Chapter 8

SYSTEM RECOVERY AND DIAGNOSTIC TRICKS

Backup and Restore Center

Computers die. It's true. They overheat; they get old and run down. A lightning strike creeps up the wires into your box. They call them *terminals* for a reason. It's because their lifespan is terminal (okay, not really, but you take my point). The difference with a computer is that you have the ability to back up your data, settings, and preferences and restore them to the same machine with new hardware or an entirely new machine.

IN THIS CHAPTER

The Backup and Restore Center

Even novice users can open the Backup and Restore Center (shown in Figure 8.1) and work their way through the wizards. To find it you can type **Backup and Restore Center** from the Start orb search pane, or you can open the All Programs folder, go to Maintenance, and select it from there to start the wizards.

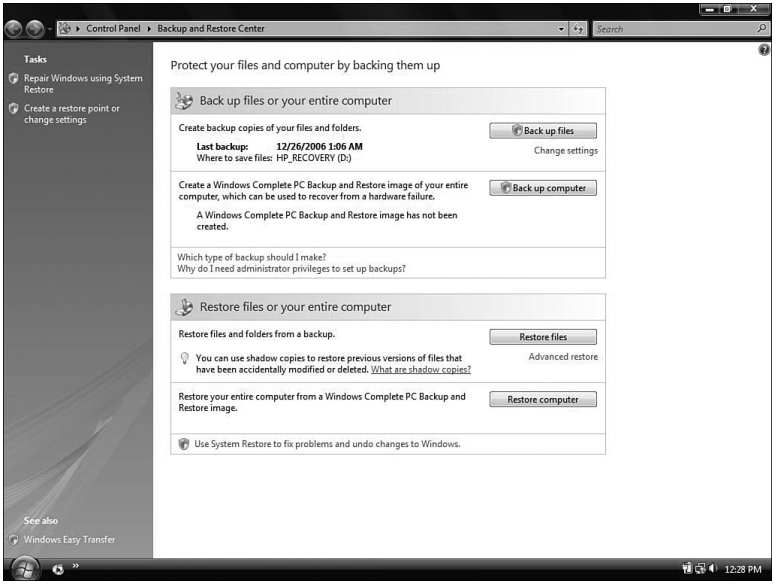

FIGURE 8.1

The Backup and Restore Center is an easy console for novice users to work with.

From within the center you can do the following:

- Back up your data files (or schedule your files to be backed up at regular intervals to ensure data protection).
- Perform a Windows CompletePC Backup image (which creates a snapshot of the entire system, including files). CompletePC Backup is available in the Business, Enterprise, and Ultimate versions of Vista.
- Restore your files or entire PC from the backups you've created.

There are some improvements of the backup program in Vista besides ease of use. Mitch Tulloch, a Microsoft MVP and president of MTIT Enterprises (www.mtit.com), says that choosing "where you want to store your backup files…. This is the biggest improvement in the Windows Vista version of Windows Backup over the Windows XP version of the

same tool." You can back up files to another drive on your system, to a removable drive (such as USB), a CD, a DVD, or even to another system using a shared folder on that other system. Keep in mind that you need to include the proper credentials on the other system if you use a network location.

Before you go backing up your complete system, it would be good to know what the caveats are. When you restore your CompletePC backup, you are pretty much overwriting the drive, which can be destructive to the existing contents, so keep that in mind before you decide to test this on your home system just for fun (although reports show that the process works quite smoothly, much like restore CDs that have been included PCs). It's an emergency tool. Also, be sure you have enough disk space for the backup. Compression varies depending on the type of data you backup, so until you get a handle on how much backup space you need, assume a 1:1 backup (meaning if you have 1 GB of data to backup, make sure you have that amount of space available for your backup). With a CompletePC backup, because of the way it works, you cannot save the image to the same hard drive that holds the location of the system files. You'll need another drive (formatted as NTFS) or a bunch of DVD's (the more data, the more DVD's).

Accessing Backups with Virtual PC or Virtual Server

Keep in mind that a CompletePC backup saves its data to a virtual hard disk file (`.vhd` extension). This is the same format used by Virtual PC and Virtual Server. Now the coolest part about this is—you guessed it—you can mount the virtual disk! Note, this doesn't mean you can boot up the VHD file, just that you can access the information off of it from an existing virtual machine.

Daniel Nerenberg
www.thelazyadmin.com

Ever wish you could grab just one file from a PC backup rather than having to restore the entire backup? Now with Vista CompletePC Backup you can! Using Vista CompletePC Backup, you can now create full backups of your entire hard drive to external media—for instance, a USB hard drive. To browse to the folder you specified, you need to drill down to the folder that contains the VHD file. Now that you know where the VHD is located, you need to open it. Using either Virtual PC 2007 or Virtual Server 2005, you can add the VHD to the list of hard drives installed on a virtual machine (VM) you have already created (a VM install on XP or Vista works best). Now turn on your VM as usual. When the VM is running, you should see the backed-up data listed as a new drive in your VM's hard drive list. You can pick and choose the files you need to recover.

Note: You need to ensure that the account you are using to run Virtual PC or Virtual Server has read/write permission on the VHD file. If the account does not, you might not see the drive and will not be able to mount it in Windows.

After your VM is up and running, you can see the backed-up data listed as a drive by going through My Computer (or Explorer). Philip Colmer (http://pcmusings.spaces.live.com/) says, "If you've got Virtual Server 2005 installed, there is also a command (`vhdmount`) that allows you to mount a VHD file as a virtual drive within a running system, so you don't need to start up a virtual environment."

Here is a story that demonstrates the real-world side to these solutions:

Bryant Likes, MVP
Senior Solution Developer for Avanade
http://blogs.sqlxml.org/bryantlikes

When I upgraded from Vista Pre-RC1 to RC1, I used the built-in backup program to back up my files. It worked very well for me so when I was upgrading from the Sept CTP to RC2, I decided to use it again. I also put a little more confidence in it and didn't do a completely thorough job of backing up my files (besides the full backup, that is). So, when I realized that I forgot to back something up, I fired up the backup program and pointed it to my Sept CTP backup. However, the tool complained that there were no backup sets on the drive. Hmmmm. I wasn't able to get the restore to ever recognize the backup set, but I did find that Microsoft is storing the backup as a VHD file. Those of you familiar with virtualization will know that that is a virtual hard disk. So, with some help from the Virtual PC guy (http://blogs.msdn.com/virtual_pc_guy/default.aspx), I was able to mount the VHD using Virtual Server R2 SP1 Beta 2's VHDMount utility (yes, that really is the product's name). So I now have a drive on my Vista RC2 machine that contains all the files from my Sept CTP machine and I can browse them and restore them at my leisure. Whoever made the call to back up to VHD, I owe you a beer. Great choice!

The "Virtual Machine Guy" is Ben Armstrong, program manager of the Virtual Machine Team (http://blogs.msdn.com/Virtual_PC_Guy/). He has some great advice to give. One cool trick he offers is to make some Registry changes using a `.reg` file that enables you to double-click a VHD file to mount it and right-click it to unmount it using the vhdmount tool from your OS (keep in mind that you need to download the tool for your Vista system, although it is installed automatically on systems running Virtual Server 2005).

Virtual Server 2005 R2 SP1 Beta 2 includes vhdmount, a tool that enables you to mount a virtual hard disk directly on your host operating system. Although vhdmount is provided as a command-line tool, a very small amount of work lets you mount VHDs by just double-clicking them. You can create a `.reg` file with the following contents:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Virtual.Machine.HD]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Virtual.Machine.HD\shell]
@="Mount"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Virtual.Machine.HD\shell\Dismount]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Virtual.Machine.HD\shell\Dismount\com
mand]
@="\"C:\\Program Files\\Microsoft Virtual Server\\Vhdmount\\vhdmount.exe\"
/u \"%1\""
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Virtual.Machine.HD\shell\Mount]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Virtual.Machine.HD\shell\Mount\command]
@="\"C:\\Program Files\\Microsoft Virtual Server\\Vhdmount\\vhdmount.exe\"
/p \"%1\""
[HKEY_CLASSES_ROOT\.vhd]
@="Virtual.Machine.HD"
```

Then if you double-click the `.reg` file (to load it into your Registry), you will be able to double-click a VHD to mount it and right-click it to dismount it.

Backup Status and Configuration

The Backup and Restore Center is the simple way to protect your data. But if you want to make some changes to the process, you need to use the Backup Status and Configuration tool found by selecting Programs, Accessories, System Tools (see Figure 8.2).

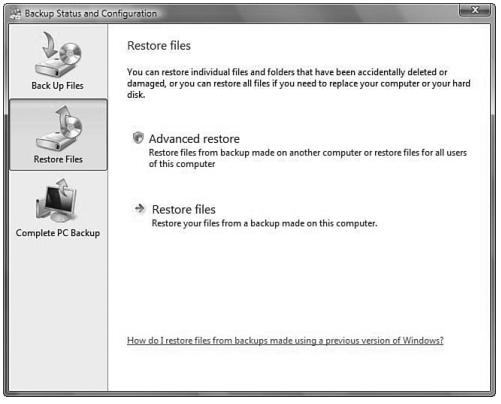

FIGURE 8.2

Backup Status and Configuration options.

It's from within the BSC options that you can choose which disk or network drive to back up to. You can also choose the types of files you want backed up regularly (Pictures, Music, Videos, E-mail, Documents, TV shows, Compressed Files, Additional Files, and so on). And the cool side to all of this is that you can schedule your backup to occur whenever you like.

The System Rating

If you open Control Panel and select System, you are greeted with some basic information about your system, including the version of Vista, the processor and memory settings, and even the Product ID (as shown in Figure 8.3).

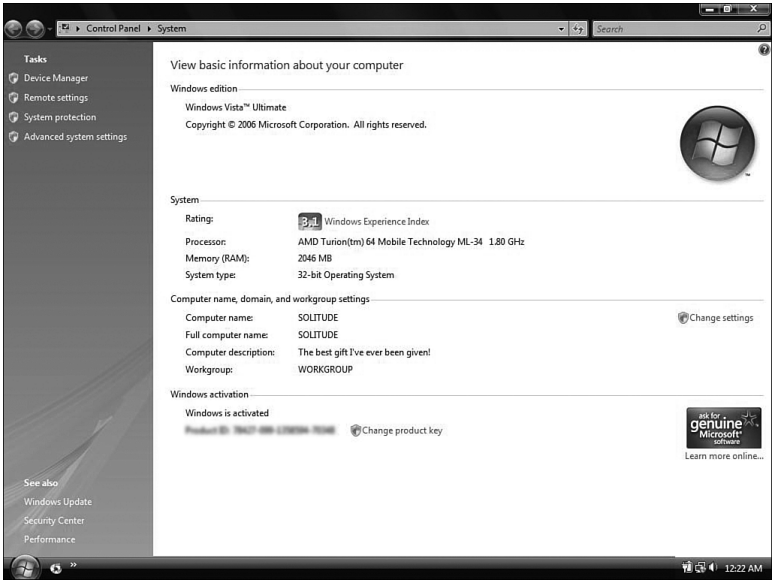

FIGURE 8.3

System information at your fingertips.

One of the more important pieces of information included in System Info is the system rating. This is calculated by Vista on a per-system basis, and it can be changed based on different hardware and configuration changes you can make to your system.

The rating (called the Windows Experience Index) is based on five ratings that are given to your system in the following categories: Processor, RAM, Graphics, Gaming Graphics,

and Primary Hard Disk. The final rating is not, as you might expect, a compilation of all the ratings; it's actually the lowest of the subcomponent scores.

You'll find a good explanation of the level indexing at http://news.softpedia.com/news/Windows-Experience-Index-Calculate-the-Vista-PC-Score-41047.shtml. In general, the levels indicate the following:

Level 1 = Vista capable (just barely)

Level 2 = Upgradeable (target) system

Level 3 = Value end machine

Level 4 = High end

Level 5 = High performance/gaming

Level 6 = Not yet defined

Keep in mind a couple of things regarding this score: First, it's usually wrong when you first look at it. Run it again! Select the link for the Windows Experience Index; then you can see the five subcomponents shown in Figure 8.4. Select the option Update My Score.

FIGURE 8.4

Rerunning the WEI—second time's a charm.

A big reason for this recommendation is that all the Vista gurus are up in arms over it. Mitch Denny ran the test on his "Ferrari 1000" and came up with an initial reading of 2.8. Ed Bott says he received the same score on his "Ferrari 5000." Keep in mind that it's because of the lowest rating that came from Aero settings on those systems. After readjusting a few settings and making sure they had the latest drivers and updates,

they re-ran the tests and they got better scores. The highest rating possible is a 5.9 (for now, obviously Microsoft can alter the settings as hardware improves).

What does that mean? Should we be going crazy to meet these numbers? Well, it depends on how your system is actually performing. The Microsoft help files tell you that a system with a base score of 3 will run Aero and function nicely. But others have run Aero with a lower base score. It's all in the details, and it all depends on what you are looking for.

Alan Wright
Hardware guru

You can alter the results of the WEI if you know how. You can find the XML file (its location is mentioned in the following section) and actually change the numbers. You should first save the original, make the numbers what you like, and then take another look at the tool. Sometimes it works; sometimes it doesn't. But it's fun to try to tweak the numbers.

One odd site on the Net for those who like to compete over these things lets you compare your WEI score to others. Some of these scores seem a little too good to be true, but check it out at http://www.shareyourscore.com/.

But as a Vista Master, you might want to know how the test is performed. When you kick off the update of the score, you can see that it asks for permission to run the Window System Assessment Tool (WinSAT).

Windows System Assessment Tool

For the most part, when you install an OS like XP, you get XP in all its glory, regardless of the box on which you are running it. So, although the underlying DLLs might be different, the OS options should be the same, right? Or should they? Does it really make sense that two systems, one of which is a $200 cheap-o box with cheesy hardware, should be put in the same position to handle the OS features of a mega system? Well, Vista has an underlying tool that helps to differentiate between the two. It's called WinSAT.

When you first install Vista, but before the first login, WinSAT runs its testing process to see what your individual system can handle. It takes that information to determine which operating system features should be enabled or disabled by default. For example, if your system cannot handle Aero, the settings on your OS reduce to Vista Basic mode.

One of the benefits to WinSAT that was discussed at the Microsoft Meltdown Conference in 2005 is that game developers can use the API to focus on the performance for their games as a result of the tests. The game can be developed so that, during installation, the WinSAT tool is run to tell the game which features should be enabled/disabled depending on your hardware. Logically, users who want to tweak their own games can do so, but at least initially the game will perform to the best of your system's ability because WinSAT has informed the game of where that level is.

Phillip Colmer
http://pcmusings.spaces.live.com

Many bloggers have written about the location of the WinSAT data store. The best of these blogs came from Tony Campbell on the http://vista.beyondthemanual.com blog site. He says, "The WinSAT utility creates its output in the system directory: `%systemroot%\Performance\WinSAT\DataStore`. Each time you run WinSAT, a new XML file is generated in this folder with the date of the assessment at the beginning of the filename—for example, `2007-01-01 12.00.00.000 Assessment (Formal).WinSAT.xml`. In addition, a file exists in this directory with the word *Initial* inside the bracketed part of the filename. This is the system performance assessment carried out when Vista was first installed on your PC.

Keith Combs (a technical evangelist with Microsoft for more than six years, http://blogs.technet.com/keithcombs) tipped us off from his blog site that we "should definitely take a close look at the information inside that file. We only present part of the information in the UI."

When you open the XML file, you can see the extensive level of tests that were performed and, instead of just a simple numerical response, literal response times for the tests run. The average user would never know what to do with all this, but it's cool to know what is happening on your system.

Problem Reports and Solutions

Found in the Control Panel (or by typing **`wercon.exe`** in the Search pane), this is a new tool in Vista to help you find solutions to your problems (as the name implies). So, when a program closes down unexpectedly it is recorded into a log that you can then request additional information about.

When you open the tool you see a list of tasks you can perform, including the following:

- **Check for New Solutions**—Sometimes (many times) your problem doesn't have a solution, so you can wait until a later time to try again. This will recheck all the problems you have listed in the log and see whether an update to the solutions is offered.
- **See Problems to Check**—Shown in Figure 8.5, you can see all the problems your system has had, the date, and any additional details that might be available. This option enables you to select check boxes for the solutions you want checked as opposed to checking for solutions to all the problems in the log of problems.
- **View Problem History**—Shows you a list of problems Windows has detected up to that point.
- **Change Settings**—You can have Windows automatically check for solutions to problems, or it can prompt you first. You have a variety of "consent levels" from which to choose. You can configure advanced settings, such as the ability to block reports being sent regarding certain applications.
- **Clear Solution and Problem History**—This is a quick way to erase all the recorded problems. After you've made the necessary changes or fixes, you might want a clean slate to start from.

> **TIP** One consent level you cannot configure through the Control Panel interface is the Send All Data option, which can be configured only through Group Policy settings. If this setting is configured within Group Policy, all the data is sent without prompts. You can also use Group Policy to completely disable sending these reports from your network systems. Or you can use Corporate Error Reporting.

The Problem Reports and Solutions tool uses a web browser control to help users control information sent back and forth between their systems and Microsoft, but Windows Error Reporting does the underlying work to request solutions. Those solutions can include instructions for fixing the problem, or a *workaround*; it could also include a link to the Windows Update website or to a Microsoft Knowledge Base article.

What Is Corporate Error Reporting?

Consider a scenario larger than just one system (for home users), such as an office with hundreds of systems with which you want to use the Windows Error Reporting (WER). The interface from Control Panel is great for a couple of systems, but analyzing data one system at a time would take forever. Event Viewer is helpful, and you can compile multiple logs, but Corporate Error Reporting is a better way to see the application errors on your network.

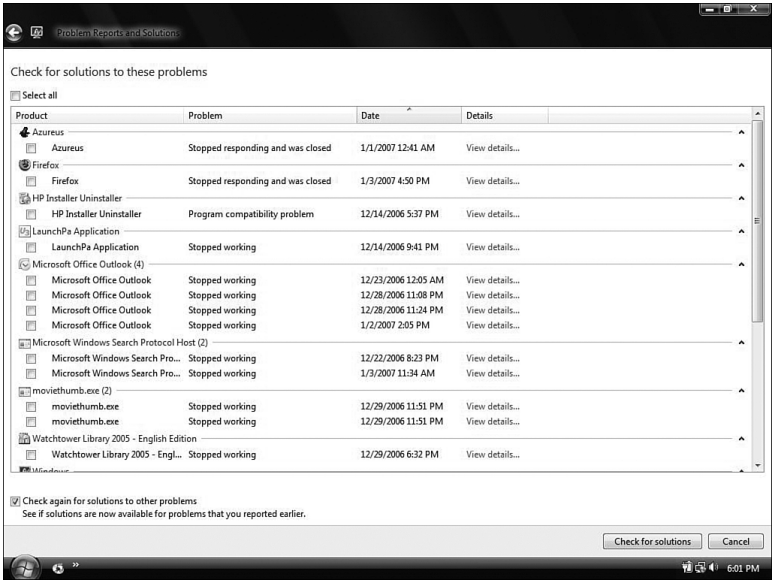

FIGURE 8.5

See which problems you want to check with Microsoft about solutions.

To set this up, you use Group Policy to redirect your error reports to an intranet server using the Corporate Windows Error Reporting GP setting. Then you need to get the analysis programs from Microsoft so you can gather and filter through the many errors you will receive before sending it to Microsoft.

To learn more about Corporate Error Reporting, check out the website http://www.microsoft.com/resources/satech/cer/.

Microsoft organized the error reports into *bucket* categories. With user-mode crashes, these buckets are defined by the name and version of the application, along with the module name and version. With kernel-mode crashes, the bucket includes the stop codes and associated parameters. You can discover the bucket associated with your particular application problem by going through Event Viewer, opening the application logs, and then finding the application crash that relates to your problem. The event includes the bucket number, which Microsoft keeps track of.

Microsoft keeps track of the buckets. Chris Pratley (Microsoft program manager; http://blogs.msdn.com/chris_pratley) discusses how this works on his blog site.

Chris Pratley
Microsoft Program Manager for the Office Team
http://blogs.msdn.com/chris_pratley

When you report the crash, if that is a crash that someone else has already had, we increment the count on that "bucket." After a while, we'll start to get a "crash curve" histogram. On the left will be the bucket with the most "hits." On the far right will be a long list of "buckets" so rare that only one person in all those millions had that particular crash and cared to report it. This curve will then give you a "top N" for crashes. You can literally count what percentage of people would be happier if we fixed just the top 10 crashes.

An article was posted in the October 9, 2006 issue of the *New York Times* by John Markoff called "After a Debugging Race, Will Vista Measure Up?" In it he described the concepts of the 80/20 rule, which basically says that fixing 20% of the coding problems Microsoft gets eliminate 80% of the problems users are exposed to. The point is clear, though, that Error Reporting has assisted in significantly reducing the number of bugs in Vista and Office 2007 software. So, this is one set of features to be thankful for.

Keep in mind that error reporting is a submission tool that should be used in order to help fix existing problems and to create service packs and other updates. Although users may not get a personal response, the information they submit is included in a database for fixes and updates.

Reliability and Performance Monitor

"It is an immutable law in business that words are words, explanations are explanations, promises are promises but only performance is reality." What Harold S. Geneen, CEO of ITT from 1959 to 1977, was trying to say is that "talk is cheap," but performance stands on its own. The question for computer users is how do we determine whether our computers are performing up to par.

Each computer has a baseline. A *baseline* is the optimum, standard way of operating for a computer under its current set of hardware and software. Once you know your system's baseline, you can watch to see whether time or a new application takes a toll on the system's performance and reliability. But literally "seeing" that happen requires a good performance monitoring tool. Vista includes a new version of its Performance Monitor of old.

Reliability Monitoring

What is your standard method for determining the reliability of your system? Most of us determine a system's reliability by how long it has been since it has blue-screened on us or forced us to reboot. Not a truly "technical" way to assess reliability, huh?

So, it is with open arms that sys admins welcome the new reliability monitor. To open it, you can type **`perfmon.msc`** into any Search field or go to your Administrative Tools and select the Reliability and Performance Monitor.

The main goal of the reliability monitor is to keep track of reliability events that have been defined as changes to your system that could alter the stability or other events that might indicate system instability. Events monitored include:

- Windows updates
- Software installs and uninstalls
- Device driver installs, updates, rollbacks, and uninstalls
- Application hangs and crashes
- Device drivers that fail to load or unload
- Disk and memory failures
- Windows failures, including boot failures, system crashes, and sleep failures

Figure 8.6 shows a system that is becoming more unreliable over time. You can literally watch as your Vista decays. Using the monitor, you can see what is causing the instability. Is it an application or a set of applications? Did it begin with the addition of something new?

The System Stability Chart gives you a visual on how reliable your system looks over time. You are given an overall stability index score: 10 is perfection; 1 is the lowest. The Reliability Monitor retains up to a year's worth of data so you can really see how your system has been performing.

If you see a drop in the stability, you can check the date the drop began and then see if it was one of the following that caused the instability: Software (Un)Installs, Application Failures, Hardware Failures, Windows Failures, or Miscellaneous Failures.

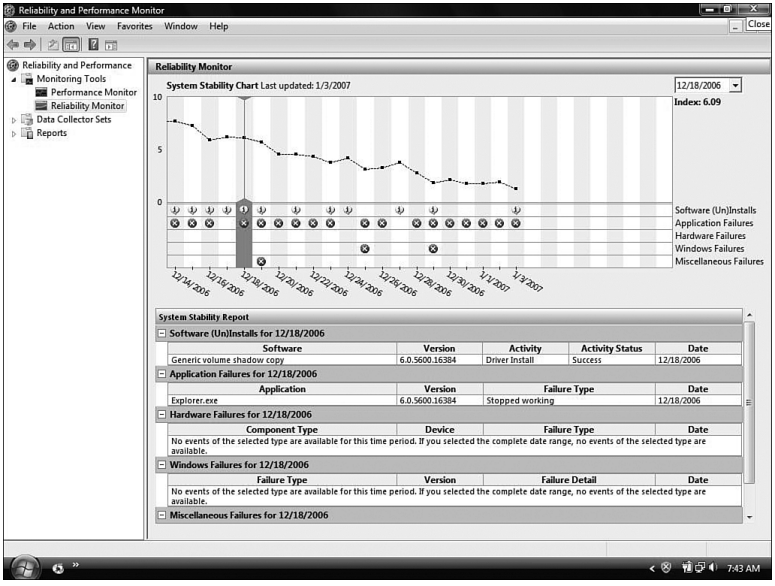

FIGURE 8.6

Reliability Monitor lets you see if your system is something you can depend on.

Many have questioned the validity of the Reliability Monitor. Some of the questions asked by prominent writer Ed Bott include:

If my Stability Index slips below 5, is it time to do a complete reinstall? Is it really fair to conclude that my overall system stability dropped from a perfect 10 to 8.17 because Explorer crashed twice on May 25, or that it then slid all the way down to 5.77 the next day because OneNote 2007 Beta 1 stopped working twice (and hasn't failed since)?

The monitor, especially that line chart, needs to be taken with a grain of salt. Its real strength lies in an organized way to see system performance decline based upon specific, recorded situations.

Resource Monitor

The Resource Monitor isn't a different tool, actually. When you first open the Reliability and Performance Monitor, you are presented with real-time views of your CPU, disk, network, and memory in four charts. You can

NOTE

You can stop the Resource Monitor by clicking the Stop button on the toolbar. You can also quickly navigate to any of the more detailed lists by putting your cursor over a chart (it forms a target icon) and clicking in the chart.

click down arrows next to each category to see a more detailed list of what is being done by any one of those resources at that moment (see Figure 8.7).

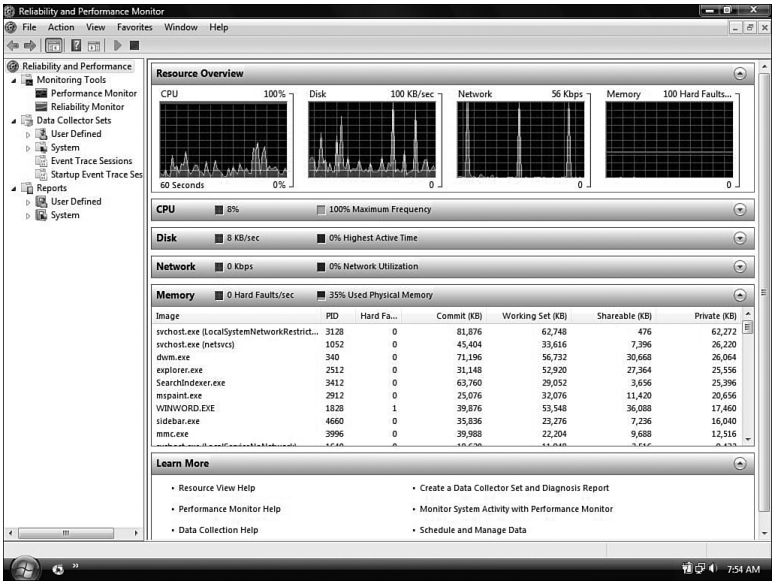

FIGURE 8.7

Resource Monitors let you see your system activity at that moment for CPU, disk, network, and memory.

Performance Monitor

This tool shows you a visual representation of your system so you can inspect a variety of components, beyond what the Resource Monitor shows you. Initially, you won't see more than the % Process Time initially displayed. You can add more performance metrics, called *counters*, by clicking the + sign. When you first see the number of possible counters and instances, you can see that the task of choosing which items to monitor can be overwhelming (see Figure 8.8). Any given system has roughly 85 different performance objects (you can monitor the local system or a remote one). Each of those objects contain counters (there are way too many to know them all). After you have all your counters set up, you can make changes to the way they are displayed. For example, you can change the line colors for each counter to make it easier to determine which line you are watching. You can change the format of the display from a graph to a histogram to a report (numeric display).

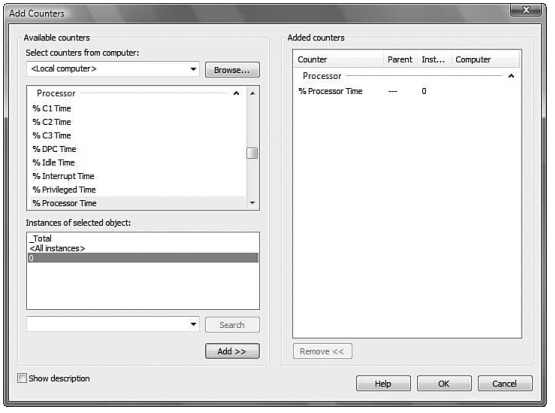

FIGURE 8.8

Adding counters to your performance monitor can be a daunting task.

Baselines and Bottlenecks

Before you can truly know the performance of your system, you need to be able to compare it to something. A *baseline* is a collection of performance data for your system over a set period of time that indicates where your system normally performs under normal working conditions. Without a baseline you have nothing with which to compare your system. You need to compare it to itself at a better time in its past, if that makes sense. When you do see items in the future that indicate your system is running more slowly, these are called *bottlenecks*, because they are tying up your system's traffic in some way. You need to eliminate bottlenecks.

John Kellett (http://www.johnkellett.co.uk) gives the following advice about creating your baseline:

You may want to take a baseline reading with Performance Monitor before installing an application, install the application, and then take the reading again using the same Performance Monitor counters while the application is in use. Taking the baseline reading itself has been known to throw up a few issues. If your system has decent hardware and a user that doesn't really push it to the limit, I would be expecting the system to be pretty much flatlining. If one counter is a lot higher than you are expecting, then you can troubleshoot this before going any further.

Keep in mind that even though you technically can monitor and perform a baseline remotely, because of the congestion on a network for remote monitoring, Microsoft

recommends that you perform baselines locally. In addition, you should log across multiple days at multiple time intervals to really see the performance. Finally, you should check the system's baseline at regular intervals (once a month or every other month) to see how it's doing. Keep in mind that, for larger networks, you might want to obtain third-party monitoring solutions.

Important Objects and Counters to Monitor

We already mentioned that you have many options from which to choose when using Performance Monitor. That's why we went to the masters to ask them which ones are the most important ones to know.

Richard Brucrew of Sebring, Florida, remembers some of the important ones that were important according to the Microsoft exams to be an engineer. Here are some of the exam objects and counters:

Memory

- **Pages/sec**—Over 20 pages/sec could indicate too little RAM. This counter shows the transfer of data from the physical memory in your system to your pagefile. When these counters are too high it indicates a memory shortage. What's the solution? Adding more memory to your system might be your first thought, but before doing that you should consider stopping unnecessary services and background applications that might be using up your memory.
- **Available Bytes**—This should be more than 4MB. If it drops under 4MB, this indicates a memory issue. This setting monitors the amount of memory that is available after the working sets of applications and the cache have been served.

Derek Melber
Independent technical trainer and consultant
From Windows XP Professional Exam Cram, 1st Edition

Memory is often the first performance bottleneck in the real world. The counters related to processor and hard drive utilization might be well beyond their thresholds simply because inadequate memory is causing paging, which impacts those two components.

Processor

- **% Total Processor Time**—A continuously high value can indicate a bottleneck. Anything over 80% for extended periods of time should give you cause to worry. Make sure, though, this isn't during the running of some of those elaborate screensavers (they take up a lot of processor time when running) and that your memory isn't the main cause for the problem.

- **Processor Queue Length**—This should be less than 2, on average. This measures the number of threads waiting in the queue to be processed.

Disk

- **Logical Disk: % Free Space**—Lets you see how much space you have left on your disk.
- **Physical/Logical Disk: % Disk Time**—This counter shows the amount of time spent reading and writing requests. Anything from 50% to 100% indicates a bottleneck.
- **Physical/Logical Disk: Disk Queue Length**—Similar to the processor queue, this should be under 2 for read/write requests that are pending.

TIP Although a high processor time can indicate the need for a faster processor, you should check the queue length, too. If this is above 2 on average, you might consider adding a second processor or trying to remove pressure from your system by moving certain processes to other systems.

TIP Where do you turn next? To Guy Thomas, Microsoft MVP). He has a lot of information on his site regarding performance counters. He has an ebook titled *The Art and Science of Performance Monitoring* that is worth downloading from http://www.computerperformance.co.uk/ebooks.htm.

Data Collector Sets and Reports

Although the real-time view of your system is fun to watch for about a minute, to really collect data and manage it for future comparison you need to know about data collector sets and reports, which are new to Vista.

Data Collector sets allow you to put together a collection of alerts and thresholds that allow you to monitor your system immediately or over a period of time. Data collector sets can contain the following types of data collectors: performance counters, event trace data, and system configuration information (including Registry key values). You can create a data collector set from a template, from an existing set of data collectors in a Performance Monitor view, or by selecting individual data collectors and setting each individual option in the data collector set properties.

Nathan Greal
Network admin and Internet blogger

The library of data collector sets you can configure may seem a bit overwhelming. Start off by setting your performance counters and then saving that as a data collector set. Then you know exactly what you are monitoring. You'll graduate over time to the bigger items.

Performance logs are created with a `.blg` extension and are kept in the Peflogs folder by default. You don't open them from the folder, but from within Performance Monitor itself. If you want to convert these `.blg` files to other types or you review your logs frequently to see recent data, we recommend that you use limits to automatically segment your logs. You can use the `relog` command to segment long log files or combine multiple short log files. Type **`relog /?`** from a command prompt to learn more about this tool.

System Diagnostics Report

Data collector sets are absolutely incredible. Diagnostic capability in Vista is much better than in previous versions. Previously, we mentioned that you can set counters, save these as a data collector set, and view your log files. This has been available for some time. But moving to the next level, you can configure a more granular view of your system. To prove it, there are system data collector sets that really impress us.

Nick White, Microsoft product manager for Windows Client, has this to say about Vista's diagnostic capabilities:

To see a quick system checkup, you can do one of the following:

- The simple method is to open Control Panel, go through System and Maintenance, and then click Performance Information and Tools (or you can go through the System applet and select the Windows Experience Index). In the Tasks pane you can select Advanced Tools. Many items are available that you might consider for later reference (quick links can be found to several performance tools, and you might also note some performance issue tips at the top to help you fix some of your performance problems). Locate the Generate a System Health Report option and then wait one minute while the test runs. You'll notice that, even though you went through a different path, you are still using the Reliability and Performance Monitor to run the report.
- Another way to run the same report is to do it from the Reliability and Performance Monitor itself. Open the tool; then from the system data collector sets, you'll notice four preconfigured tests. Select System Diagnostics, right-click, and select Start. Then, under Reports, open System Diagnostics and select the report that is running (the latest one). You will see that it's the same as the previously mentioned method.
- The simplest method to run the test is to open a command prompt (elevated ornonelevated—it asks you for permission to proceed if it is nonelevated) and then type **`perfmon /report`**.

TIP One of my favorites, as with many others here internally at Microsoft, is the ability to create a System Health Report. This report will help you diagnose your system's health and provides possible solutions [to] issues that may be affecting your PC's health.

You might wonder why you should use this complicated way when you could use the simple Control Panel method. It's a fair point; however, the Control Panel method doesn't give you the other three preconfigured tests—namely, LAN Diagnostics, System Performance, and Wireless Diagnostics. These are also great to work with from the new diagnostics tools to see how your system is doing.

NOTE If you wanted to run a different data collector set, you could type **`perfmon /report "Name of Data Collector Set"`** to start it.

System Information Tool

In scouring the world for Vista Masters, we gathered together a few additional tools and tricks for you to use. First is System Information (located under Accessories, System Tools). D. David Dugan, the president of DD&C (http://www.dugancom.com), an IT consulting and solution providing organization, has written several posts regarding the importance of the System Information tool (`msinfo32.exe`). This free tool will really surprise you with the level of detail regarding your system's hardware configuration, the components in your system, and the software installed (including drivers and the services that are running). If you aren't sure whether this tool has value for you, just open it one time. Just once and you will clearly see the level of immediate information that is placed before you…and you'll love it.

You'll notice a high volume of Vista tips and tricks sites on the Web, and most of them will offer the same information. Computer Power User (http://www.computerpoweruser.com) gave us this tip that was worth repeating:

Vista users have a hidden resource, systeminfo, that gives them a quick, comprehensive snapshot of their installed hardware and even minutiae such as the original installation date of the OS, BIOS version, installed and available memory, and much more. To bring up systeminfo, click Start, Run; type **`cmd`** in the Open field; and click OK. At the command window prompt, type **`systeminfo`** and press Enter.

What's New in Task Manager

Task Manager, for many of us, is our go-to guy for problems. You have a problem; you go to Task Manager—it's almost ingrained in us. You'll see quick and dirty information about your processes, CPU usage, memory, network, and so forth. So any changes that can benefit us are worth considering.

For one thing, the first time you start it you'll see that you can see just your computer's processes. You can also choose to see processes from all the users of the system. One

thing you'll notice right away is the new Description aspect to the Processes tab (see Figure 8.9).

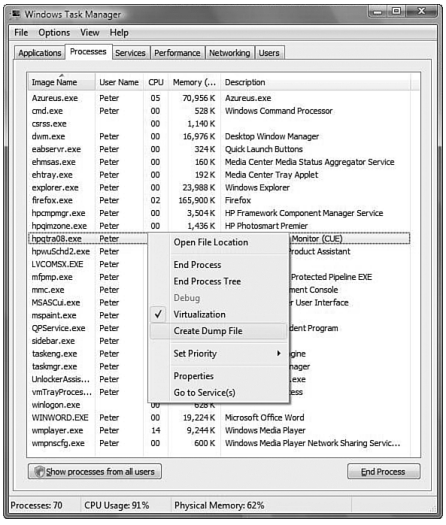

FIGURE 8.9

The new Task Manager adds a Description column and a Services tab.

One of the new features of Task Manager is the capability to create a minidump file of an application that is running. You can right-click an application or process that is running and select Create Dump File (refer to Figure 8.9). You will be presented with a dialog box that shows you where that file has been written. You can use this feature to discover why a particular application might be crashing so often; conversely, if a process has already crashed and is no longer responding, you can try to discover the cause.

After you have the dump file, you need to install the symbols for Vista (which you can get at http://www.microsoft.com/whdc/devtools/debugging/symbolpkg.mspx) and then install the latest debugging tools (which you can find at http://www.microsoft.com/whdc/devtools/debugging/default.mspx). Then, as Mitch says, "Then, I can run the Windows Debugger (WinDbg), load the symbols, open the crash-dump file, and try to determine what went wrong."

NOTE Mitch Tulloch, a Microsoft MVP and president of MTIT Enterprises (www.mtit.com), gave some great pointers on using the new Task Manager in an article in Windows Networking.com (http://www.windowsnetworking.com/articles_tutorials/Managing-Processes-Tasks-Windows-Vista.html).

Obviously, that sounds a lot simpler than it really is. Reading dump files is a specialized talent that requires a bit of study and research on the Web. But there is a starter article for beginners at http://www.microsoft.com/whdc/devtools/debugging/debugstart.mspx.

What Else Can Task Manager Do?

There's still more that you can do with Task Manager. For one thing, it now has a Services tab. From here, you can see all your services, some descriptive information regarding them (description and group information), and whether they are running. You can stop or start services from here. So, now you don't have to open your Services console to simply stop or start a service. You will still need to use that console if you want to do any permanent service adjustment (disabling a service, for example).

You can also right-click an application and select the Properties option, which is new in Vista. This allows you to go the properties of that particular executable so you change things such as the Compatibility options or other aspects of the program.

Process Monitor v10.21

Some of you might already be using tools created by Mark Russinovich, such as Filemon and Regmon. These are some of the most popular tools Sysinternals has offered the world. Microsoft acknowledged the strength of these tools and has acquired Mark's abilities with his tools. They are still offered freely on the Microsoft site at http://www.microsoft.com/technet/sysinternals/.

Filemon and Regmon had some limitations, such as a lack of detailed event information, limited filtering, poor scalability, and no insight into process events. Process Monitor, on the other hand, offers all those features. It has been likened to putting Windows under an x-ray machine. The tool is free on the Microsoft TechNet site. Learning to use it may take some time, though.

You'll never have the advantage of Mark Russinovich sitting in your living room and explaining to you the inner workings of his tools, but here is the next best thing: a set of videos Mark made with David Solomon that are absolutely incredible. You can get them from the Microsoft site, or the Solomon site at http://www.solsem.com/videolibrary.html.

If the videos seem a bit pricey for you (although they're worth every penny), you can check out their book, *Microsoft Windows Internals, Fourth Edition: Microsoft Windows Server 2003, Windows XP, and Windows 2000 (Pro-Developer)* (hardcover; ISBN 0-7356-1917-4).

Memory Diagnostics Tool

It's a fact of life that memory problems are hard to diagnose, and it's frustrating if you are the one dealing with them. Microsoft used to make the memory diagnostics tool available as a separate download for those in the know, but now it's included in the Vista OS.

In fact, two tools are running in the background to address memory issues with Vista. The first one is titled Resource Exhaustion Detection and Recovery (RADAR), runs completely in the background, and monitors the system-wide virtual memory commit limit. That is to say, it basically keeps track of all your virtual memory on the system, so it can tell when your virtual memory is running low and also identifies which programs are using the most virtual memory. When it detects a shortage of virtual memory, it displays a warning and lists the highest-level offenders for you to shut down. This is a nice enhancement from earlier times where you had to start shutting down programs to conserve virtual memory but couldn't be sure which ones were the culprits.

TIP If you want to see RADAR in action, you can use Performance Monitor. RADAR divides the current level of committed virtual memory by the commit limit, which is the maximum size of the paging file. When the percentage reaches 100%, RADAR warns you. However, you can set the Memory object in Performance Monitor to track the % Committed Bytes in Use counter and the Committed Bytes and Commit Limit counters. This gives you a visual representation of what RADAR works with in the background.

TIP Sometimes you might be surprised if your memory gives you a problem. Kerry Brown, Microsoft MVP, says, "Get a second opinion here http://www.memtest.org/."

The other tool is Memory Diagnostics, which also runs in the background (if it discovers a problem, it runs diagnostic tests, which is added to the event logs), but you can kick start it if you think your system is having memory issues. You can run the tool from the Administrative tools or from a command prompt: MdSched.exe. You'll have to restart the computer for the test to be run, so be sure you save your work before the test.

To get a more detailed look at the tool, you can download the User Guide from http://oca.microsoft.com/en/windiag.asp.

But what if you cannot even install your OS or boot to your OS to run this tool?

Parveen Patel
Developer on the WinRE team blog
http://blogs.msdn.com/winre/default.aspx

Running Windows Memory Diagnostic without installing Vista. I have gotten multiple queries on this. Yes, it is possible to run Windows Memory Diagnostic without installing Vista!

You can do it through the Windows installation disc. To run memory diagnostic, insert the installation disc in the computer and reboot. When you get the prompt `Press any key to boot from CD or DVD`, press and hold the spacebar or tap it multiple times. This should bring up the Windows boot manager menu that lists Windows Memory Diagnostic as an advanced tool. Hit the Tan key to select Windows Memory Diagnostic and then hit Enter to run it.

After Memory Diagnostic is done, the machine will continue booting into the installation disc.

The System Recovery Options (shown in Figure 8.10) have a variety of tools, including Memory Diagnostics. By using this tool, you just might find out why Vista isn't installing.

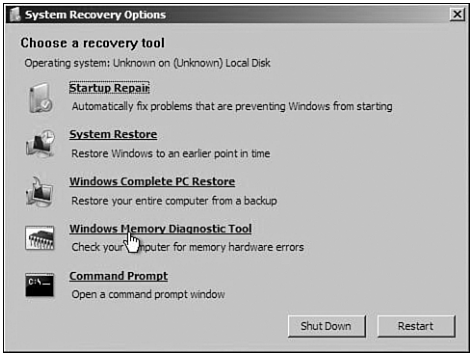

FIGURE 8.10

System Recovery options using the DVD.

We are discussing Memory Diagnostics, but you'll note that Figure 8.10 shows several other important recovery options you might need at any given time to restore your system or bring it back from a major issue. One of those is Startup Repair. In the event your system cannot start, try this option. The Startup Repair Tool (SRT) looks through startup logs and runs a set of diagnostics to determine the failure's cause. It could be incompatible or corrupted device drivers, missing or corrupted startup configuration files, or even corrupted disk metadata. SRT attempts to fix the problem. If it does, it writes to a log file to let you know what the cause was. If it cannot, it tries to use the Last Known Good Configuration as a last resort. If this doesn't work, it writes the diagnostics information to a log and offers to assist you in trying to fix the problem yourself.

The SRT log is located at `%WINDIR%\System32\LogFiles\Srt\SrtTrail.txt`.

Parveen Patel
Developer on the WinRE team blog http://blogs.msdn.com/winre/default.aspx

In this post, we describe how to use Startup Repair to repair a missing file that is preventing Windows Vista from booting. The goal is to familiarize yourself with Startup Repair so that you can use it when you or your customers need it. We really hope no one will need to use it :); but if you do, this knowledge might come [in] handy.

Warning: Try this at your own risk. If things don't work as planned, you might not be able to boot into your Vista installation or might even lose your data.

Preparation: Before we try to make Vista unbootable, please make sure that your machine has a good restore point. The restore point is not needed for file repair, but would be useful if things go wrong. To create a restore point: search for System Restore in the search box from Vista's Start button, click on Open System Protection, click Create. And then follow the instructions to create a restore point.

Making Vista unbootable: To demonstrate how to use Startup Repair to repair a file we will move the `%windir%\system32\winload.exe` file, which is a must-have for booting Vista. We cannot easily delete this file from Vista itself, so we'll use WinRE to delete it, as follows:

1. Boot into Vista installation DVD.
2. Choose your language settings and click Next.
3. Click Repair Your Computer.
4. Choose your operating system and click Next. This should bring up System Recovery Options.
5. Click on Command Prompt.
6. Once on the command prompt move the `winload.exe` file from your Vista installation. For example, if Vista is installed on C:, run

   ```
   move C:\Windows\System32\winload.exe
   C:\Windows\System32\winload.exe.backup
   ```

7. Now restart your computer using the Restart button on System Recovery Options.

Your Vista should now fail to boot! It should instruct you to use Repair Your Computer from the Vista installation disc.

Repairing your computer: To repair your computer using Startup Repair follow these steps:

1. Boot into Vista installation DVD.
2. Choose your language settings and click Next.
3. Click Repair Your Computer.
4. Choose your operating system and click Next. This should bring up System Recovery Options.
5. Click on Startup Repair.

Startup Repair should now start diagnosing your system to identify the root cause of the failure. Once it has identified the root cause, it would automatically start repairing your computer. If you are curious to know what Startup Repair did, you can click on the details link and see which tests Startup Repair ran to diagnose the problem.

After Startup Repair has finished the repairs, click Finish to reboot your computer.

Your computer should now be able to boot normally into Vista!!

Note: If your computer cannot boot into Vista even after repairs, then go back to System Recovery Options and run System Restore.

That's it! This is how you use Startup Repair for most unbootable situations.

ReadyBoost and SuperFetch

We've talked enough about discovering performance inhibitors; now let's get into the performance enhancers: ReadyBoost and SuperFetch.

ReadyBoost

Every Microsoft Engineer knows the one magic trick Microsoft encourages toward better performance and a stable OS is more RAM. Logically, this is not always an easy thing to achieve. Sometimes, for example, you might find yourself as one tech did (whom we shall name Charlie), needing more memory to install a virtual server on his system. He needed the memory immediately but couldn't get it where he was (in the middle-of-nowhere Florida visiting parents). ReadyBoost could have been Charlie's solution if he were running Vista, but he wasn't. Sorry Charlie.

ReadyBoost allows you to add "memory" to your system by adding a USB 2.0 keychain drive (you can use SD cards, too) to your system. You might be wondering why we used quotation marks back there: You are not actually adding memory to your system; in

actuality you use memory from your flash drive and allow it to work like a virtual cache for your hard disk. Vista can use some or all of that drive as added memory. Although hard disks are faster for large sequential I/O, ReadyBoost improves performance on the smaller random I/O.

No doubt you have questions, as many did when this was first released. Tom Archer posted a list of Q&A with Matt Ayers (the program manager in the Microsoft Windows Client Performance Group, which basically owns the ReadyBoost feature) at http://blogs.msdn.com/tomarcher/archive/2006/06/02/615199.aspx.

You can read the entire discussion at the site, but here are the highlights (and we'd like to thank Tom Archer for sharing them with the world):

First, you should know that not all USB devices will work (which you may have already discovered if you tried using ReadyBoost with your keychain USB). Performance-wise, Matt Ayers says you need 2.5MB/sec throughput for 4KB random reads and 1.75MB/sec throughput for 512KB random writes. You can use up to 4GB of flash with ReadyBoost (which turns out to be 8GB of cache thanks to the compression). The reason for the 4GB limit is that FAT32 is being used. The smallest size is 256MB, but the recommendation is that you use at least a 1:1 ratio with your system's memory, with 2.5:1 being the high end.

If you remove the drive, nothing bad happens. Because all pages on the device are also on disk, nothing is lost. As for security, everything is AES-128 encrypted.

Make sure your drive is ReadyBoost capable; otherwise, you will find yourself frustrated that it doesn't work like you hoped.

NOTE

It's good to note trends in the vernacular of computer geeks over the years. In recent years with storage becoming a central player, we heard words like *ubiquitous* and *heterogeneous*. The word for 2007 seems to be *heuristic*. Instead of using it in the wrong context or nodding in agreement when it's tossed out in conversation, let's just put a definition on it. One online dictionary defines it this way: "A computational method that uses trial and error methods to approximate a solution for computationally difficult problems."

Sounds a little iffy for a solution to a computer speed problem, right? Well, it's not a perfect science. It's what you might call an educated guess about what you're going to use. Suse Linux kernel developer Andrea Arcangeli says, "In many cases, preloading new memory means flushing away an existing cache." So it's not a risk-free, perfect arrangement.

SuperFetch

Improving performance requires getting over the disk I/O bottleneck. Windows XP has a technology called Prefetch, and this is the next generation of that feature—hence the name SuperFetch. These technologies improve memory management by keeping track of which applications you use most often and keeping them ready to load in

memory. It also reorganizes data and applications on your hard disk to make them more available for loading into memory if it notes the need.

Jim Allchin, co-president of the Platform and Services Division, says, "We redesigned the memory manager in Windows Vista so that if you give the system more memory, it uses that memory much more efficiently than previous operating systems via a technique called SuperFetch—part of Windows Vista's intelligent heuristic memory management system."

SuperFetch uses an intelligent prioritization scheme that not only determines which applications you use most often, but also the time of day you use them. So, if every morning you start with your Firefox browser, that is preloaded in the morning for you. If you go to lunch at noon every day and start work again at 1 p.m., SuperFetch can have your applications ready for you at that time. This solves one of the problems we always had in previous Windows versions—the fact that leaving the OS idle for any period of time made the OS think it should just begin working on its background processes. But with SuperFetch, it knows to keep your applications ready.

To truly understand this technology, it would be good to ask "why" our post-lunch XP boxes were so sluggish. With an OS that uses demand paged virtual memory, when more physical RAM is needed, data gets flushed to the pagefile. So, when a person goes to lunch and another process starts to run on the machine during that time, all the person's applications and data are pushed to the paging file. So, we understand why it's pushed out, but when those other processes finish, nothing automatically calls that information back. When you sit down and start working, the system is sluggish because it's being forced to swap the data back into physical memory. SuperFetch foresees this problem and tries to be proactive about putting the applications you need back into physical memory.

You don't configure SuperFetch; it works all on its own. A folder called Prefetch is located under the `C:\Windows` directory, and some have suggested making changes to this folder, but read the following note.

Where Is My Memory?

One of the complaints users have with SuperFetch (due to a lack of understanding) is that they remember how much available memory they had under XP's memory manager, and now in Vista, when they check out their available or free memory, it's next to nothing. Why is that?

Jeff Atwood addresses this on this site www.codinghorror.com. He explains the need to consider your memory as a cache, not as a resource. A cache that is empty isn't doing

you any good, so Vista is trying to fill it with as much preemptive material as it sees fit using SuperFetch. Jeff says, "The less free memory I have, the better; every byte of memory should be actively working on my behalf at all times."

At the same time, Jeff makes a good comment in his article that one downside involves gaming. Some games rely on free memory that SuperFetch sees as available and takes. There are different opinions on whether all this is true, with arguments on both sides, but for us, we just want to know if we can disable SuperFetch if we want to.

Fortunately, SuperFetch can be disabled in a couple of ways. The easiest is to go into the Services tab through Administrative Tools and disable or temporarily stop the SuperFetch service.

You can also disable this in the Registry. Open the Regedit and check the value of `EnablePrefetcher` and `EnableSuperfetch` in the Registry under the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\MemoryManagement\PrefetchParameters` Registry key.

Here are the descriptions of these values:

- 0 = Disabled
- 1 = Application launch prefetching enabled
- 2 = Boot prefetching enabled
- 3 = Prefetch everything enabled (optimal and default)

The recommendation is that you ensure that it's set to 3 and leave this alone…but tweakers love to tweak.

NOTE

Mythbuster: It's not often you can crush a myth that has been propagating for years (no, we aren't talking about the whole Bill Gates will give you thousands if you respond to this email myth). What we are talking about is the myth that you can clear out your Prefetch folder (in XP or Vista) or add a Registry key that enables SuperFetch for XP. The biggest advocate against this myth is tech guru Ed Bott, and you can read his tirade against it in his archives at www.edbott.com.

At `C:\windows\prefetch`, you see a set of files with names that are related to your programs and with a `.pf` extension. This information was used and is used by Windows in fetching technology to improve performance. Some have said clearing this out improves performance. The basic answer is this: Don't clean out the Prefetch folder because it will not improve performance, even though some tips on the Web say otherwise. Windows manages the folder just fine and will only cause more work because Windows will just replace that information. As for adding a Registry key to XP, from the highest sources, this is not accurate.

Vista Recovery: Advanced Boot Options, WinRE, and WinPE

The last thing you want to happen is for your system to not boot. Performance is a great thing to worry about right up to the day your system shows you a black screen with an error message instead of the colorful login screen. With a lump in your throat, you sigh with relief because you know you have a CompletePC backup…or do you? Before you go for the backup, you should try to fix your problem. Start with Advanced Boot Options.

Advanced Boot Options in Vista

By pressing F8 upon bootup, you can see the Advanced Boot Options available to help you to handle a particular crisis. Knowing how each works can enable you to make an informed decision about which tool is going to get your system up and running the fastest. Here are your choices:

- **Safe Mode**—Loads a minimal driver set and set of services.
- **Safe Mode With Networking**—This loads safe mode settings but also loads network connections, allows logon scripts to run, allows security settings and Group Policy settings (for system that connect to a domain) to be applied. If you know it's not a network problem that is preventing your system from booting, this mode can be helpful to allow you access to other resources (and to back up your system if you haven't done so already).
- **Safe Mode with Command Prompt**—Boots up your system but with a command prompt instead of the GUI. Why would you use this? Well, if you believe the system will not start due to a problem regarding a process started through the Explorer shell, this prevents the Explorer shell from executing in the first place.
- **Enable Boot Logging**—Creates a log file that lists all the services and drivers that load (or do not load, as the case may be). This log file is called `Ntbtlog.txt` and is located in the Windows folder. The modes listed previously also create boot logs, but this one does it without going into a safe mode.
- **Enable Low-resolution Video (640×480)**—This used to be called VGA mode in XP. Useful for problems you encounter with video drivers or incorrect video display settings, it provides a standard (ugly), stable (low-resolution and refresh rates settings), VGA driver to allow you to see your screen so you can fix your problem.
- **Last Known Good Configuration (Advanced)**—The last time you logged on successfully, your Registry took a snapshot and saved it. In the event you did something to your system and it prevents you from logging in again, not to worry—just use the last known

good to go back in time to your last logon. However, if you are able to log in after a poor installation of a driver or service, this option will not help you in the least. So, if you know something isn't right, don't log in first and then see whether you are right. Instead, go with your gut feeling and last known good. It doesn't solve problems caused by corrupted or missing drivers or files—that requires WinRE, which is discussed later.

- **Directory Services Restore Mode**—This setting applies only to domain controllers, so you don't need this for your desktop OS.
- **Debugging Mode**—This enables Vista to send debugging information through a serial cable to another computer for troubleshooting the kernel and other analysis of the system.
- **Disable Automatic Restart on System Failure**—This is useful for when your system is in a loop of restarting because it stops the blue-screen restart loop so you can troubleshoot the cause of the problem.
- **Disable Driver Signature Enforcement**—Allows drivers with improper signatures to be installed. This setting does not continue with multiple reboots. You use it; you install the driver you need; and when you reboot, the Driver Signature Enforcement is enabled again.
- **Start Windows Normally**—Starts the system normally, as you might have guessed.

Nick Peers, the freelance journalist (http://www.nickpeers.com) says:

A damaged Registry can lock you out of your system and important files. The Registry is a massive database that contains all your system and program configuration and is central to the way Windows works. If it becomes damaged (or corrupt) in any way, you may find yourself unable to boot into your system. The simplest thing to try is Last Known Good Configuration. This replaces the Registry with the version that was used the last time Windows successfully loaded. In most cases this will fix the boot problem, although you'll find any changes made to the Registry since that copy was made are lost.

Nick is correct, but if you really find yourself in trouble, your next step is the Windows Recovery options.

The Windows Recovery Environment

For those of you familiar with the Recovery Console in XP, it has been replaced by the Windows Recovery Environment (WinRE). WinRE is a recovery platform based off the Windows Preinstallation Environment (WinPE), the core deployment foundation for Vista. WinRE has two primary functions, that of diagnosing problems using the Startup

Repair tool (discussed earlier in this chapter) and providing a platform for advanced recovery tools, according to the WinRE team. You can read their postings at http://blogs.msdn.com/winre/ for some great information.

Using the WinRE is easy enough. You boot up your Vista installation disk (or ISO). You will be asked to select a language, time, and so forth. When you see the button labeled Install, you can look to the bottom-left corner for the option to Repair Your Computer. This takes you into the System Recovery Options (that we mentioned earlier for memory diagnostics and Startup Repair).

Windows PE 2.0

The Windows Pre-installation Environment (WinPE 2.0) is a tool that enables you to boot the PE operating system, which is a mini-OS that allows you to handle installation, diagnostic troubleshooting, and recovery solutions for Vista. Some say WinPE is super-DOS. It's not DOS; it's more like Son-of-DOS, so call it SOD if you like.

When you load the WinRE options of the Vista DVD, it is actually running WinPE as the underlying OS. The same is true when you start the installation from the DVD. But you can actually make your own boot CDs or boot from a USB flash drive.

To begin, you should download the Windows Automated Installation Kit (Windows AIK) from Microsoft. Be sure you obtain the one from the final Vista release (in the event you are downloading or borrowing the kit from another source). The Windows AIK includes tools you need for deployment, as well as ones for creating the boot environment for WinRE. One of the most important tools you will need is `imagex.exe`, a command-line tool used for capturing, modifying, and applying installation images.

There is quite a bit of documentation to go through to fully understand the new deployment and troubleshooting tools, but it is worth it to keep your system humming along. But to understand the following discussions, you need to at least understand the basics.

The Basic Tools of WinPE

After you install the Windows AIK, the tools you need will be in those folders. If you don't want to remember all the paths, you can make a quick edit in your system's environment variables to include the paths. To do this, open your System properties, select the Advanced tab, and click the Environment Variables button. For the system variables you want to add to the path variables, be

NOTE You can also get the Windows AIK by obtaining the Business Desktop Deployment 2007 Kit. The BDD 2007 includes the Windows AIK along with other necessary deployment tools and documentation.

sure to include the paths you need. For the following examples, you add the following two paths:

```
C:\Program Files\Windows AIK\Tools\PETools
C:\Program Files\Windows AIK\Tools\x86
```

Some of the tools mentioned include the following:

- **CopyPE**—Run the `copype.cmd` script to automatically create a local Windows PE build directory. The script is located in the PETools folder. The script requires two arguments: hardware architecture and target location:

  `copype.cmd <arch> <destination>`
  Where `<arch>` can be x86, amd64, or ia64 and `<destination>` is a path to a local directory. For example

  `copype.cmd x86 c:\winpe_x86`
  (Don't create the folder ahead of time because the tool creates the folder for you.)

  The script creates the following directory structure and copies all the necessary files for that architecture:

  ```
  \winpe_x86
  \winpe_x86\ISO
  \winpe_x86\mount
  ```

- **imagex**—This tool is the mega-tool. It is "the" tool for creating and reconfiguring, as well as applying, `.wim` files. Some have compared this tool to an advanced `.zip-ping` tool, and it is in some ways. You can take files, or your entire system, and pull it into one `.wim` file. You can also compress that file. It looks at the `.wim` file as a directory so you can add to it any parts that are missing. One example of the capabilities of imagex can be seen just by looking at the `install.wim` for Vista. For starters, it's a 2GB+ file that expands out to be about 8GB. That speaks volumes for imagex's capabilities. OEMs can use this to open their Vista images, input their own Welcome Center information and other restore features, and close them again.
- **PEImg**—After you use imagex to expand a Windows PE structure, you can use PEImg to make changes to Windows PE, such as installing packages, drivers, and language packs.
- **OsCDimg**—Lets you take your `.wim` files and make them ISO files. After they're in ISO format they can be burned onto a CD to make them bootable.
- **Diskpart**—This is a command-line tool for disk management. You use this tool in preparing your keychain drive for it to be a bootable tool later.

There are other tools to consider that you can learn more about through the Windows AIK.

Creating a Windows PE Boot CD with Windows Vista and Windows AIK

Section by Mario Szpuszta (mszCool)
Microsoft Developer
http://blogs.msdn.com/mszCool

About two months ago I discovered the Windows Automated Installation Toolkit (Windows AIK or just WAIK) to be able to work with different demo images for the sessions I did at TechEd Europe with physical machines instead of the (still much slower) Virtual PC images. The WAIK includes imagex.exe, which is a tool that allows you to create images of a partition of your machine and package them into the new Windows Imaging Files (WIM).

The first steps involve using WAIK and imagex.exe. These files can be used for centralized deployment via the Windows Deployment Services (successor of Remote Installation Services). But in my case I used it to image and restore different types of demo images for my physical machines as I did not want to work with the slower VPC counterparts at a conference such as TechEd Europe. Therefore, I created two partitions on my developer machine, one with my primary OS-instance (Vista joined into our working domain for email, etc.) and a second partition for my different demo images. On the second partition I installed Windows Server 2003 with everything I needed for my demo sessions (different images, detailed steps, see below) and then I created a WIM-image from the Vista OS instance using imagex.exe from the WAIK as follows:

```
imagex /capture D: M:\WindowsImages\Windows2003_OfficeDev.wim "Windows
Server 2003 Office Development"
```

This command captures everything on drive D: into a WIM file stored on my external hard disk M:. Then I tried the demos for the session and to get the original situation again I just restored the image as follows:

```
format D: /q
imagex /apply M:\WindowsImages\Windows2003_OfficeDev.wim 1 D:\
```

To get the complete picture, here is what I did for TechEd, where I required, for example, one image for SharePoint 2007 Office Development, one image for Windows Vista for WPF and Composite UI Application Block Development, and a third one for plain old Office 2003 development (during the beta stage of Office 2007 and especially VSTO 2005 SE installing Office 2003 and Office 2007 side-by-side was not supported…right now fortunately this is supported and works really fine, therefore I have tried the imaging stuff on several machines already):

1. First I created a basic install of Windows Server 2003 on my second partition D:.
2. Then I installed my main Vista partition for regular work (email, development in our office, etc.).

3. On my main Vista instance I installed the WAIK.
4. Then I have created the first image of the Windows Server 2003 partition using `imagex /capture`.
5. Afterwards I installed everything for Office 2003 development on this Windows Server 2003.
6. Now I captured this Office 2003 development workstation using `imagex /capture`.
7. Next, I restored the original Windows Server 2003 instance using `imagex /apply`.
8. On the restored instance of Windows Server 2003, I installed everything for Office 2007 development.
9. I imaged the Office 2007 development workstation using `imagex /capture` again.
10. Now I had my demo images as WIM images available and could switch between Office 2003 and Office 2007 (beta at that point of time) within 15 minutes by restoring the appropriate image via `imagex /apply`.

With that, management of my demo partitions became really fairly easy and I was not forced to use Virtual PCs but still remain with the same advantages such as restoring an original stage of my machines very quickly.

The next step was fairly obvious. At home I used the days between Christmas and New Years to get my IT infrastructure done, at home. And of course I wanted to have a very smooth way of restoring my test servers and workstations quickly if something went wrong. So my idea was creating WIM images for each of the servers and either deploying them via Windows Deployment Services from my PDC or just from external hard disks. But I didn't want to have two OS instances on each machine (one for imaging and image restore and the other one for "productive work"). So I required a CD-bootable version of Windows to be used as imaging and restore OS-instance with imagex.exe installed. Finally, the WAIK includes all the tools for creating Windows PE instances which are bootable from either CDs, DVDs, or USB sticks (!!).

I thought before the new year starts, right now I need to try something risky with my home machine. After searching a while I've found…the steps are so simple that I was completely surprised:

1. Download and install WAIK (obvious).
2. Open the Windows PE Tools Command Prompt.

3. Create a directory for the template of your Windows PE image (e.g. `C:\WinPE` as I use it here).
4. Next switch to `C:\Program Files\Windows AIK\Tools\PETools`.
5. Execute `copype x86 C:\WinPE`.

   Now copy anything (tools, programs, etc.) you want into the ISO directory of your Windows PE template directory (in my case, `C:\WinPE`). You can create any subdirectory you want within the ISO subdirectory such as "Imaging" in the example below where I copy the imagex.exe tool to the Imaging directory of my ISO template directory as follows:

   ```
   copy "C:\Program Files\Windows AIK\Tools\x86\imagex.exe"
   c:\WinPE\ISO\Imaging
   ```

6. Then switch to `C:\Program Files\Windows AIK\Tools\PETools\x86`.

   Now apply the original Windows PE boot image:

   ```
   imagex /apply winpe.wim 1 c:\WinPE\mount
   ```

7. Using the peimg.exe tool you can install either additional drivers by specifying an INF file, or prebuilt packages such as MDAC, MSXML, or Windows Scripting support (see the following table). Examples:

   ```
   peimg /install=WinPE-XML-Package C:\WinPE\mount
   peimg /install=WinPE-Scripting-Package C:\WinPE\mount
   ```

Package Name	Description
WinPE-HTA-Package	HTML Application support
WinPE-MDAC-Package	Microsoft Data Access Component support
WinPE-Scripting-Package	Windows Script Host support
WinPE-SRT-Package	Windows Recovery Environment component
WinPE-XML-Package	Microsoft XML (MSMXL) Parser support

8. After the "mount" directory has been prepared (using `peimg.exe` with the `/prep` switch), you can create a WIM image for your ISO template directory as follows:

   ```
   imagex /capture /boot /compress max "C:\WinPE\mount"
   "C:\winpe\iso\sources\boot.wim" "mszCool PE"
   ```

9. Next you need to create the ISO image that you can burn onto a CD using any tool you want (such as Nero):

   ```
   Oscdimg -n c:\winpe\ISO c:\winpe\mszCool_winpe.iso -n
   -bc:\winpe\etfsboot.com
   ```

10. Using the OSCDIMG.EXE tool, you have created a ready-to-use ISO image that you can burn onto a CD. That CD is then a bootable version of Windows PE. From within this CD-booted instance, you can image and restore any partition on your computer you want—for free.

NOTE

If you have an error message using the tool this way, the install notes say you should actually type is:

```
Oscdimg -n –bc:\winpe\
etfsboot.com c:\winpe\ISO
c:\winpe\winpe.iso
```

As I wanted to have some fun and risk on the second-to-last day of this year, I just tried this on my home workstation by imaging and restoring my primary OS instance partition (which is the boot partition as well)…and it just rocks…it only took about 40 minutes including all the Internet search on how-to create such a Windows PE images.

Bootable USB Keys

Mario Szpuszta mentions in the previous section the capability to use Windows PE from a CD, DVD, or USB Flash drive. James O' Neil (another Microsoft developer) has some excellent advice on how to make this happen at http://blogs.technet.com/jamesone/default.aspx.

To make a USB key bootable using the Vista/Windows PE version, you need to use the Diskpart commands. Here are the commands:

1. `Select disk 1` (or the number of your USB key, be careful!)
2. `Clean` (like I said, be careful! This erases the disk.)
3. `Create partition primary`
4. `Select partition 1`
5. `Active`
6. `Format fs=fat32`
7. `Assign`
8. `Exit`

Having done that, you copy the ISO folder to the USB key

That's it. Now you have your universal tool for imaging and repairing Vista.

Now at this point you have a disk which will try to boot using BootMgr in the style of Windows PE/Vista/Longhorn server. Several people have asked about making a key which boots in the style of Server 2003/XP/Windows 2000/Windows NT. I can't make the Vista/PE version of diskpart run on Windows XP, and the older version won't prepare a USB key. So you need to do this from Vista or the Vista build of Windows PE. Once the drive is formatted, it has a Vista Boot sector—this won't boot NT/200x/XP operating systems. You need to use the BootSect utility:

```
Boosect /nt52 E:
```

This stamps a Window 2003 Server boot sector (one which uses `boot.ini`) onto drive E:. I haven't tried it, but you should be able copy NTLDR, BOOT.INI, and NTDETECT.COM onto a USB key as a way of starting a machine suffering from a corrupt boot environment.