor features.

Utilizing Customized Counters in Performance Monitor

You can add numerous counters from any of the subsystems within Windows 7. To access the configurable Performance Monitor window, select the Performance Monitor item in the left pane, as shown in Figure 15.8.

FIGURE 15.8
Customizable Performance Monitor window
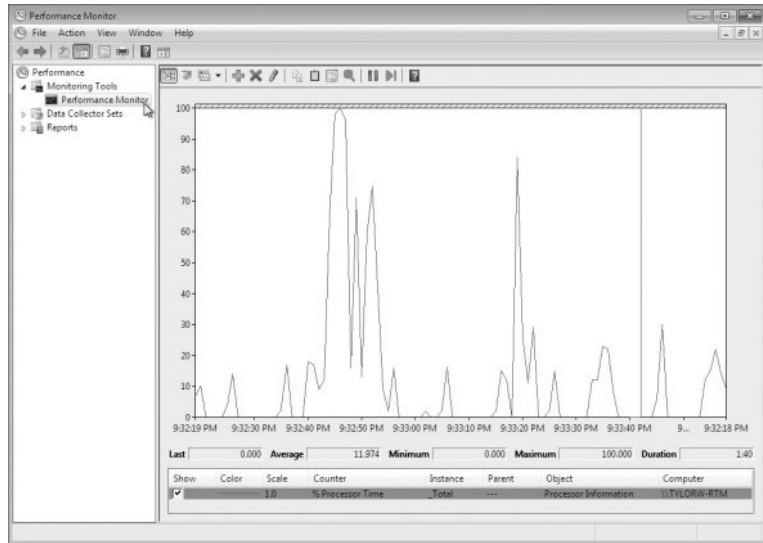
Customizable counters are listed at the bottom of the Performance Monitor window. By default, only the % Processor Time counter is tracked for the local computer. The fields just above the counter list will contain data based on the counter that is highlighted in the list, as follows:

Last   Displays the most current data

Average   Shows the average of the counter

Minimum   Shows the lowest value that has been recorded for the counter

Maximum   Shows the highest value that has been recorded for the counter

**Duration**   Shows how long the counter has been tracking data

Before we add counters to Performance Monitor, let's discuss the three Performance Monitor views.

SELECTING THE APPROPRIATE VIEW

Click the Change Graph Type button on the Performance Monitor toolbar to see your data in one of three views, as shown in Figure 15.9.

Line View   The line view is Performance Monitor's default view. It's useful for viewing a small number of counters in a graphical format. The main advantage of line view is that you can see how the data has been tracked during the defined time period.

FIGURE 15.9
Change Graph Type
button
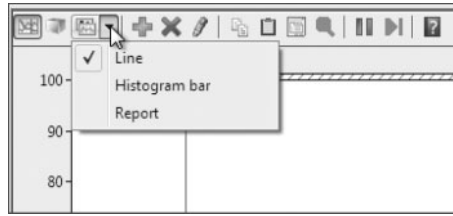
Histogram View   The histogram view, shown in Figure 15.10, shows the Performance Monitor data in a bar graph. This view is useful for examining large amounts of data. However, it shows performance only for the current period. You do not see a record of performance over time, as you do with the line view.

FIGURE 15.10
Performance Monitor
histogram view
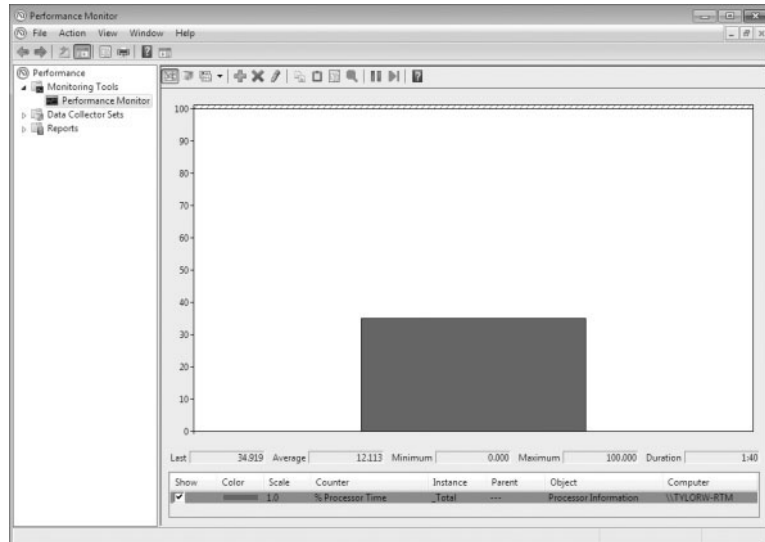
Report View   The report view, shown in Figure 15.11, offers a logical text-based report of all the counters that are being tracked through Performance Monitor. Only the current session's data is displayed. The advantage of report view is that it allows you to easily track large numbers of counters in real time. It is important to note that when you view data in real-time format, the data can appear skewed as applications and processes are started. It is typically more useful to view data as an average over a specified interval.
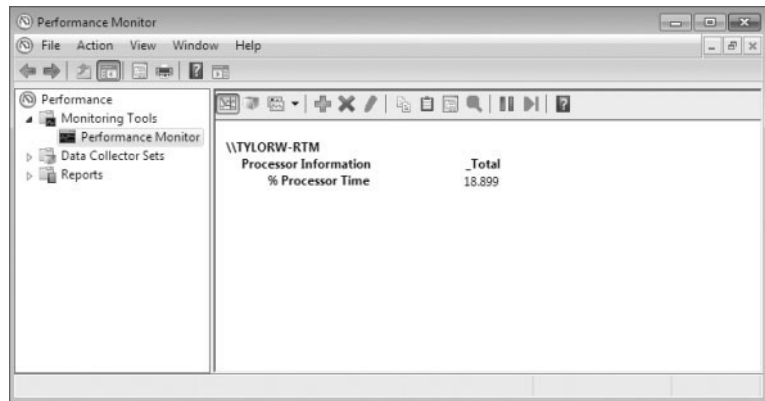
ADDING COUNTERS

As mentioned previously, you can add customized counters to Performance Monitor to track data.

Follow these steps to add counters:

1. In Performance Monitor, click the Add button on the toolbar, which looks like a green plus sign (+). This brings up the Add Counters dialog box.

SEEING DETAILS ABOUT COUNTER OBJECTS

To see information about a specific counter, in the Add Counters dialog box select the counter from the list and select the Show Description check box beneath the list on the left. Performance Monitor displays detail text regarding the highlighted counter.

2. In the Add Counters dialog box, ensure that the Select Counters From The Computer drop-down list displays <Local Computer> so that you can monitor the local computer. Alternatively, to select counters from a specific computer, pick a computer from the drop-down list.

MONITORING REMOTELY

You can monitor remote computers if you have administrative permissions. This option is useful when you do not want the overhead of the Performance Monitor graphics running on the computer you are trying to monitor. Although Microsoft has minimized the effect of running Performance Monitor, even without the graphical display, there will be minimal impact of running the data collection of Performance Monitor within the counter statistics. You can connect to another machine by selecting Connect To Another Computer in the context window of Performance within the Performance Monitor window as shown here:
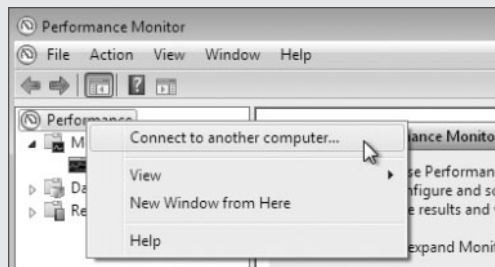
3. Select a performance object from the drop-down list. All Windows 7 system resources are tracked as performance objects, such as Cache, Memory, Paging File, Process, and Processor.

VIEWING COUNTER OBJECTS IN PERFORMANCE MONITOR

All the objects together represent your total system. Some performance objects exist on all Windows 7 computers; other objects appear only if specific processes or services are running. For example, if you want to track the physical disk's level of activity, choose the PhysicalDisk performance object.

4. Select the counter or counters within the performance object that you want to track. Each performance object has an associated set of counters. Counters are used to track specific information regarding a performance object. For example, the PhysicalDisk performance object has a % Disk Time counter, which will tell you how busy a disk has been in servicing read and write requests. PhysicalDisk also has % Disk Read Time and % Disk Write Time counters, which show you what percentage of disk requests are read requests and what percentage are write requests, respectively.

5. Select <All Instances> to track all the associated instances or pick specific instances from the list box.

USING INSTANCES WITHIN PERFORMANCE MONITOR

An instance is a mechanism that allows you to track the performance of a specific object when you have more than one item associated with a specific performance object. For example, suppose your computer has two physical drives. When you track the PhysicalDisk performance object, you can track one or both of your drives. If a counter has more than one instance, you can monitor the sum of all of the instances by selecting the _Total option.

6. Click the Add button to add the counters for the performance object.

7. Repeat steps 2 through 6 to specify any additional counters you want to track. When you finish, click OK.

After you've added counters, you can select a specific counter by highlighting it in Performance Monitor. To highlight a counter, click it and then click the Highlight button (which looks like a highlighter) on the Performance Monitor toolbar, or select the counter and press Ctrl+H.

To stop showing data for a counter, deselect the check box under Show for that counter. To remove a counter, highlight it in Performance Monitor and click the Delete button on the toolbar. The Delete button looks like a red X.

MANAGING PERFORMANCE MONITOR PROPERTIES

To configure the Performance Monitor properties, click the Properties button on the Performance Monitor toolbar and the Performance Monitor Properties dialog box opens, as shown in Figure 15.12.

FIGURE 15.12
Performance
Monitor Counter
Properties
dialog box
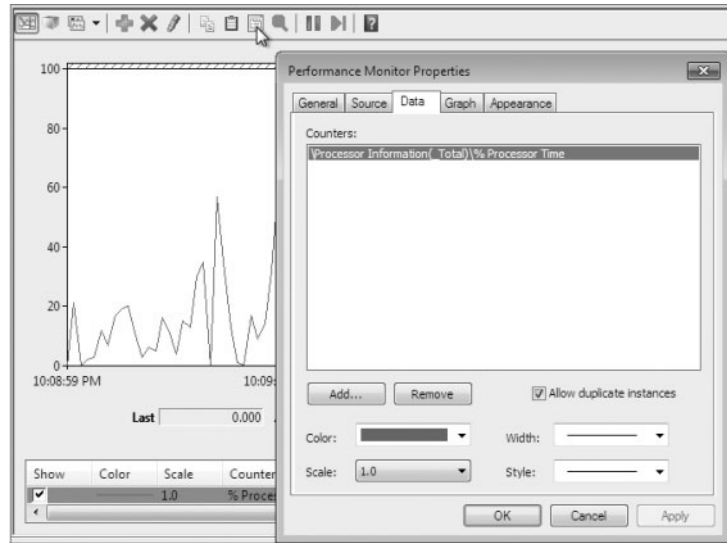
The Performance Monitor Properties dialog box has the following five tabs:

General Tab The General tab of the Performance Monitor Properties dialog box, as shown in Figure 15.13, contains the following options:

◆ The display elements that will be used — legend, value bar, and/or toolbar

◆ The data that will be displayed — default (for reports or histograms, this is current data; for logs, this is average data), current, minimum, maximum, or average

◆ How often the data is updated, in seconds

FIGURE 15.13
The General tab of the
Performance Counter
Properties dialog box

Source Tab   The Source tab, shown in Figure 15.14, allows you to specify the data source. This can be current activity, or it can be data that has been collected in a log file or database. If you import data, you can specify the time range that you want to view.
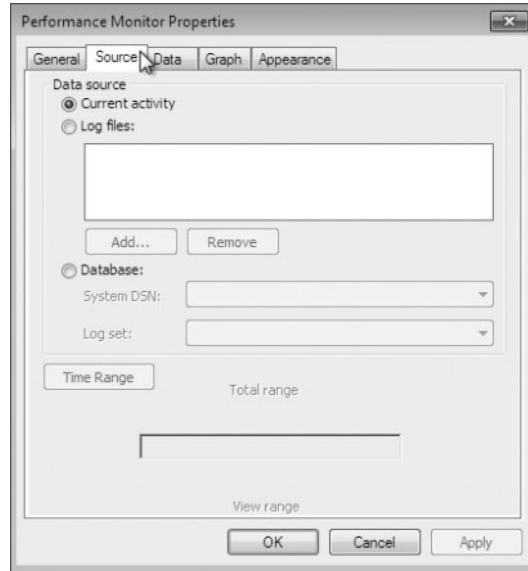
Data Tab   The Data tab (the default tab that is active when the properties window opens, as shown in Figure 15.12 earlier) lets you specify the counters that you want to track. You can add and remove counters by clicking the Add and Remove buttons. You can also select a specific counter and define the color, scale, width, and style that are used to represent the counter in the graph.

Graph Tab   The Graph tab, shown in Figure 15.15, contains the following options, which you can apply to the line or histogram bar view:

◆   Whether the data will scroll or wrap (line view only)

◆   A title

◆   A vertical axis label

◆   Whether you will show a vertical grid, a horizontal grid, vertical scale numbers, and/or time axis labels

◆   The minimum and maximum numbers for the vertical scale

Appearance Tab   The Appearance tab of the Performance Monitor Properties dialog box, shown in Figure 15.16, has options for customizing the colors and fonts used in the Performance Monitor display.

After you have set counters and viewed them in real time, you might be interested in collecting the data over time and saving it to a file for maintaining a baseline of data for comparison. You do this in Performance Monitor by using data collector sets.

FIGURE 15.15
The Graph tab of the Performance Counter Properties dialog box
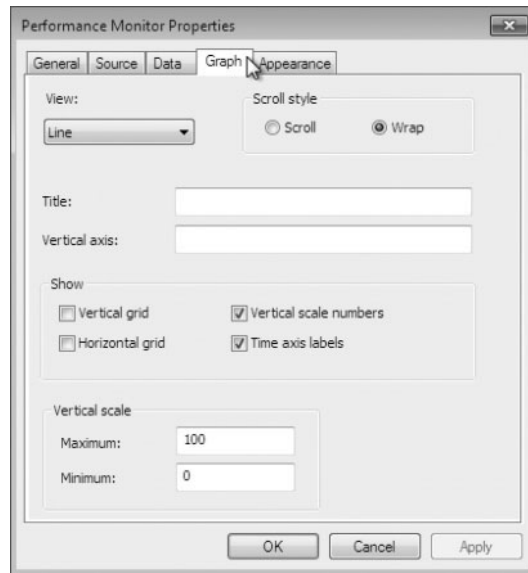

FIGURE 15.16
The Appearance tab of the Performance Counter Properties dialog box
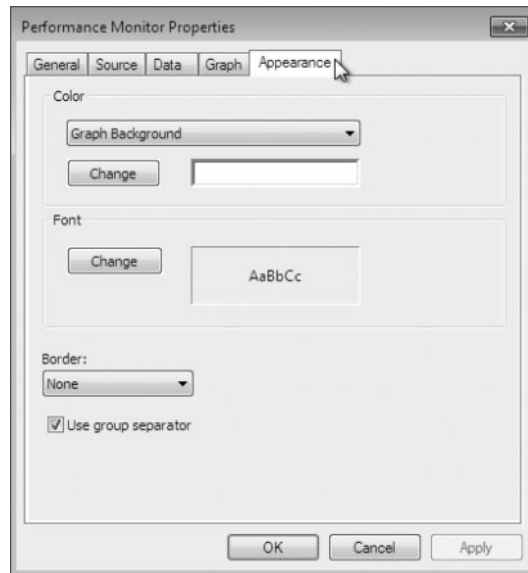
Managing Performance Monitor Data with Collector Sets

The Data Collector Sets portion of Performance Monitor is shown in Figure 15.17. Data collector sets are used to collect data into a log so that the data can be reviewed and saved for comparison at a later date (a process called base lining). You can view the log files with Performance Monitor, as described in the previous section ''Managing Performance Monitor Properties.''

FIGURE 15.17
Configuring
Performance
Monitor data
collector sets
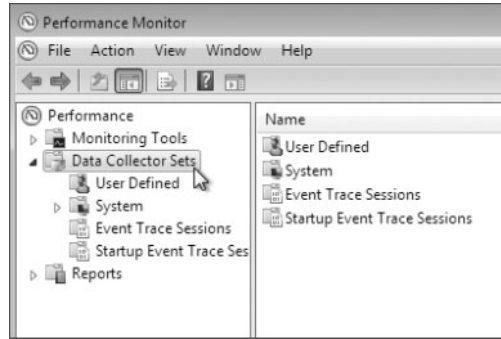
When you create a data collector set, right-click User Defined and choose New Data Collector Set from the context menu to launch the Create New Data Collector Set Wizard. You can let Windows 7 use a standard data collector set or you can define data logs from the following options:

◆ Performance counters

◆ Event trace data

◆ System configuration information

There are two built-in data collector sets that track multiple counters for system diagnostics and system performance. You can also create your own user-defined data collector sets and save them for later use. You can view the reports from these data collector sets within the Reports folder in Performance Monitor.

CREATING A USER-DEFINED DATA COLLECTOR SET

Performance counter logs record data about hardware usage and the activity of system services. You can configure logging to occur manually or on a predefined schedule.

Perform the following steps to create a data log:

1. Expand Data Collector Sets, right-click User Defined, select New, and select Data Collector Set from the pop-up menu.

2. In the Create New Data Collector Set dialog box that appears, type a name for the collector set and choose whether to create the set from a template or to create it manually; then click the Next button.

3. If you chose to create the set from a template, follow the prompts to create the set. After the set is created, you can modify it.

If you chose to create the set manually, you are asked whether you want to create data logs or a performance counter alert. Data logs can consist of the following types of data:

◆ Performance counters

◆ Event trace data

◆ System configuration information

After you select the data you want to collect, click Next.

4. Add the performance counters you want to collect and click Next after each data type.

5. You are asked where to save the data. Browse to the location, click OK, and then click Next.

6. You are asked under which user account the data collector set should run, and whether the data collector set should be edited, started, or saved. After you make your selections, click Finish.

CREATING AN ALERT

Alerts can be generated when a specific counter rises above or falls below a specified value. You can configure alerts to log an entry in the application event log and/or start a data collector set. Creating an alert is similar to creating a performance counter data log except you are required to specify the alert conditions. You create an alert by creating a user-defined collector set and manually specifying counters. In the Create New Data Collector Wizard, you select the Performance Counter Alert radio button. For example, you might configure a performance counter alert that will log an entry whenever the % Free Space counter for C: falls below 5 percent. After you create the alert, you can modify the alert parameters by right-clicking the data collector and selecting Properties.

After you create the data collector sets and set the alerts, you will want to run the sets and save the logs periodically. Reviewing the logs gives you a proactive approach to managing your Windows 7 performance.

Simply creating the logs and saving them is not enough; you need to evaluate the data using previous logs to determine trends that allow you to manage your system's performance.

Managing System Performance

By analyzing data, you can determine whether any resources are placing an excessive load on your computer that is resulting in a system slowdown. The following list gives some of the causes of poor system performance:

◆ A resource is insufficient to handle the load that is being placed upon it, and the component might need to be upgraded, or additional components might be required.

◆ If a resource has multiple instances, the resources might not be evenly balancing the workload, and the workload might need to be balanced over the multiple instances more effectively.

◆ A resource might be malfunctioning. In this case, the resource should be repaired or replaced.

◆ A specific program might be allocated resources improperly or inefficiently, in which case the program needs to be rewritten or replaced by another application.

◆ A resource might be configured improperly and causing excessive resource usage and has to be reconfigured.

You should monitor four main subsystems. Configure counters in your data collector set for each of the following:

◆ The memory subsystem

◆ The processor subsystem

◆ The disk subsystem

◆ The network subsystem

Each subsystem should be examined over time to evaluate Windows 7 performance.

MONITORING AND OPTIMIZING MEMORY

When the operating system needs a program or process, the first place it looks is in physical memory. If the required program or process is not in physical memory, the system looks in logical memory (the page file). If the program or process is not in logical memory, the system then must retrieve the program or process from the hard disk. It can take thousands of times longer to access information from the hard disk than to get it from physical RAM. If your computer is using excessive paging, that is an indication that your computer does not have enough physical memory.

Insufficient memory is the most likely cause of system bottlenecks. If you have no idea what is causing a system bottleneck, memory is usually a good place to start checking. To determine how memory is being used, examine the following two areas:

Physical Memory The physical RAM you have installed on your computer. You can't have too much memory if you are below your operating system's maximum. It's a good idea to have more memory than you think you will need just to be on the safe side. As you've probably noticed, each time you add or upgrade applications, you require more system memory.

Page File Logical memory exists on your hard drive. If you are using excessive paging (swapping between the page file and physical RAM) or hard page faults, it's a clear sign that you need to add more memory.

The first step in memory management is determining how much memory your computer has installed and what the appropriate memory requirements are based on the operating system requirements and the applications and services you are running on your computer.

KEY COUNTERS TO TRACK FOR MEMORY MANAGEMENT

The following are the three most important counters for monitoring memory:

Memory > Available MBytes Memory > Available MBytes measures the amount of physical memory that is available to run processes on the computer. If this number is less than 20 percent of your installed memory, it indicates that you might have an overall shortage of physical memory for your computer, or you possibly have an application that is not releasing memory properly. You should consider adding more memory or evaluating application memory usage.

Memory > Pages/Sec Memory > Pages/Sec shows the number of times the requested information was not in memory and had to be retrieved from disk. This counter's value should be below 20; for optimal performance, it should be 4 or 5. If the number is above 20, you should add memory or research paging file use more thoroughly. Sometimes a high Pages/Sec counter is indicative of a program that is using a memory-mapped file.

Paging File > % Usage Paging File > % Usage indicates the percentage of the allocated page file that is currently in use. If this number is consistently over 70 percent, you might need to add more memory or increase the size of the page file. You should track this counter in conjunction with Available MBytes and Pages/Sec.

These counters work together to show what is happening on your system. Use the Paging File > % Usage counter value in conjunction with the Memory > Available MBytes and Memory > Pages/Sec counters to determine how much paging is occurring on your computer.

Along with memory counters, processor (or CPU) counters are valuable in evaluating Windows 7 performance.

Managing Processor Performance

Processor bottlenecks can develop when the threads of a process require more processing cycles than are currently available. In this case, the process will wait in a processor queue and system responsiveness will be slower than if process requests could be immediately served. The most common causes of processor bottlenecks are processor-intensive applications and other subsystem components that generate excessive processor interrupts (for example, disk or network subsystems).

In a workstation environment, processors are usually not the source of bottlenecks; however, you should still monitor this subsystem to make sure that processor utilization is at an efficient level. There are several standard counters you should monitor to track processor utilization.

KEY COUNTERS TO TRACK FOR PROCESSOR

You can track processor utilization through the Processor and System objects to determine whether a processor bottleneck exists. The following are the most important counters for monitoring the system processor:

Processor > % Processor Time   Processor > % Processor Time measures the time that the processor spends responding to system requests. If this value is consistently above an average of 85 percent, you might have a processor bottleneck. The Processor > % User Time and Processor > % Privileged Time counters combine to show the total % Processor Time counter. You can monitor these counters individually for more detail.

Processor > Interrupts/Sec   Processor > Interrupts/Sec show the average number of hardware interrupts received by the processor each second. If this value is higher than 3,000, you might have a problem with a program or hardware that is generating spurious interrupts (this value will vary in optimization based on the processor type; you'll need to do a little research for your specific processor to see the appropriate value).

System > Processor Queue Length   System > Processor Queue Length is used to determine whether a processor bottleneck is due to high levels of demand for processor time. If a queue of two or more items exists for an extended period of time, a processor bottleneck might be indicated. If you suspect that a processor bottleneck is due to excessive hardware I/O requests, you should also monitor the System > File Control Bytes/Sec counter.

TUNING AND UPGRADING THE PROCESSOR

If you suspect that you have a processor bottleneck, you can try the following solutions:

◆ Use applications that are less processor-intensive.

◆ Upgrade your processor.

◆ If your computer supports multiple processors, add one.

The memory and processor subsystem objects are important counters to evaluate in determining your Windows 7 performance. You should look at the hard drive or disk subsystem to look for issues as well.

Managing the Disk Subsystem

Disk access is the amount of time your disk subsystem takes to retrieve data that is requested by the operating system. The two factors that determine how quickly your disk subsystem will

respond to system requests are the average disk access time on your hard drive and the speed of your disk controller.

KEY COUNTERS TO TRACK FOR THE DISK SUBSYSTEM

You can monitor the PhysicalDisk object, which is the sum of all logical drives on a single physical drive, or you can monitor the LogicalDisk object, which represents a specific logical disk. Here are the more important counters for monitoring the disk subsystem:

PhysicalDisk > % Disk Time and LogicalDisk > % Disk Time   PhysicalDisk > % Disk Time and LogicalDisk > % Disk Time shows the amount of time the disk is busy because it is servicing read or write requests. If your disk is busy more than 90 percent of the time, you will improve performance by adding another disk channel and splitting the disk I/O requests between the channels.

PhysicalDisk > Current Disk Queue Length and LogicalDisk > Current Disk Queue Length   PhysicalDisk > Current Disk Queue Length and LogicalDisk > Current Disk Queue Length indicates the number of outstanding disk requests that are waiting to be processed. On average, this value should be less than 2.

LogicalDisk > % Free Space   LogicalDisk > % Free Space specifies how much free disk space is available. This counter should be at least 15 percent.

TUNING AND UPGRADING THE DISK SUBSYSTEM

When you suspect that you have a disk subsystem bottleneck, the first thing you should check is your memory subsystem. Insufficient physical memory can cause excessive paging, which in turn affects the disk subsystem.

If you do not have a memory problem, try the following solutions to improve disk performance:

◆ Use faster disks and controllers.

◆ Confirm that you have the latest drivers for your disk adapters.

◆ Use disk striping to take advantage of multiple I/O channels.

◆ Balance heavily used files on multiple I/O channels.

◆ Add another disk controller for load balancing.

◆ Use Disk Defragmenter to consolidate files so that disk space and data access are optimized.

After you evaluate the first three subsystems — memory, processor, and disk — you also need to look at the network subsystem to optimize your Windows 7 performance.

Optimizing the Network Subsystem

Windows 7 does not have a built-in mechanism for monitoring the entire network. However, you can monitor and optimize the traffic that is generated on your Windows 7 machine. You can monitor the network interface (your network card) and the network protocols that have been installed on your computer.

Network bottlenecks are indicated when network traffic exceeds the capacity that can be supported by the local area network (LAN). Typically, you would monitor this activity on a

network-wide basis — for example, with the Network Monitor 3.3 (available for download at `www.microsoft.com`).

Key Counters to Track for the Network Subsystem

If you are using the Performance Monitor utility to monitor local network traffic, the following two counters are useful for monitoring the network subsystem:

Network Interface > **Bytes Total/Sec**   Network Interface > Bytes Total/Sec measures the total number of bytes sent or received from the network interface and includes all network protocols.

TCPv4 > **Segments/Sec**   TCPv4 > Segments/Sec measures the number of bytes sent or received from the network interface and includes only the TCPv4 protocol.

Tuning and Upgrading the Network Subsystem

You can use the following guidelines to help optimize and minimize network traffic:

◆ Install only the network protocols you need.

◆ Use network cards that take advantage of your bus speed.

◆ Use faster network cards — for example, 100Mbps Ethernet or 1Gbps Ethernet instead of 10Mbps Ethernet.

Microsoft added a feature to Windows Vista's Performance Monitor called Reliability Monitor (hence the Windows Vista tool named Reliability and Performance Monitor). In Windows 7, Microsoft has removed the tool from Performance Monitor and Reliability Monitor is a separate tool.

Using Reliability Monitor

Reliability Monitor (see Figure 15.18) is a stand-alone feature in Windows 7 that provides an overview of the stability of your Windows 7 computer. You can access Reliability Monitor by typing **reliability monitor** in the Start menu's search box and selecting View Reliability Report from the resulting list.

If a problem is causing system instability, Reliability Monitor can provide details about it. The data is collected and stored in the following five categories in the lower half of the display window:

Application Failures   Programs that hang or crash

Windows Failures   Includes operating system and boot failures

Miscellaneous Failures   Includes unexpected shutdowns

Warnings   Items that are detrimental, but not failures

Information   Information messages that Windows 7 issues

The upper half of the graphical display indicates the relative reliability of your Windows 7 machine on a scale of 1 to 10 (with 10 representing completely reliable). To display the tracked reliability items in the time view (which you can change to display by days or weeks), click View By: Days | Weeks in the upper left of the Reliability Monitor window. You can view the

details about failures, warnings, and informational messages by clicking the icon in the graphical window for the time period displayed.

FIGURE 15.18
Windows 7's Reliability Monitor
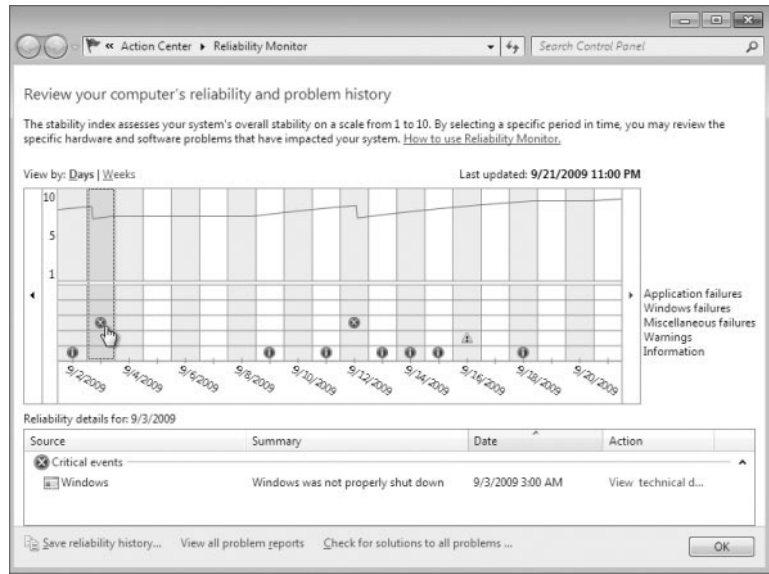
If you notice a recurring problem, choose Check For Solutions To All Problems at the bottom of the window and let Windows 7 check the issues and report potential solutions. You can view all the problems Reliability Monitor has detected by choosing View All Problem Reports, also located at the bottom of the window. By selecting Save Reliability History, you can save the current report in XML format.

Using Performance Monitor, Reliability Monitor, and Resource Monitor to manage your Windows 7 computer will make your administrative tasks simpler. Several other tools are also available for you to learn about your system information.

Using Windows 7 Tools to Discover System Information

Windows 7 contains many other tools to discover system information about your computer. In this section, we'll explore three of them:

◆ System Information

◆ Task Manager

◆ Performance Information and Tools

Getting System Information

You can use the System Information utility, shown in Figure 15.19, to learn details about your hardware, software, and resources. Type **msinfo32** in the Start menu's search box to launch this utility.

FIGURE 15.19
System Information
dialog box
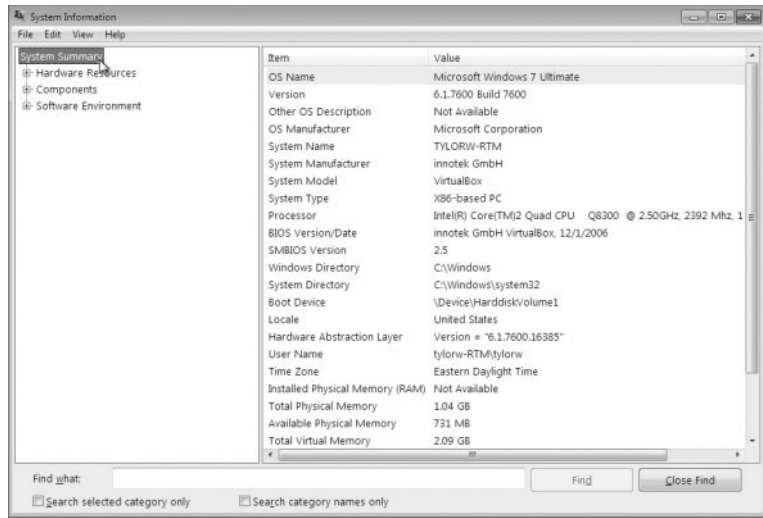
A great deal of your systems information is available within this application. Click the fields in the left pane and details are displayed in the right pane. You can also search for a term by typing it in the Find What field at the bottom of the page. This utility has been available in many releases of the Windows product.

Using Task Manager

The Task Manager utility shows the applications and processes that are currently running on your computer, as well as CPU and memory usage information. To access Task Manager, press Ctrl+Alt+Delete and click Start Task Manager. Alternatively, right-click an empty area in the Taskbar and select Task Manager from the context menu, or type **task manager** in the Start menu's search box. The Task Manager dialog box has the following six main tabs:

◆ Applications

◆ Processes

◆ Services

◆ Performance

◆ Networking

◆ Users

MANAGING APPLICATION TASKS IN TASK MANAGER

The Applications tab of the Task Manager dialog box, shown in Figure 15.20, lists all the applications that are currently running on the computer. For each task, you will see the name of the task and the current status (Running, Not Responding, or Stopped).

To close an application, select it in Task Manager and click the End Task button at the bottom of the dialog box. To make the application window active, select it and click the Switch To

button. If you want to start an application that isn't running, click the New Task button and specify the location and name of the program you wish to start.

FIGURE 15.20
Applications tab in Task Manager
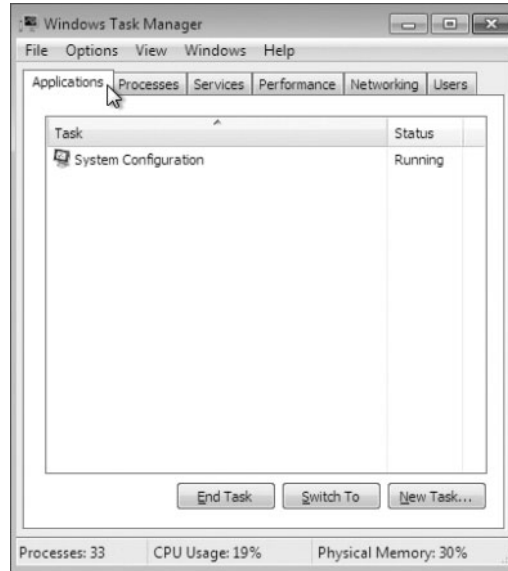
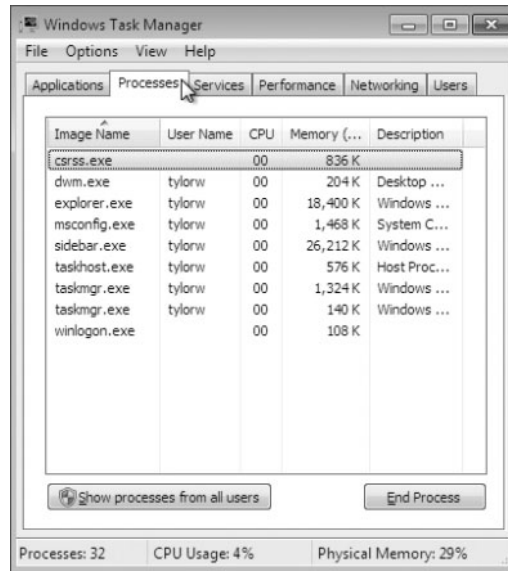MANAGING PROCESS TASKS IN TASK MANAGER

The Processes tab of the Task Manager dialog box, shown in Figure 15.21, lists all the processes that are currently running on the computer. This is a convenient way to get a quick look at how your system is performing. For each process, you will see the Image Name (the name of the process), the User Name (the user account that is running the process), CPU (the amount of CPU utilization for the process), Memory (Private Working Set) (the amount of memory that is being used by the process), and Description (a description of the process).

From the Processes tab, you can organize the listing and control processes as follows:

◆ To organize the processes, click the column headings. For example, if you click the CPU column, the listing will start with the processes that use the most CPU resources. If you click the CPU column a second time, the listing will be reversed so that the processes that use the least CPU resources are listed first.

◆ To manage a process, right-click it and choose an option from the context menu. You can choose to end the process, end the process tree, debug the process, specify virtualization, create a dump file, or set the priority of the process (to Realtime, High, Above Normal, Normal, Below Normal, or Low). If your computer has multiple processors installed, you can also set processor affinity (the process of associating a specific process with a specific processor) for a process.

◆ To customize the counters that are listed, select View ➢ Select Columns. This brings up the Select Columns dialog box where you can select various information you want to see listed on the Processes tab.

FIGURE 15.21
Processes tab in Task
Manager

On the Processes tab in Task Manager, you can also stop a process and manage process
priority:

Stopping Processes   You might need to stop a process that isn't executing properly. To stop
a specific process, select the process you want to stop in the Task Manager's Processes tab
and click the End Process button. Task Manager displays a Warning dialog box. Click the End
Process button to terminate the process. If you right-click a process, you can end the specific
process or you can use the option End Process Tree. The End Process Tree option ends all pro-
cesses that have been created either directly or indirectly by the process.

Managing Process Priority   To change the priority of a process that is already running, use
the Processes tab of Task Manager. Right-click the process you want to manage and select
Set Priority from the context menu. You can select from Realtime, High, Above Normal, Nor-
mal, Below Normal, and Low. As you might expect, applications launch at Normal priority by
default.

Perform the following steps to set a process priority and end a process from within Task
Manager:

1. Right-click an empty space on your Taskbar and select Task Manager from the context
   menu.

2. On the Applications tab, click the New Task button.

3. In the Create A New Task dialog box, type **calc** and click OK.

4. Click the Processes tab. Right-click calc.exe and select Set Priority, then select Low. In the Warning dialog box, click the Change Priority button to continue.

5. Right-click calc.exe and select End Process. In the Warning dialog box, click the End Process button.

⊕ Real World Scenario

RESTARTING YOUR WINDOWS 7 DESKTOP

Windows 7 is much better at closing all graphical displays when programs close or crash than other Windows legacy operating systems. But, I have still had issues when something seems to stay on my desktop when it shouldn't. A piece of a window, some graphic component, or just some distracting piece of garbage that is not supposed to be there is just hanging around. Most of the time you'll see users reboot their machine to clean up the desktop, I know I used to. Using the Process tab of Task Manager can provide a solution to this problem. If you select the explorer.exe process and end it, you will see your desktop programs, icons, and random stuck graphics go away (and not come back). You can then just restart the explorer.exe process (the desktop) by choosing File ➤ New Task and typing explorer.exe to bring back your desktop (Task Manager stays with the ending of the explorer process). This is a much faster and more efficient way of restoring your desktop without rebooting.

MANAGING SERVICES IN TASK MANAGER

The Services tab of the Task Manager dialog box, shown in Figure 15.22, lists all the services that can run on the computer. For each service, you will see the Name (the name of the service), the PID (the associated process identifier), Description (a description of the service, Status (whether a process is Running or Stopped), and Group (the service group).

To start a stopped service, click the service and select Start Service. To stop a running service, click the service and select Stop Service. You can also open the Services tool by clicking the Services button. The Services tool allows you to specify whether a process starts automatically, automatically with a delayed start, manually, or is disabled.
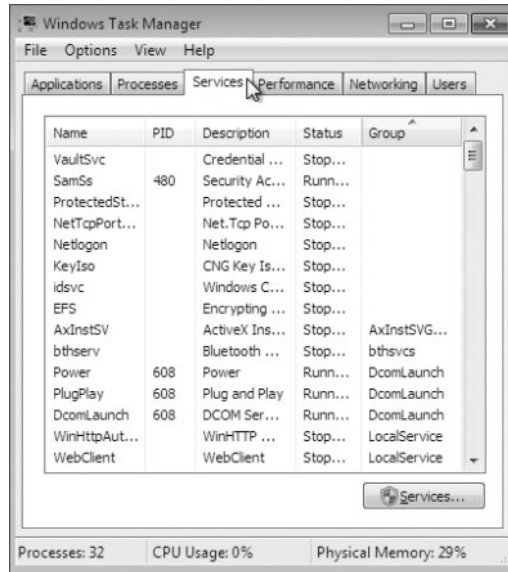
MANAGING PERFORMANCE TASKS IN TASK MANAGER

The Performance tab of Task Manager, shown in Figure 15.23, provides an overview of your computer's CPU and memory usage. This information is similar to the information tracked by Performance Monitor.
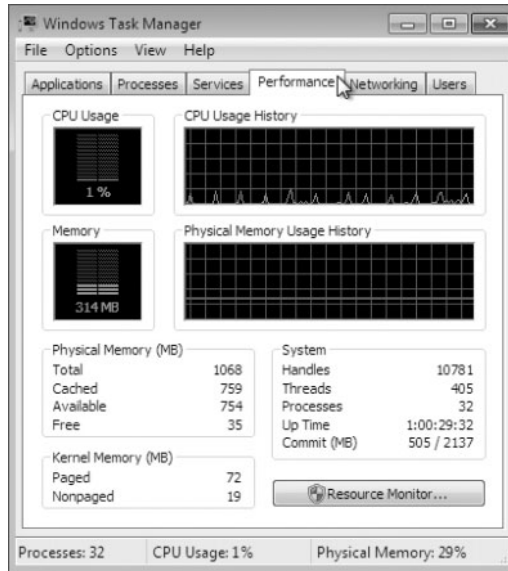
The Performance tab shows the following information:

◆ CPU usage, in real time and in a history graph

◆ Memory usage, in real time and in a history graph

◆ Physical memory statistics

◆ Kernel memory statistics

◆ System totals for handles, threads, processes, uptime, and the pagefile

FIGURE 15.22
Services tab of Task
Manager

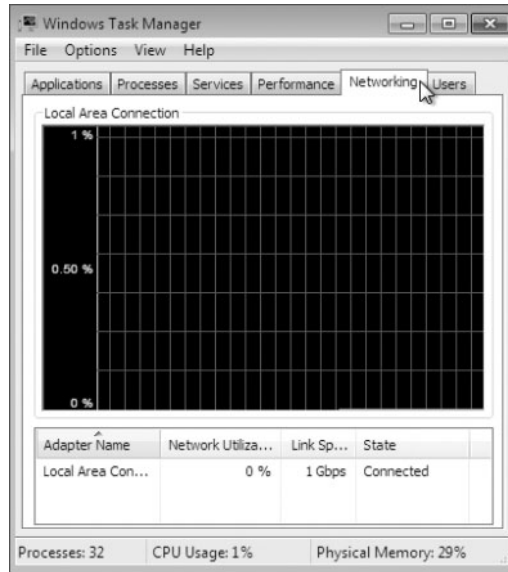**FIGURE 15.23**
Performance tab of Task
Manager

Click the Resource Monitor button to launch the Resource Monitor that you can also find in
Performance Monitor.

MANAGING NETWORKING TASKS IN TASK MANAGER

The Networking tab of Task Manager, shown in Figure 15.24, provides an overview of your
networking usage. Statistics for each adapter are displayed at the bottom of the tab.

FIGURE 15.24
Networking tab of Task
Manager

MANAGING USERS IN TASK MANAGER

The Users tab of Task Manager, shown in Figure 15.25, shows the active and disconnected users on your computer. For each user, you will see the User (the name of the user), the ID (the current user ID), Status (whether Active or Disconnected), Client Name, and Session (whether the user is connected via the console session or by another method, such as Remote Desktop).

FIGURE 15.25
Users tab of Task
Manager
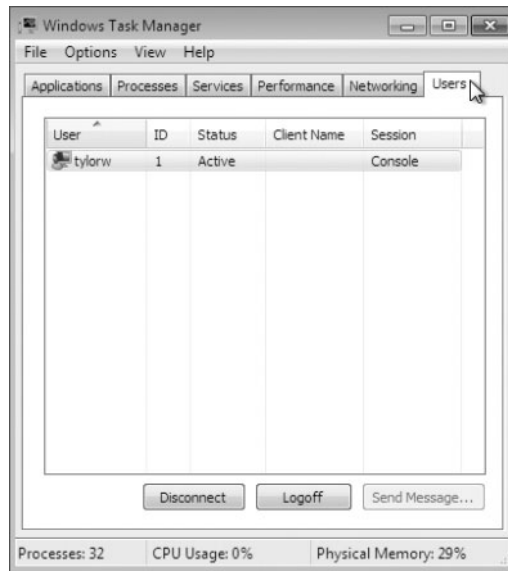
To send a message to a user, select the user and click the Send Message button. To connect to a user session, right-click the user and select Connect. To disconnect a user session, select the user and click the Disconnect button. To log off a user, select the user and click the Logoff button.

Next let's look at another tool available in Windows 7 that reveals how well your machine is working: Performance Information and Tools.

Scoring Windows 7 with Performance Information and Tools

If you enjoy seeing how well your computer performs by running benchmarking applications that provide a score rating, then you will love Performance Information and Tools, shown in Figure 15.26. This utility provides you with a numerical score that lets you know how well your system performs. To launch Performance Information and Tools, click Start ➢ Control Panel ➢ System and Maintenance ➢ Performance Information and Tools, or type **performance information** in the Start menu's search box.

FIGURE 15.26
Performance Information and Tools window
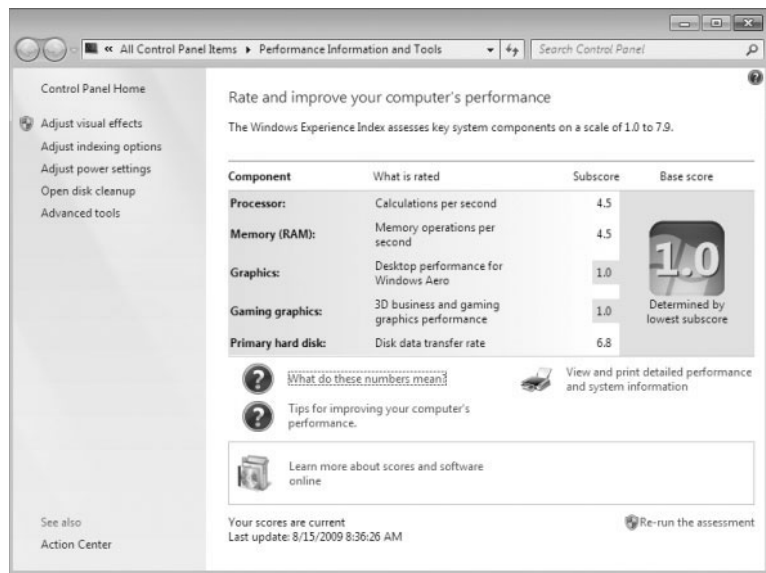
The main pane reveals a calculated score, called the Windows Experience Index. The Windows Experience Index base score is calculated by taking the lowest subscore among five rated components:

◆ Processor, based on calculations per second

◆ Memory (RAM), based on memory operations per second

◆ Graphics, based on Windows Aero performance

◆ Gaming Graphics, based on 3D graphics performance

◆ Primary Hard Disk, based on disk transfer rate

A computer with a base score of 1 or 2 will be able to perform only the most basic tasks. A base score of 3 indicates that a computer can run Windows Aero and all but the most advanced Windows 7 features. A computer with a base score of 4 or 5 should be able to run all Windows 7 features, as well as play graphics-intensive 3D games.

Each component subscore determines how well each individual component performs. Because the base score is equal to the lowest component subscore, the Windows Experience Index base score should give you an overview of how well your computer will run applications. This enables application developers to give their applications a numerical rating so that consumers can easily determine whether the application will run well on their computer. If an application requires a higher base score than your computer has, it might be time to upgrade your hardware. After you install new hardware, you can select Update My Score to have Windows 7 recalculate your Windows Experience Index base score.

The left pane of Performance Information and Tools contains useful links to help you improve the performance of your computer. Click Adjust Visual Effects to open the Visual Effects tab of the Performance Options dialog box, which you can use for configuring how Windows will graphically display windows, menu items, and icons. Click Adjust Indexing Options to launch Indexing Options, which can improve the speed of searching files on your computer. Click Adjust Indexing Options to launch the Indexing Options dialog box, where you can choose which resources on your Windows 7 machine are included in indexing. Click Adjust Power Settings to launch Power Options, which you can use to adjust your power plan. Click Open Disk Cleanup to launch Disk Cleanup Options so that you can clean up unnecessary files on your hard disk. Finally, click Advanced Tools to launch a list of tools that you can use to further improve your computer's performance:

◆ Clear all Windows Experience Index scores and re-rate the system

◆ View Performance Details in Event Log

◆ Open Performance Monitor

◆ Open Resource Monitor

◆ Open Task Manager

◆ View Advanced System Details in System Information

◆ Adjust the Appearance and Performance of Windows

◆ Open Disk Defragmenter

◆ Generate a System Health Report

The Performance Information and Tools menu is a great display of your system and a launching point for many tools in Windows 7. Another useful tool that has been around in many versions of Windows and is still available in version 7 is the System Configuration utility, or MSConfig.

Using System Configuration

You can use the System Configuration utility to help you view and troubleshoot how Windows 7 starts and what programs and services launch at startup. You might recognize this utility as `msconfig.exe`. To launch it, run `msconfig.exe` from the Start menu's search box. Use the

General tab, shown in Figure 15.27, to specify startup options. You can choose from the following three startup options:

◆ Normal Startup, which loads all device drivers and services

◆ Diagnostic Startup, which loads basic services and drivers

◆ Selective Startup, from which you can choose whether or not to load system services, load startup items, and use the original boot configuration

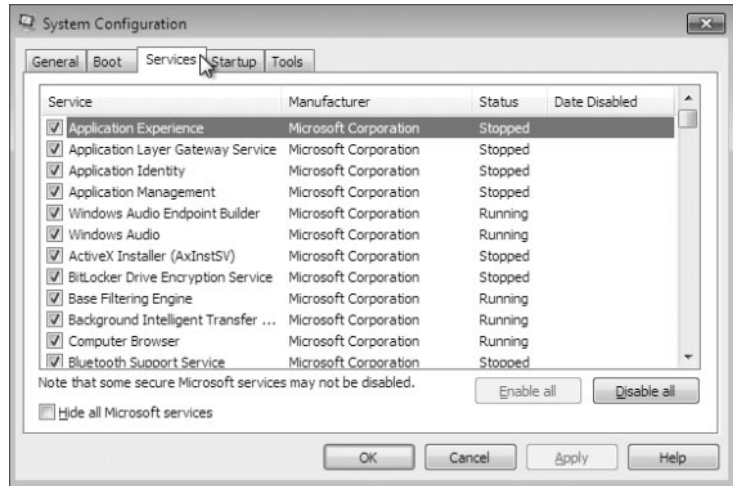**FIGURE 15.27**
General tab in System
Configuration
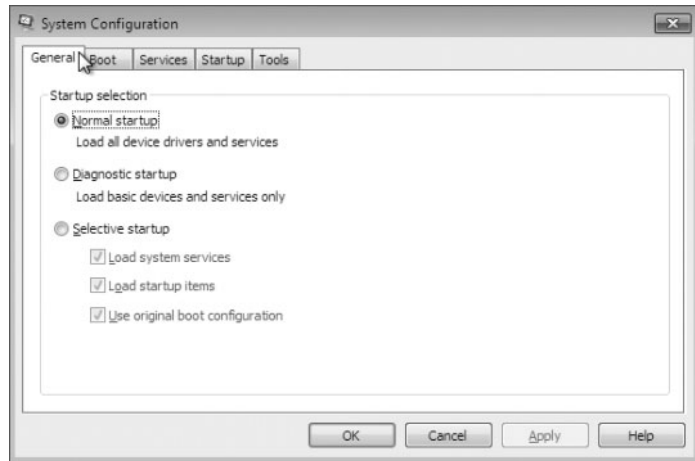
Use the Boot tab, shown in Figure 15.28, to configure whether Windows boots in Safe Mode, runs an Active Directory repair, boots to a graphical user interface (GUI), logs boot information, boots in VGA mode, and displays driver names while booting. Select any of the options on this screen to change the settings on the General tab; conversely, select Normal Startup on the General tab to clear the settings on the Boot tab.

FIGURE 15.28
Boot tab in System
Configuration
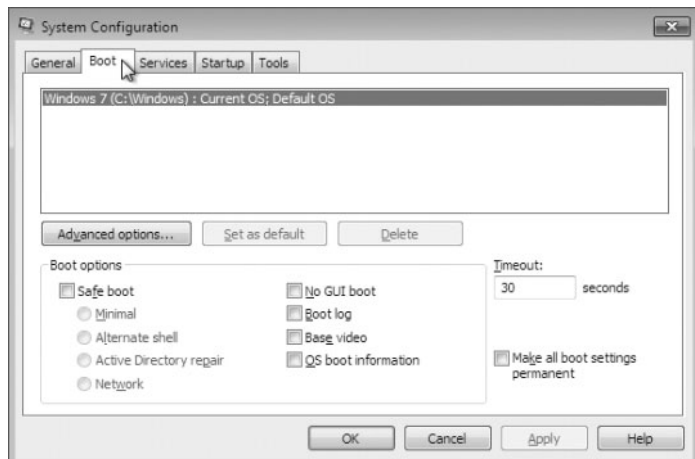
Use the Services tab to list Windows 7 services and indicate which services are running. You can deselect services on this tab so that they do not launch at startup. Select any of the services on this screen to change the settings on the General tab; conversely, select Normal Startup on the General tab to clear the settings on the Services tab. The Services tab of the System Configuration tool is shown in Figure 15.29.

FIGURE 15.29
Services tab in System Configuration

Use the Startup tab, shown in Figure 15.30, to show applications that start when Windows 7 starts. You can deselect applications on this tab so that they do not launch at startup. If you've read through the previous two paragraphs, you can probably guess that selecting any of the services on this screen changes the settings on the General tab, and selecting Normal Startup on the General tab clears the settings on the Startup tab.

**FIGURE 15.30**
Startup tab in System Configuration
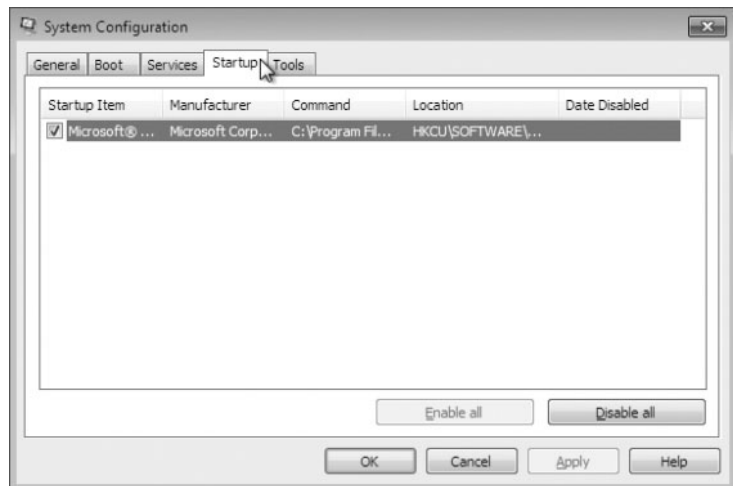
Use the Tools tab, shown in Figure 15.31, to view the tools you can launch from System Configuration. Simply click the tool name and click Launch to launch the tool. You can launch the following tools from this tab:

◆ About Windows

◆ Change UAC Settings

◆ Action Center

◆ Windows Troubleshooting

◆ Computer Management

◆ System Information

◆ Event Viewer

◆ Programs

◆ System Properties

◆ Internet Options

◆ Internet Protocol Configuration

◆ Performance Monitor

◆ Resource Monitor

◆ Task Manager

◆ Command Prompt

◆ Registry Editor

◆ Remote Assistance

◆ System Restore

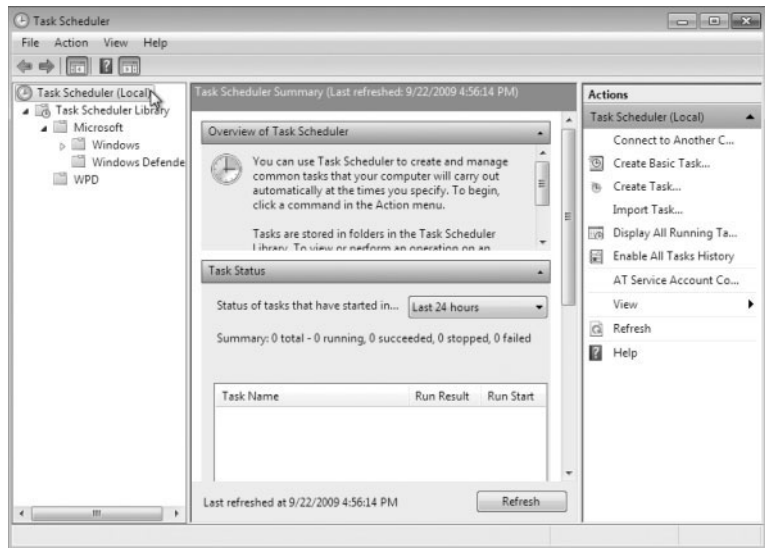**FIGURE 15.31**
Tools tab in System Configuration
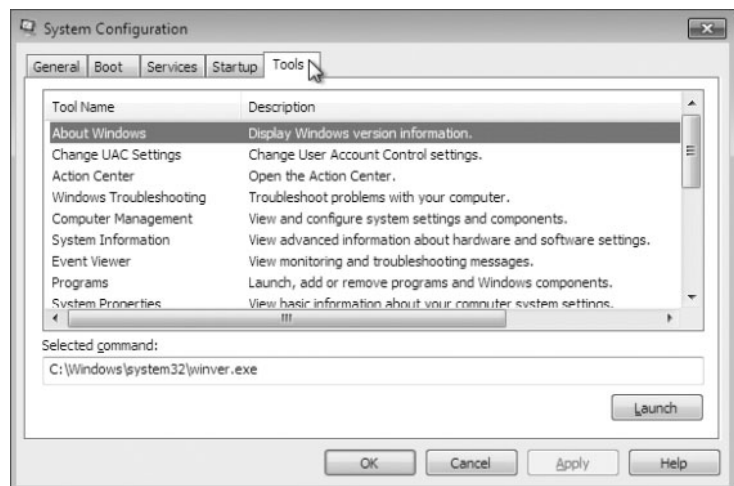
From the Tools tab you can launch many of the utilities offered by Windows 7 manually. You might have some tools or programs you want to launch automatically and run at a predetermined time; this ability is available using Task Scheduler.

Setting Up Task Scheduler

Use the Task Scheduler utility in Windows 7 to schedule actions to occur at specified intervals. Windows 7 Task Scheduler (shown in Figure 15.32) can be accessed by typing **task scheduler** in the Start menu's search box.

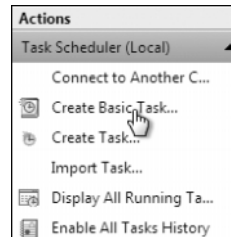**FIGURE 15.32**
Windows 7 Task Scheduler

After the Task Scheduler starts, you can create a scheduled task.

Creating a Scheduled Task

You can create a basic task by selecting the Create Basic Task item in the Actions pane in the right side of Task Scheduler, as shown in Figure 15.33.

FIGURE 15.33
Creating a basic task in Task Scheduler

By creating a basic task, a Task Manager wizard lets you set any of your Windows programs to run automatically at a specific time and at a set interval, such as daily, weekly, or monthly. For example, you might schedule an application to run daily at 2:00 a.m. Actions can be performed at the following events (called triggers) available in the Task Manager wizard:

◆ Daily, or once every number of days (such as once every three days)

◆ Weekly, or on certain days of the week, or every number of weeks (such as every four weeks on Monday)

◆ Monthly, or on selected days of the month, or only on selected months

◆ One time only

◆ When the computer starts

◆ When you log on

◆ When a specific event is logged

If you've chosen a time trigger, you configure the time/date when the action will occur. When a trigger is activated, Task Scheduler can perform the following actions:

◆ Start a program.

◆ Send an email.

◆ Display a message.

Perform the following steps to set up a scheduled task to launch Windows 7 Calculator at a predetermined weekly time:

1. Select Start and type **task scheduler** in the Start menu's search box or choose Start ➢ Control Panel ➢ System And Security ➢ Administrative Tools ➢ and double-click Task Scheduler.

2. In the Actions pane of the Task Scheduler window, select Create Basic Task.

3. The Create Basic Task wizard appears; type **Monday's calculator** as a name for your task, enter a description, and then click Next.

4. Select how often you want the action to occur; we will select Weekly and click Next to continue.

5. Specify that the action should occur every Monday at 9 a.m. and click Next.

6. Select the Start A Program radio button and click Next.

7. Browse for the Calculator application at `C:\%windir%\system32\calc.exe`; click Next.

8. The final screen shows your selections for the scheduled task; click Finish.

Select the Windows folder in the left pane and then select the arrow to expand the folder's contents to reveal a complete set of preconfigured tasks. Figure 15.34 shows the Windows folder expanded and the Defrag task selected. You can view the Defrag task settings, edit the task, and even run the Defrag task manually if you desire.

FIGURE 15.34
Task Scheduler
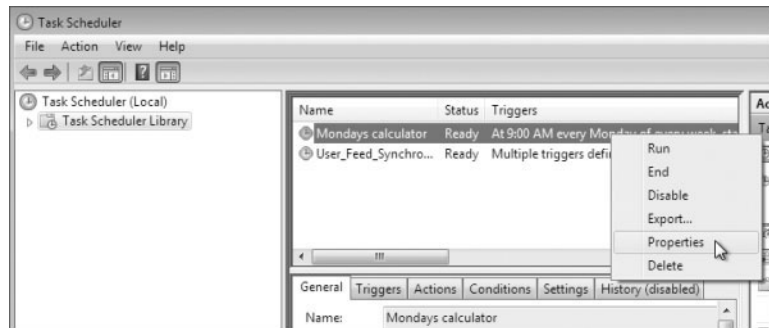preconfigured
Defrag task
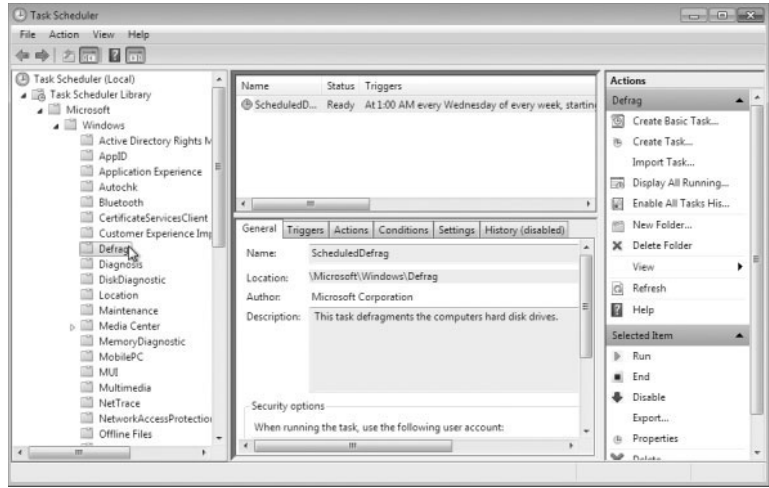
Task Scheduler also allows you to run tasks manually by selecting the task and clicking Run in the right pane. Select a task and click Disable to disable a task.

Managing Scheduled Task Properties

You can manage a scheduled task through its properties dialog box. To access this dialog box, right-click the task you want to manage and choose Properties from the context menu, as shown in Figure 15.35.

FIGURE 15.35
Right-click the task you
want to manage and
choose Properties.

The scheduled task's properties dialog box has six tabs for configuration, as follows:

◆ General

◆ Triggers

◆ Actions

◆ Conditions

◆ Settings

◆ History

Each options tab is described here:

General Tab   On the General tab, you can configure the following options:

◆ The description of the task

◆ The username or group to be used to run the specified task

◆ Whether the task is run when the user is logged off

◆ Whether the task is hidden

Triggers Tab   The Triggers tab shows the schedule configured for the task. You can click Edit to edit the trigger, which brings up the Edit Trigger dialog box. You can also click New to create a new trigger or click Delete to delete an existing trigger.

Actions Tab   The Actions tab shows the action that is configured for the task. You can click Edit to edit the action, which brings up the Edit Action dialog box. You can also click New to create a new action or click Delete to delete an existing action.

Conditions Tab   The Conditions tab shows the conditions associated with the task. The options in the Idle section are useful if the computer must be idle when the task is run. You can specify how long the computer must be idle before the task begins and whether the task should be stopped if the computer ceases to be idle. The options in the Power section are applicable when the computer on which the task runs is battery powered. You can specify that the task should not start if the computer is running from batteries and choose to stop the task if battery mode begins. You can also select whether to wake the computer in order to run the task. The option in the Network section defines whether the task starts when a particular network connection is available.

Settings Tab   The Settings tab shows the settings that affect the task's behavior with the following settings:

◆ Whether the task can be run on demand

◆ Whether the task should be restarted if it is missed

◆ How often the task should be restarted if it fails

◆ When to stop the task if it runs a long time

◆ Whether you can force the task to stop

◆ When the task should be deleted

◆ What actions should occur if the task is already running

History Tab   The History tab shows historical information regarding the task, including the task's start time, stop time, and whether the task completed successfully. Once set up, the scheduled task should commence at the appropriate time; if not, you might need to troubleshoot it.

Troubleshooting Scheduled Tasks

If you are trying to use Task Scheduler and the tasks are not properly being executed, one of the following troubleshooting options might resolve the problem:

◆ If a scheduled task does not run as expected, right-click the task and select Properties. In the Task Scheduler Library, ensure that the task status is Ready. In the task's properties page, verify the schedule has been defined on the Triggers tab.

◆ If the scheduled task is a command-line utility, make sure that you have properly defined the command-line utility, including any options that are required for the utility to run properly.

◆ Verify that the user who is configured to run the scheduled task has the necessary permissions for the task to be run.

◆ Within the Task Status section, check the task status to see when the task last ran successfully, if ever.

◆ Verify that the Task Scheduler service has been enabled on the computer if no tasks can be run on the computer.

Task Scheduler is a great utility that you can use to run scheduled maintenance applications and proactively maintain a Windows 7 system. If there are issues that occur within Windows 7, you use a different utility, called Event Viewer, to view these events.

Using Event Viewer

Event Viewer, shown in Figure 15.36, enables you to view event logs that are created by the operating system. This utility is useful when troubleshooting problems that occur on your computer.

FIGURE 15.36
Windows 7 Event Viewer
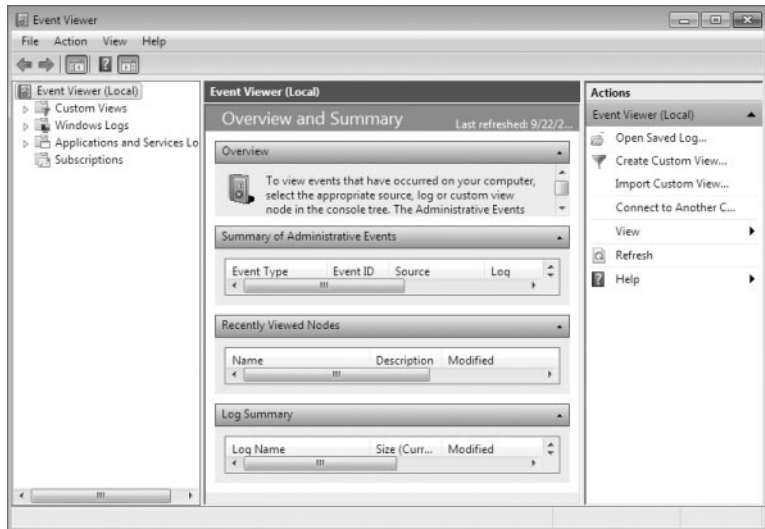
Whenever an error occurs, an event is usually placed in one or more event logs. To open Event Viewer, click Start ➢ Control Panel ➢ System And Security ➢ Administrative Tools ➢ View Event Logs, or you can type **event viewer** in the Start menu's search box.

Whereas old versions of Event Viewer contained only the Application, Security, and System logs, the Windows 7 version of Event Viewer contains the following logs:

◆ Application

◆ Security

◆ Setup

◆ System

◆ Forwarded Events

The Application log is used to log events relating to applications, such as whether an application, driver, or service fails. The Security log is used to log security events, such as successful or failed logon events. The Setup log is used only by domain controllers, so it doesn't have much practical use in Windows 7. The System log is used to log events concerning the operating system and related services. The Forwarded Events log is used to collect events that have been forwarded from other computers.

To configure log settings, right-click the log that you want to configure and select Properties. The Log Properties dialog box appears. The application log properties are shown in Figure 15.37.

The Log Properties dialog box shows the following information:

◆ The full name of the log

◆ Where the log is stored

◆ The size of the log

◆ When the log was created, modified, and accessed

◆ Whether logging is enabled for the log

◆ The maximum log size in KB

◆ The action that occurs when the log reaches the max size

The left pane of Event Viewer is where you find the Windows logs noted previously, but it also contains other logs and views that can be helpful when troubleshooting a specific application. The Custom Views section can be used to create a view that contains only the information you want to see, such as only events in a particular log or only Critical events. One custom view, Administrative Events, is created for you by default, as shown in Figure 15.38.

The Administrative Events view contains Critical, Error, and Warning events from all logs, enabling you to easily view only the most important events. Another section in the left pane contains logs that relate to Applications and Services, as shown in Figure 15.39.

The Microsoft folder within the Application and Services Log contains many other logs related to specific Microsoft components and applications.

The Subscription folder enables you to receive event logs from other computers. Having other machines send its event to one machine is useful to us as it gives us one central to view events from multiple locations. To use subscriptions, you must start the Windows Event Collector Service.

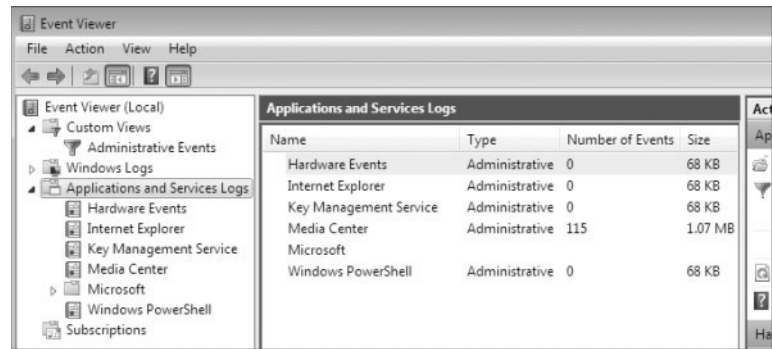**FIGURE 15.37**
Event Viewer
Application log
properties
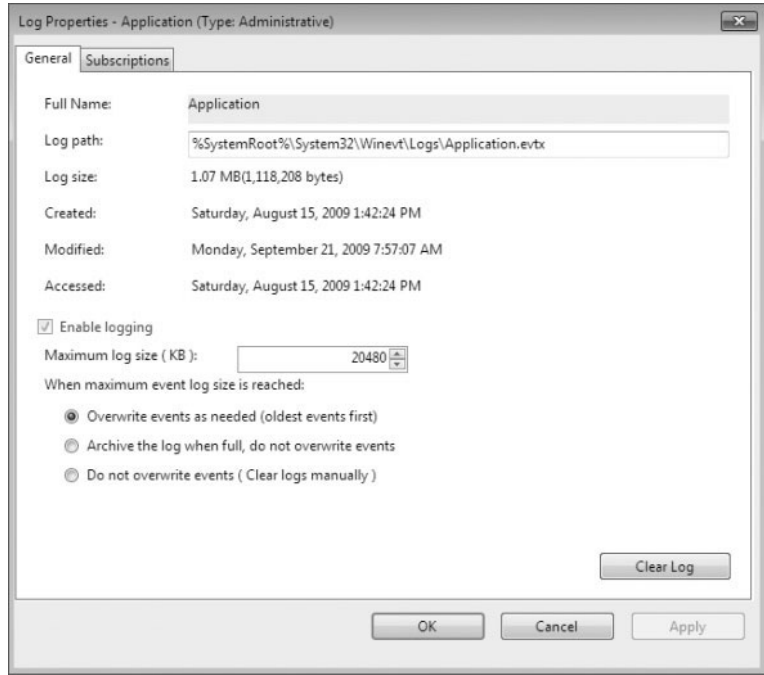
FIGURE 15.38
Event Viewer
Custom Views section:
Administrative Events
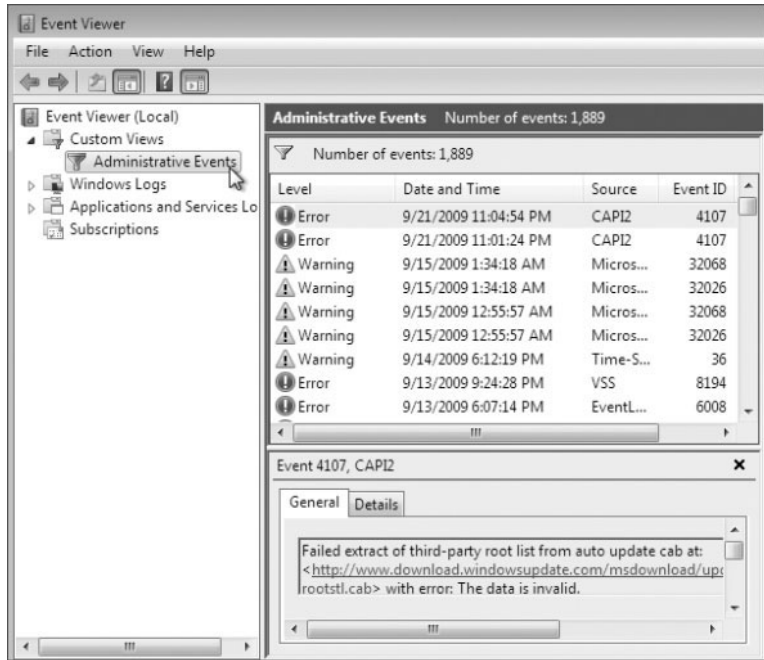
FIGURE 15.39
Event Viewer
Application and
Services Logs

The center pane of Event Viewer displays the events and information that relates to those events. You can also view a summary of your administrative events, which contains a count of Critical, Error, Warning, Information, Audit Success, and Audit Failure events. A count of these events is displayed for the last hour, day, and week, and the total number of events is also provided. Each event is assigned an event level of Critical, Error, Warning, Information, or Verbose.

The right pane of Event Viewer enables you to perform actions related to items you have selected in the left and center panes. You can save logs, open saved logs, create or import views, clear logs, filter logs, and find logs with certain keywords. You can also attach a task to an event. Clicking Attach Task To This Event opens the Create Basic Task wizard in Task Scheduler so that you can easily create a task related to the selected event.

Perform the following tasks to view events in Event Viewer and set log properties:

1. Select Start ≻ Control Panel ≻ System And Security ≻ Administrative Tools ≻ View Event Logs, or type **event viewer** in the Start menu's search box.

2. Open Windows Logs and click System in the left pane of the Event Viewer window to display the System log events.

3. Double-click the first event in the center pane of the Event Viewer window to see its Event Properties dialog box.

4. After you view the event properties, click the Close button to close the dialog box.

5. Right-click System in the left pane of the Event Viewer window and select Properties.

6. Configure the System log to archive the log file when it is full by clicking Archive The Log File When Full; Do Not Overwrite Events; click OK to close the dialog box.

7. Right-click System in the left pane of the Event Viewer window and select Filter Current Log.

8. Select the Critical and Error check boxes; then click OK (you will see only Critical and Error events listed in the System log).

9. Right-click System and select Clear Log.

10. A dialog box appears that asks if you want to save the System log before you clear it; click the Save And Clear button.

11. Specify the path and filename for the log file, and then click the Save button (the events will be saved in an `.evtx` file, and the events will be cleared from the System log).

Event Viewer is one of the first places to look when you suspect Windows 7 is not behaving correctly. But what if you know Windows 7 is having a problem and you need to restore the configuration or restore files? You need to use Windows 7 Backup and Restore.

## Maintaining Windows 7 with Backup and Restore

The Windows 7 Backup and Restore utility allows you to create and restore backups. Backups protect your data in the event of system failure by storing the data on another medium, such a hard disk, CD, DVD, or network location. If your original data is lost due to corruption, deletion, or media failure, you can restore the data using your saved backup.

To access Backup and Restore (Shown in Figure 15.40), type **backup and restore** in the Start menu's search box or select Start ➢ Control Panel ➢ System And Security ➢ Backup And Restore.

Creating a Backup

You can see in Figure 15.40 that no backups of this Windows 7 machine have been taken. To set up a backup, choose the Set Up Backup link to launch a wizard that takes you through the process of creating a backup. The Backup wizard first asks you for a location to save your backup. This location can be a hard disk (removable or fixed), a CD, a DVD, or even a network location (if you have Windows 7 Premium or Ultimate).

FIGURE 15.40
Windows 7 Backup and Restore
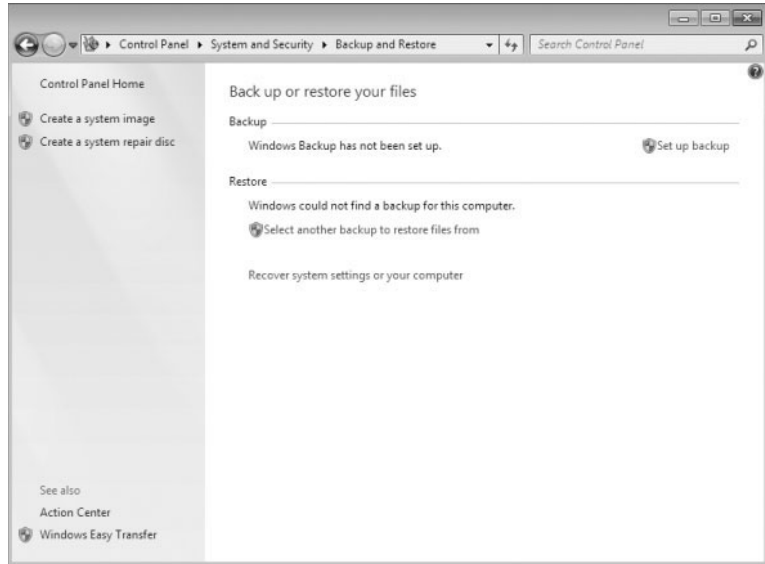
Next you are asked to either let Windows 7 choose the files and folders to back up or let you manually select the resources you want to back up. In your manual selection you can choose just the data libraries of Windows 7 for you as a user, or other users. You can also choose to create a backup of the Windows 7 systems files. If you want to choose other files and folders, you have the option of selecting any resources individually on your hard disk(s).

The final page of the wizard allows you to view the items you have selected as well as set up a schedule for your backups to occur. If you're happy with the setup, click the Save Settings And Run Backup button. The backup commences and you are able to restore the resources if necessary in the future. Figure 15.41 shows this author's Windows 7 machine right after he chose to save settings and run the backup. You can see the backup in progress and the history of his backups.

FIGURE 15.41
Windows 7 initial backup in progress
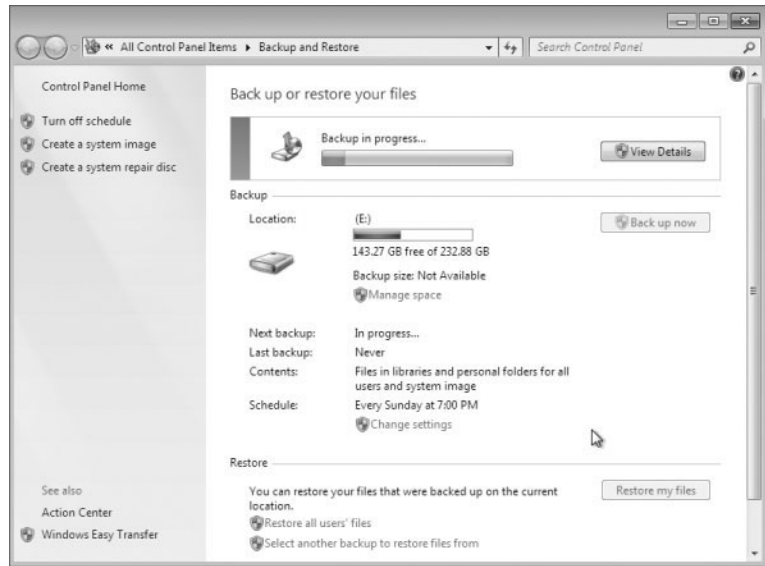
After you have created your backup, you can restore systems files and user data files with the restore utility.

Restoring Files from a Backup

If you have lost or destroyed files that you still want on your Windows 7 system, you can restore them from your backup. To restore files to your computer, launch the Backup and Restore program by typing **backup and restore** in the Start menu's search box. Assuming the media where your backup was saved is available, you can click the Restore My Files button, as shown in Figure 15.42.

FIGURE 15.42
Click the Restore My Files button to launch a restore wizard.
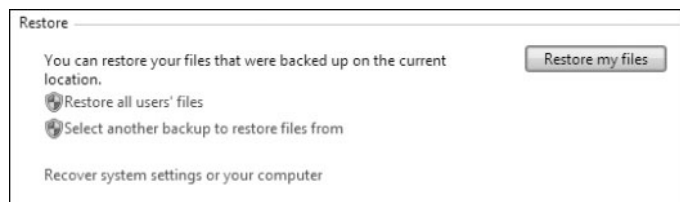
Clicking the Restore My Files button launches a restore wizard that prompts you to search for the files you want to restore. You can select multiple files and folders to restore. When you

have selected all the files and folders you want to restore, click Next and you will have one final option: to restore to the original location or to pick an alternate location for restoration. After you make the restore location decision, click Restore and the restore operation commences and your original files and folders are available for you from the backup media.

You also have options in the Backup and Restore window to restore all users' files and to select another backup to restore files from. You would use this second option if you have saved your backup to multiple locations, and the last one (the one listed in the backup section) is not the set of backup files you want to use in your current session. Other than just files and folders, you have the choice to use other advanced backup options.

Using Advanced Backup Options

In the main backup and restore window, you have options in the left pane (as shown in Figure 15.43): Turn Off Schedule, Create A System Image, and Create A System Repair Disc.

FIGURE 15.43
Other backup options
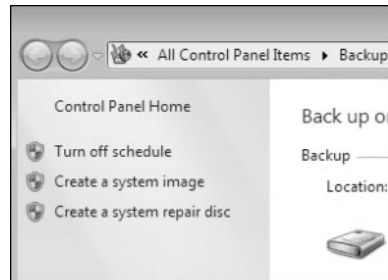
Choosing Turn Off Schedule lets you take your backup out of the current backup scheduling as seen in Task Scheduler. Create A System Image lets you back up critical operating system files for restoration later if your operating system has become corrupted. Create A System Repair Disc allows you to create a bootable disc that will store a limited setup, repair utilities, and the ability to restore your backup files if necessary.

There's one more option for restoring your Windows 7 configuration: System Protection.
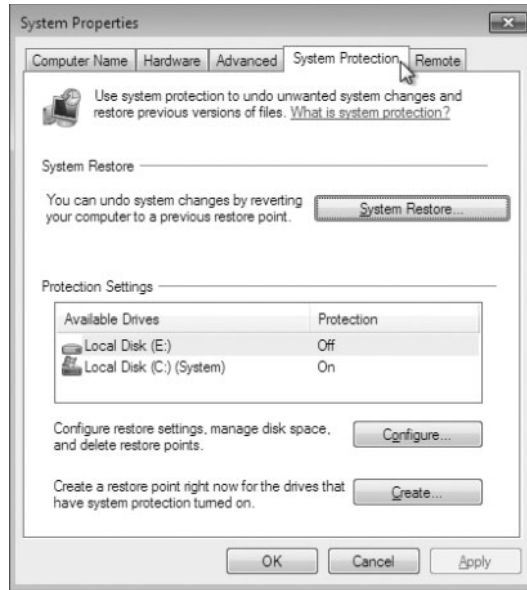
Using System Protection

System Protection is a feature of Windows 7 that creates a backup and saves the configuration information of your computer's system files and settings on a regular basis. System Protection saves previous versions of saved configurations rather than just overwriting them. This makes it possible to return to multiple configurations, known as restore points, in your Windows 7 history. These restore points are created before most significant events, such as installing a new driver. Restore points are also created automatically every seven days. System Protection is turned on by default in Windows7 for any drive formatted with NTFS.

You manage System Protection and the restore points from the System Protection tab of the System Properties dialog box. You access this tab directly by typing **restore point** in the Start menu's search box, as shown in Figure 15.44.

Clicking the System Restore button launches the System Restore wizard, which walks you through the process of returning Windows 7 to a previous point in time. Also on the System Protection tab of the System Properties dialog box you'll find the Protection Settings section, where you can configure any of your available drives. Select the drive on which you would

like to modify the configuration and click the Configure button. The System Protection configuration dialog box for the drive appears, as shown in Figure 15.45.
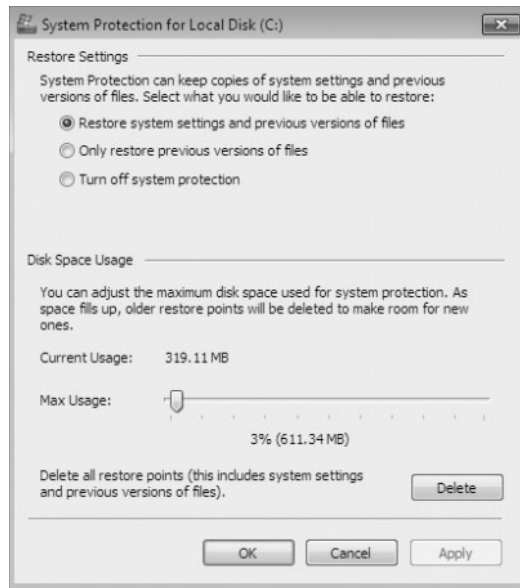
The System Protection for the selected disk properties box allows you to enable or disable system protection for the drive. When you enable protection, you can opt for previous versions

for files or previous versions of files and system settings. You also have the ability to set the maximum usage your restore points will use for storage. One final function of the System Protection dialog box for the selected disk is to delete all restore points (including system setting and previous versions of files) by clicking the Delete button.

The Bottom Line

Use Performance Monitor to view CPU usage.   Performance Monitor gives you a way to view real-time statistics of several of the Windows 7 subsystems.

> **Master It**   You recently installed a new Windows 7 application. It seems as though your machine is operating more slowly than normal. Someone told you to look at how busy your CPU is while the application is running. How will you view the CPU utilization while the application is running?

Maintain Windows 7 with system tools.   There are several system tools within Windows 7 to help you monitor and maintain your operating system. These tools include Task Manager, Performance Information and Tools, and System Configuration (MSConfig).

> **Master It**   After you install a new application on your Windows 7 machine, you find that it is causing you problems in performance. The longer the application runs, the more your machine seems to lag. After a period of time, the application no longer responds. It even displays ''Not Responding'' in its title bar and the whole application interface has become translucent. You would like to shut the application down but can't even click the close ''X'' in the upper-right corner. How can you force the application to close?

Schedule a task to launch daily.   There are times when you would like an application to run periodically to perform some function on your Windows 7 machine. You can use Task Scheduler to perform this operation.

> **Master It**   You are concerned about security on your local machine and have purchased a software product to collect security information such as open ports, applications that are running, and services that are enabled. The application has the ability to take a snapshot of several of the security parameters you're concerned with and save them to a log file; you just have to run the application. You would like to run the program daily and save the logs so you can review them periodically at your convenience. How can you run the program daily without having to launch it manually?

Back up critical data files.   You can use the Backup and Restore application in Windows 7 to make backup copies of operating system and critical data files that might be needed even if they're deleted by mistake or become corrupted.

> **Master It**   Your main application that stores critical financial data files for your company is stored locally on your Windows 7 machine. You're nervous that these files can severely impact your day-to-day operation if they somehow become corrupted or are deleted. You would like to save a copy of the whole financial data folders so you can recover any or all of the data files with minimal impact. How can you back up the critical files in Windows 7?